SmartSuite

Framework / Risk Management / COSO

# COSO ERM Framework (2017)

COSO ERM is a framework that helps organizations identify, assess, manage, and monitor enterprise risks to achieve objectives.

## What it is

The COSO Enterprise Risk Management (ERM) Framework—2017 is an integrated risk management framework that enables organizations to identify, assess, manage, and monitor risks to achieve their strategic and operational objectives. It provides a structured approach for embedding risk management practices into decision-making processes, supporting both value creation and the protection of enterprise assets.

Developed and published by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), this framework is widely adopted by organizations, board members, auditors, and compliance professionals. It spans risk management, internal controls, compliance oversight, and operational resilience, offering a foundation that aligns with other regulatory frameworks and standards, such as Sarbanes-Oxley (SOX), ISO 31000, and industry-specific guidance.

## At a glance

| | | |
|---|---|---|
| PUBLISHER<br>Committee of Sponsoring Organizations of the Treadway Commission (COSO) | TYPE<br>Framework | VERSION<br>COSO ERM 2017 — Enterprise Risk Management: Integrating with Strategy and Performance |
| EFFECTIVE<br>September 2017 | DOMAIN<br>Risk Management | FAMILY<br>COSO |
| REGION<br>United States | ADOPTION MODEL<br>Risk Management | IMPLEMENTATION COMPLEXITY<br>High |

Source: https://www.coso.org/erm-framework

## Why it matters

- **Strengthen risk-based decision-making** Enable leadership to make informed strategic choices by integrating risk assessment into core business planning processes.
- **Enhance regulatory alignment** Support compliance with Sarbanes-Oxley and other regulations by embedding risk management into internal controls and oversight activities.
- **Improve operational resilience** Mitigate disruptions by identifying, assessing, and responding to operational risks in a structured and consistent manner.
- **Increase audit readiness** Facilitate transparent reporting and documentation, making it easier to demonstrate effective risk management during audits.

 © 2026 SmartSuite Inc. All rights reserved. 

## How SmartSuite supports COSO ERM 2017

### Enterprise Risk Register and Taxonomy

Standardize risk categories, scoring, ownership, and enterprise-wide visibility.

### Risk Appetite and Tolerance Tracking

Document appetite statements, thresholds, and escalation triggers with evidence.

### KRIs and Ongoing Monitoring

Track KRIs, thresholds, and recurring reviews to detect changing risk early.

### Risk Treatment and Residual Risk Management

Manage mitigation actions, due dates, approvals, and residual risk acceptance.

### Issue and Event Linkage

Connect incidents, findings, and issues to the risks they impact for faster response.

### Executive and Board Reporting

Deliver leadership-ready dashboards on exposure, trends, and open actions.

## Common framework mappings

COBIT 2019 | COSO IC 2013 | ISO 22301 | ISO 31000:2018 | ISO 27001:2022 | NIST CSF 2.0 | NIST 800-37 Rev.2

## Official resources

### COSO Enterprise Risk Management (ERM) Framework — 2017

Defines the COSO ERM framework for effective risk management and oversight processes.

coso.org/erm-framework

### COSO ERM Implementation Guidance

Provides actionable insights for integrating ERM principles across an organization.

coso.org/guidance-erm

### COSO ERM Executive Summary

Outlines the key aspects and benefits of implementing the COSO ERM framework.

coso.org/guidance-erm

## Frequently asked questions

### What is the COSO ERM Framework used for?

The COSO ERM Framework is used to help organizations identify, assess, manage, and monitor risks that could impact the achievement of their strategic and operational objectives. It provides a systematic approach to embedding risk management into decision-making processes, supporting both value creation and the protection of enterprise assets.

### Is COSO ERM certifiable or required by law?

COSO ERM is not a certifiable standard, nor is it legally mandatory. However, it is widely adopted as best practice and often referenced by regulators, auditors, and industry standards—particularly in connection with compliance programs like Sarbanes-Oxley (SOX).

### Who should use the COSO ERM Framework?

The COSO ERM Framework is applicable to organizations of all sizes and sectors, including public, private, and not-for-profit entities. It is particularly relevant for executive leadership, risk managers, compliance teams, auditors, and board members involved in risk oversight and governance.


Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

### What are the key components and artifacts of COSO ERM?

COSO ERM is structured around five interrelated components: Governance and Culture; Strategy and Objective-Setting; Performance; Review and Revision; and Information, Communication, and Reporting. Key artifacts include risk registers, risk appetite statements, control libraries, and documentation of risk assessments and mitigation actions.

### How do organizations implement the COSO ERM Framework?

Organizations implement COSO ERM by integrating risk management activities into governance protocols, strategic planning, and daily operations. Practical steps involve conducting risk assessments, maintaining risk registers, defining internal controls, assigning risk ownership, and establishing ongoing monitoring and reporting processes.

### How does COSO ERM relate to other regulatory frameworks and standards?

COSO ERM aligns well with other risk management frameworks such as ISO 31000 and regulatory requirements like Sarbanes-Oxley (SOX). Its principles provide a foundation that can be mapped to controls and processes required by various industry regulations and standards, supporting a unified approach to compliance.

### What are the ongoing requirements to maintain COSO ERM compliance?

Maintaining COSO ERM compliance requires continuous risk monitoring, regular review and updating of risk registers and control activities, periodic risk assessments, ongoing staff training, and effective risk communication to stakeholders. Documentation and evidence of these activities are crucial for demonstrating compliance during audits.

### How would SmartSuite support COSO ERM Framework?

SmartSuite supports COSO ERM by enabling organizations to maintain centralized risk registers, manage control libraries, track governance and compliance activities, and collect evidence needed for audit readiness. The platform facilitates risk tracking, remediation workflows, compliance reporting, and dashboard-based oversight to ensure ongoing risk governance and alignment with COSO ERM principles.

License included / downloadable: No The COSO ERM Framework is published by the Committee of Sponsoring Organizations of the Treadway Commission. Access to the full framework documentation typically requires purchasing official materials from COSO. License not included with platform

Full framework page and mappings: smartsuite.com/frameworks/coso-enterprise-risk-management-framework-2017