Free Legal Aid Coordination Centre

Ukraine

Guidance on COSO 2013 Internal Control – Integrated Framework

Table of Contents

Foreword

1. **Overview**
2. **Control Environment**
3. **Risk Assessment**
4. **Control Activities**
5. **Information and Communication**
6. **Monitoring**
7. **Role of Internal Audit**

Foreword [1]

In 1992 the Committee of Sponsoring Organisations of the Treadway Commission (COSO) released its Internal Control—Integrated Framework (the original framework). The original framework has gained broad acceptance and is widely used around the world. It is recognised as a leading framework for designing, implementing, and con ducting internal control and assessing the effectiveness of internal control.

In the twenty years since the inception of the original framework, business and operating environments have changed dramatically, becoming increasingly complex, techno logically driven, and global. At the same time, stakeholders are more engaged, seeking greater transparency and accountability for the integrity of systems of internal control that support business decisions and governance of the organisation.

COSO is pleased to present the updated Internal Control—Integrated Framework (Framework). COSO believes the Framework will enable organisations to effectively and efficiently develop and maintain systems of internal control that can enhance the likelihood of achieving the entity's objectives and adapt to changes in the business and operating environments.

The experienced reader will find much that is familiar in the Framework, which builds on what has proven useful in the original version. It retains the core definition of internal control and the five components of internal control. The requirement to consider the five components to assess the effectiveness of a system of internal control remains unchanged fundamentally. Also, the Framework continues to emphasise the importance of management judgment in designing, implementing, and conducting internal control, and in assessing the effectiveness of a system of internal control.

At the same time, the Framework includes enhancements and clarifications that are intended to ease use and application. One of the more significant enhancements is the formalisation of fundamental concepts that were introduced in the original framework. In the updated Framework, these concepts are now principles, which are associated with the five components, and which provide clarity for the user in designing and implementing systems of internal control and for understanding requirements for effective internal control.

The Framework has been enhanced by expanding the financial reporting category of objectives to include other important forms of reporting, such as non-financial and internal reporting. Also, the Framework reflects considerations of many changes in the business and operating environments over the past decades, including:

• Expectations for governance oversight • Globalisation of markets and operations

• Changes and greater complexities of business

• Demands and complexities in laws, rules, regulations, and standards • Expectations for competencies and accountabilities

• Use of, and reliance on, evolving technologies • Expectations relating to preventing and detecting fraud

[1] Source: COSO Internal Control – Integrated Framework 2013

1. Overview

Definition

Internal control is defined as:

A process, effected by an entity's management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.

Objectives of Internal Control

The framework identifies **three categories of objectives**:

1. **Operations** – effectiveness and efficiency of operations, including safeguarding of assets.
2. **Reporting** – reliability, timeliness, and transparency of internal and external reporting.
3. **Compliance** – adherence to applicable laws and regulations.

Five Components of Internal Control

The 2013 framework has **five components**, which must be present and functioning:

1. **Control Environment** – the foundation, tone at the top, ethics, integrity, and governance.
2. **Risk Assessment** – identification and analysis of risks to achieving objectives.
3. **Control Activities** – policies, procedures, and practices that help ensure management directives are carried out.
4. **Information and Communication** – systems and processes that support internal control by providing relevant, timely, and quality information.
5. **Monitoring Activities** – ongoing or separate evaluations to assess effectiveness of controls over time.

Seventeen Principles of Internal Control

Each component is supported by **specific principles** to clarify expectations:

1. Control Environment

Principles

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

2. Risk Assessment

Principles

6. Specifies suitable objectives.
7. Identifies and analyses risk.
8. Assesses fraud risk.
9. Identifies and analyses significant change.

3. Control Activities

Principles

10. Selects and develops control activities.
11. Selects and develops general controls over technology.
12. Deploys control activities through policies and procedures.

4. Information and Communication

Principles

13. Uses relevant information.
14. Communicates internally.
15. Communicates externally.

5. Monitoring Activities

Principles

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

The **principles are mandatory** – all seventeen must be “present and functioning” to conclude that a system of internal control is effective.

Key Updates in 2013

- **Added seventeen principles** to make components more practical and explicit.
- Expanded emphasis on **technology** and **outsourced services**.
- Strengthened focus on **fraud risk assessment**.
- Linked controls more closely to **operations, reporting, and compliance objectives**.

2. Control Environment

Definition

The **Control Environment** sets the tone at the top. It provides the discipline, ethics, and structure that influence how people within the organisation conduct themselves and how control responsibilities are carried out.

Without a strong control environment, other four components (risk assessment, control activities, information & communication, monitoring) may not function effectively.

Principles of the Control Environment

There are **five principles** under this component:

1. **Commitment to Integrity and Ethical Values**
    - Establishing a culture of honesty and ethical behaviour.
    - Developing a code of conduct and communicating it clearly.
    - Leadership must lead by example (“tone at the top”).
2. **Management Exercises Oversight Responsibility**
    - Active, independent oversight of management.
    - Audit committee effectiveness.
    - Management involvement in setting expectations for integrity and accountability.
3. **Establishes Structure, Authority, and Responsibility**
    - Clear organisational structure, reporting lines, and delegation of authority.
    - Defined roles and responsibilities across all levels.
    - Avoiding conflicts of interest in roles.
4. **Commitment to Competence**
    - Attracting, developing, and retaining competent employees.
    - Providing necessary training and development.
    - Aligning individual skills with organisational objectives.
5. **Enforces Accountability**
    - Performance measures and incentives linked to integrity and ethics.
    - Holding individuals accountable for internal control responsibilities.
    - Clear escalation paths for reporting misconduct.

Key Elements in Practice

- **Tone at the Top** → Leadership actions strongly influence the culture.
- **Governance** → Management independence, oversight committees, and clear lines of authority.

- **Policies & Standards** → Codes of ethics, HR policies, disciplinary measures.
- **People** → Competence, recruitment, training, and succession planning.
- **Accountability Mechanisms** → Performance reviews, disciplinary action, whistleblower protections.

In short: the Control Environment is about **culture, structure, ethics, governance, and people** — the bedrock on which all other controls rest.

3. Risk Assessment

Definition

Risk Assessment is the process of identifying and analysing risks that may prevent an organisation from achieving its objectives and forming the basis for determining how risks should be managed.

It requires management to think systematically about uncertainty, fraud, and change — and to put in place processes to assess their impact on operations, reporting, and compliance.

Principles of Risk Assessment

There are **four principles** under this component:

1. **Specifies Suitable Objectives**
    - Objectives must be clear, measurable, and aligned with the entity's mission.
    - They should cover all three categories: operations, reporting, and compliance.
    - Well-defined objectives make it easier to spot risks that could derail them.
2. **Identifies and Analyses Risk**
    - Risks to objectives are identified across the entity (strategic, operational, financial, compliance, reputational, etc.
    - Risks are analysed in terms of **likelihood** and **impact**.
    - Both internal and external factors are considered.
    - Often documented in a **risk register**.
3. **Assesses Fraud Risk**
    - The organisation considers the potential for fraud in:
        - Misappropriation of assets
        - Fraudulent reporting
        - Corruption/bribery
    - Includes assessing pressures, opportunities, and rationalisations (fraud triangle).
4. **Identifies and Analyses Significant Change**
    - Monitoring external and internal changes that may impact risk (e.g., regulatory changes, economic shifts, new IT systems, restructuring).
    - Ensuring the risk assessment remains **current and dynamic**.

Key Elements in Practice

- **Risk Appetite & Tolerance** → Defining the acceptable level of risk.
- **Risk Assessment Process** → Methodology for scoring/assessing risks (heat maps, scoring matrices, etc.)
- **Fraud Risk Management** → Whistleblower lines, forensic audits, fraud awareness training.
- **Change Management** → Identifying risks when entering new markets, adopting new systems, or undergoing restructuring.
- **Documentation** → Risk registers, risk maps, and regular reporting to management and the board.

Example Risk Assessment Flow

1. Define objectives.
2. Identify risks that could prevent achieving them.
3. Assess the **likelihood** and **impact** of each risk.
4. Prioritise risks based on severity.
5. Decide on risk response (accept, avoid, reduce, transfer).
6. Document all above (Risk Register).

In short: **Risk Assessment provides the structured thinking that lets management anticipate threats and prepare controls before risks materialise.**

Sample Risk Register

Low Likelihood/Impact = 1

Medium Likelihood/Impact = 3

High Likelihood/Impact = 5

Objective	Risk Description	Likelihood	Impact	Risk Score (L×I)	Risk Response / Control Activities	Owner	Status
Ensure timely financial reporting	Delay in month-end close due to system failures	Medium	High	15	Implement backup systems; regular IT maintenance; financial close calendar	CFO	In progress
Safeguard assets	Theft or misappropriation of cash	Low	High	5	Segregation of duties; surprise cash counts; CCTV monitoring	Finance Manager	Active
Comply with laws & regulations	Non-compliance with new data protection regulations	High	High	25	Regular legal compliance reviews; staff training on data privacy; appoint Data Protection Officer	Compliance Officer	Ongoing
Maintain business continuity	Disruption from cyber-attack (ransomware)	Medium	High	15	Firewalls; multi-factor authentication; incident response plan; cyber insurance	CIO	In progress
Ensure reliable financial reporting	Fraudulent revenue recognition by sales team	Low	High	5	Audit committee oversight; whistleblower hotline; revenue recognition policy; fraud awareness training	Internal Audit	Active
Achieve operational efficiency	Staff turnover in critical roles	High	Medium	15	Succession planning; staff retention programs; knowledge management system	HR Director	Ongoing

How this links to COSO Risk Assessment principles:

- **Principle 6 – Suitable Objectives** → Each risk ties to a clear objective (operations, reporting, or compliance).
- **Principle 7 – Risk Identification & Analysis** → Risks assessed by likelihood & impact.
- **Principle 8 – Fraud Risk** → Fraudulent revenue recognition & asset misappropriation addressed.
- **Principle 9 – Change Management** → Cyber-attacks and regulatory shifts considered.

4. Control Activities

Definition

Control Activities are the policies, procedures, and practices that help ensure management directives are done to mitigate risks to achieving objectives.

They exist **throughout the organisation**, at all levels, and in all functions.

They can be **preventive** (stop errors or fraud before they happen) or **detective** (identify errors or fraud after they occur).

Principles of Control Activities

There are **three principles** under this component:

1. **Selects and Develops Control Activities**
    - Management designs control activities that address identified risks.
    - Balancing cost vs. benefit.
    - Mix of preventive and detective controls (e.g., approvals, reconciliations, segregation of duties).
2. **Selects and Develops General Controls over Technology**
    - Addressing risks from IT systems and digital processes.
    - Includes:
        - Access controls (passwords, MFA, role-based permissions)
        - Change management (testing updates before deployment)
        - Backup and recovery systems
    - Ensuring IT controls support reliable reporting, compliance, and operations.
3. **Deploys Control Activities through Policies and Procedures**
    - Formalising controls through **policies, SOPs (standard operating procedures), and manuals**.
    - Communicating these effectively across the organisation.
    - Ensuring employees understand and follow them.
    - Embedding controls into daily processes (e.g., procurement approvals, automated reconciliations).

Types of Control Activities

- **Manual Controls** → Human-performed (e.g., manager approval of expenses).
- **Automated Controls** → System-performed (e.g., system rejects duplicate vendor invoices).
- **Hybrid Controls** → Combination (e.g., system flags anomalies, staff investigates).

By purpose:

- **Preventive Controls** → Aim to stop an error/fraud (e.g., segregation of duties, pre-approval of transactions).
- **Detective Controls** → Identify when something has gone wrong (e.g., reconciliations, exception reports).
- **Corrective Controls** → Fix issues after detection (e.g., adjusting journal entries, disciplinary action).

Examples in Practice

- **Finance** → Bank reconciliations, approval hierarchies, restricted access to accounting systems.
- **Procurement** → Three-way match (purchase order, delivery note, invoice).
- **Payroll** → Independent review of payroll reports, segregation between HR and finance.
- **IT** → Role-based access, log monitoring, encryption, system backup.
- **Compliance** → Automated checks against regulatory lists, policy compliance certifications.

Why Control Activities Matter

- They **translate risk assessment into action**.
- They provide **reasonable assurance** that objectives will be achieved.
- They help organisations **prevent, detect, and respond** to errors, fraud, and inefficiencies.

5. Information & Communication

Definition:
Information & Communication is one of the five components of the COSO 2013 Internal Control Framework. It ensures that the organisation obtains or generates and uses relevant, quality information, and that this information is communicated effectively within the entity and with external parties, so that people can carry out their internal control responsibilities.

This component ensures that relevant, timely, and quality information flows within the organisation and to external stakeholders so that internal control responsibilities can be carried out effectively.

It has **three principles:**

1. **Use of Relevant Information**

- The organisation obtains or generates and uses quality information to support the functioning of internal control.
    - Data must be relevant, reliable, timely.
    - Sources may be internal (financial, operational) or external (economic, regulatory, industry).
    - Information systems must capture data consistently and accurately.

2. **Internal Communication**

- The organisation internally communicates information, including objectives and responsibilities for internal control, necessary to support its functioning.
    - Communication flows up, down, and across the entity.
    - Clear policies, procedures, and expectations must be conveyed.
    - Employees understand their role in internal control and how to escalate issues.

3. **External Communication**

- The organisation communicates with external parties about matters affecting the functioning of internal control.
    - Two-way communication with regulators, auditors, customers, suppliers, and shareholders.
    - Stakeholders are given reliable, transparent, and timely information.
    - Feedback from external parties is used to strengthen internal control.

Here is an **example for Information & Communication**

Aspect	COSO 2013 Internal Control – Information & Communication
Purpose	Provide relevant, timely, and quality information to support internal control activities.
Scope of Information	Internal control–related data (policies, compliance, operations, reporting).
Principles / Components	• 13: Use relevant information • 14: Internal communication • 15: External communication
Internal Communication	Focus on communicating control responsibilities, expectations, and escalation paths across levels.
External Communication	Communicate with auditors, regulators, customers, suppliers, and shareholders to support controls.
Reporting	Reports are about internal control effectiveness and compliance.
Objective Orientation	Supports achievement of operations, reporting, and compliance objectives.

Here are **three full public sector case studies** using the template, showing how **COSO 2013 Internal Control** handles **Information & Communication**:

1. Public Finance – Budget Execution

Principle	COSO 2013 Internal Control
Use of Relevant Information	Ministry gathers expenditure and revenue data to ensure accuracy of financial reports and compliance with budget law.
Internal Communication	Directives circulate within departments ensuring staff follow expenditure controls, procurement rules, and reporting deadlines.
External Communication	Mandatory financial reports are submitted to Parliament, auditors, and donors for accountability.
Reporting	Reports focus on legality, accuracy, and compliance of spending.

2. Education – National School System

Principle	COSO 2013 Internal Control
Use of Relevant Information	Ministry gathers enrolment, attendance, and exam pass rates to monitor compliance with education standards.
Internal Communication	Circulars ensure schools report attendance and exam results consistently; teachers know compliance requirements.

Principle	COSO 2013 Internal Control
External Communication	Reports sent to Parliament and oversight bodies on enrolment, graduation rates, and budget use.
Reporting	Focused on achievement of basic operational objectives (attendance, budget use).

3. Infrastructure – National Transport Projects

Principle	COSO 2013 Internal Control
Use of Relevant Information	Ministry tracks project costs, timelines, and contract compliance to ensure proper internal control.
Internal Communication	Contractors and regional offices submit compliance reports; central ministry monitors control adherence.
External Communication	Reports shared with Parliament, auditors, and funding agencies to demonstrate compliance.
Reporting	Reports highlight whether projects stayed within budget and schedule.

Takeaway

- Information & Communication ensures compliance, accountability, and reliable data for **internal control effectiveness**.

6. Monitoring Activities

Definition:

Monitoring Activities are one of the five components of the COSO 2013 Internal Control Framework. They consist of ongoing evaluations, separate evaluations, or a combination of both, to ascertain whether the five components of internal control are present and functioning. Any identified deficiencies are communicated in a timely manner to those responsible for corrective action, including senior management.

It has **two principles:**

1. **Ongoing and/or Separate Evaluations** – The organisation selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

2. **Evaluation and Communication of Deficiencies** – The organisation evaluates and communicates internal control deficiencies in a timely manner to parties responsible for taking corrective action.

In simple terms: Monitoring Activities ensure that internal controls are not just designed properly but are **working effectively over time** — and that problems are found and fixed quickly.

Here are a couple of **public sector examples** of how **COSO 2013 Monitoring Activities** work in practice:

Example 1: Public Finance – Expenditure Controls

- **Ongoing Evaluations:**

  The Ministry of Finance uses an automated system to monitor daily expenditure transactions against the approved budget, flagging overspending in real time.

- **Separate Evaluations:**

  The Internal Audit Unit performs periodic reviews of procurement and payment processes to assess whether controls are effective.

- **Communication of Deficiencies:**

  If irregularities are found (e.g., unauthorised spending), they are reported to management and Parliament's Public Accounts Committee for corrective action.

Example 2: Education – School Performance Monitoring

- **Ongoing Evaluations:**

  Regional education offices track student attendance and teacher performance through regular monthly reporting.

- **Separate Evaluations:**

  The Ministry commissions external evaluations every three years to assess curriculum delivery and compliance with education standards.

- **Communication of Deficiencies:**

  Weaknesses (e.g., low literacy rates, high dropout rates) are reported to the Minister of Education, with recommendations for corrective measures such as teacher training or resource allocation.

Example 3: Infrastructure – Public Works Projects

- **Ongoing Evaluations:**

  Project managers monitor construction progress, cost, and safety compliance using digital dashboards.

- **Separate Evaluations:**

  An independent engineering firm audits project quality and contract adherence at completion milestones.

- **Communication of Deficiencies:**

  Findings (e.g., delays, substandard materials) are escalated to the Infrastructure Ministry and funding agencies for remediation.

Takeaway:

In the public sector, **Monitoring Activities** combine **real-time tracking** (ongoing) with **independent reviews** (separate), ensuring that internal controls remain effective and that problems are promptly escalated to decision-makers.

7. Role of Internal Audit

In the **COSO Internal Control – Integrated Framework (2013)**, internal audit is not explicitly listed as one of the five components or 17 principles, but it plays an important **supporting and assurance role** across the entire framework. Internal audit helps ensure that management's system of internal control is designed well and operating effectively.

Here's a structured breakdown of its role:

1. Independent Assurance

- Internal audit provides **independent, objective assurance** to the board, audit committee, and senior management on whether the five components of internal control (Control Environment, Risk Assessment, Control Activities, Information & Communication, Monitoring) are present and functioning.
- Confirms whether risks are identified and addressed properly within the internal control framework.

2. Monitoring Activities (Component 5)

- Internal audit is a **key element of the Monitoring Activities** component.
- The framework distinguishes between:
    - **Ongoing monitoring** (performed by management as part of daily operations)
    - **Separate evaluations** (independent assessments) → internal audit typically performs these.
- Provides feedback on control deficiencies and makes recommendations for improvement.

3. Supporting Governance & Oversight

- Reinforces the **tone at the top** by reporting to the board/audit committee.
- Enhances accountability by assessing whether management has established a proper internal control culture.

4. Risk-Based Auditing

- Uses the **risk assessment component** of COSO to focus audit plans on the areas of greatest risk.
- Aligns internal audit's work with the organization's strategic, operational, compliance, and reporting objectives.

5. Advisory Role (without taking ownership)

- Internal audit may act as a **trusted advisor** by:
    - Recommending improvements to control design.
    - Sharing insights on emerging risks.
    - Helping embed the COSO framework in business processes.
- But it must **avoid assuming management responsibilities** (so independence is not compromised).

In summary: internal audit, within COSO 2013, is primarily linked to the **Monitoring Activities** component, where it performs **separate, independent evaluations** of internal control effectiveness. At the same time, it supports the other four components by giving assurance, identifying control gaps, and promoting continuous improvement, while maintaining independence from management.