SmartSuite

Framework / Risk Management / COSO

COSO ERM Framework (2017)

COSO ERM (2017) sets five components and 20 principles for integrating risk management with strategy and performance. It is voluntary guidance from COSO, not a regulation.



What it is

COSO's Enterprise Risk Management: Integrating with Strategy and Performance (2017) is a framework of five components and 20 principles for building risk management into strategy-setting and performance. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) published it in 2017 as an update to its 2004 Enterprise Risk Management: Integrated Framework. It is guidance that organizations adopt voluntarily, not a law.

COSO is a private-sector initiative sponsored and funded by the American Accounting Association, the American Institute of Certified Public Accountants, Financial Executives International, the Institute of Management Accountants and The Institute of Internal Auditors. The Framework is written for boards and management in entities of any size, from small businesses and social enterprises to government agencies and large public companies.

At a glance

PUBLISHER Committee of Sponsoring Organizations of the Treadway Commission (COSO)	TYPE Framework	VERSION Enterprise Risk Management: Integrating with Strategy and Performance (2017), five components and 20 principles
EFFECTIVE June 2017	DOMAIN Risk Management	FAMILY COSO
REGION United States	ADOPTION MODEL Risk Management	IMPLEMENTATION COMPLEXITY High

Source: coso.org/erm-framework

Why it matters

- **Risk considered when strategy is chosen** Strategy selection weighs three things: risk to the chosen strategy, the possibility that the strategy does not align with mission, vision and core values, and the implications of the strategy chosen (executive summary, pages 4 and 5).
- **Risk appetite tied to decisions** The organization defines risk appetite in the context of creating, preserving and realizing value, and aligns it with strategy and business objectives (principle 7).
- **An entity-wide view** Management develops and evaluates a portfolio view of risk, because a risk can start in one part of the entity and affect another (principle 14).
- **Less variability in performance** Understanding the risks that affect performance targets lets management act early, whether performance runs behind or ahead of expectations (executive summary, page 4).

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports COSO ERM 2017

Governance and Culture Records

Record board oversight, operating structures, the desired culture and core-value commitments as the evidence for principles 1 to 5.

Risk Appetite and Strategy Link

Hold the risk appetite statement, the alternative strategies evaluated and the business objectives each risk affects (principles 7 to 9).

Risk Register and Severity

Log identified risks with severity, priority and owner, linked to the objective they could affect (principles 10 to 12).

Responses and Portfolio View

Track the risk response chosen for each risk and view exposure by objective, unit and category as a portfolio (principles 13 and 14).

Change and Performance Reviews

Schedule reviews of performance and risk, and log substantial changes and improvement actions (principles 15 to 17).

Risk, Culture and Performance Reporting

Build dashboards of risk, culture and performance for management, the board and other stakeholders (principles 18 to 20).

Common framework mappings

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

Official resources

COSO ERM Framework Page (COSO)

COSO's ERM framework page, which features its guidance on compliance risk management.

coso.org/erm-framework

COSO Enterprise Risk Management Guidance (COSO)

The 2017 publication, free executive summary, compendium of examples and ERM thought papers.

coso.org/guidance-erm

ERM Executive Summary, June 2017 (COSO PDF)

Free executive summary: the five components, 20 principles and key concepts.

coso.org/_files/ugd/3059fc_61ea5985b03c4293960642fdce408eaa.pdf

Frequently asked questions

What is the COSO ERM Framework, and what does it contain?

Enterprise Risk Management: Integrating with Strategy and Performance (2017) is COSO's framework for managing risk together with strategy and performance. It sets out five interrelated components supported by 20 principles, and it updates COSO's 2004 Enterprise Risk Management: Integrated Framework. COSO describes enterprise risk management as the culture, capabilities and practices applied with strategy-setting, not a department.

Is COSO ERM mandatory?

No. COSO is a private-sector initiative, and the Framework is guidance that organizations choose to adopt. No regulator enforces it. Organizations use it to give boards and management a common approach to risk and to show how risk is considered in strategy and performance.

What are the five components and 20 principles?

The components are Governance and Culture (principles 1 to 5), Strategy and Objective-Setting (6 to 9), Performance (10 to 14), Review and Revision (15 to 17) and Information, Communication, and Reporting (18 to 20). The principles run from exercising board risk oversight (1) to reporting on risk, culture and performance (20), and include defining risk appetite (7) and developing a portfolio view (14).

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How does COSO ERM differ from COSO Internal Control, and which one is used for SOX 404?

The two publications are distinct, and neither supersedes the other. Internal control is one part of what enterprise risk management covers. For assessments of internal control over financial reporting under SOX section 404, the control framework used is COSO's Internal Control: Integrated Framework (2013), which PCAOB standards describe as a suitable and available framework for management's annual assessment.

Where can an organization get the Framework text?

COSO publishes a free executive summary dated June 2017 on coso.org. The full Framework is sold by COSO as an eBook or softcover. COSO's copyright notice states that no part may be reproduced, redistributed, transmitted or displayed without COSO's written permission, so SmartSuite links to the publication rather than reproducing it.

License included / downloadable: No COSO publishes a free executive summary. The full Framework is a paid publication (eBook or softcover) from COSO, and COSO's copyright notice bars reproduction without its written permission. The framework text is not included with the platform.

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