RISK AND RESILIENCE

Enterprise Risk Frameworks

COSO ERM · ISO 31000 · Kaplan & Mikes

PAPER 01 / 03

A Furtherance reference compendium on the intellectual traditions behind organisational design, leadership, execution, and culture.

IN THIS PAPER

This paper opens the Risk and Resilience series in Furtherance's reference library. It covers the formal frameworks for managing risk across an enterprise – the standards boards and auditors rely on, and the managerial reframing that makes them useful. The question it answers: how should an organisation structure the way it identifies, weighs and treats risk?

COSO integrates risk with strategy and performance; ISO 31000 offers a principles-based, universal process; Kaplan and Mikes cut through both with the crucial insight that different *kinds* of risk demand different management.

COSO ERM Enterprise Risk Management framework, 2004 / 2017

US-origin ERM · strategy and performance

CORE THESIS

Enterprise risk management should be **integrated with strategy and performance**, embedded across the organisation and governed from the top – not run as a separate compliance silo. The 2017 update reframed ERM explicitly around strategy-setting and value.

FRAMEWORK

Component	Focus
Governance and culture	Board oversight, risk culture, values
Strategy and objective-setting	Risk appetite tied to strategy
Performance	Identify, assess and prioritise risk to objectives
Review and revision	Reassess as conditions change
Information and reporting	Communicate risk across the organisation

METHODOLOGY

A consensus framework from the sponsoring accounting and audit bodies, grounded in internal control.

SIGNIFICANCE AND CRITIQUE

The dominant US-origin ERM framework, familiar to boards and auditors. The critique: its internal-control heritage can make it feel compliance-heavy and checklist-driven.

ISO 31000 Risk Management, 2009 / 2018

International standard · principles-based

CORE THESIS

A **principles-based, universally applicable** approach: risk is “the effect of uncertainty on objectives,” and managing it should be integrated into every activity, customised to context, and continually improved.

FRAMEWORK

Layer	Content
Principles	Integrated, structured, customised, inclusive, dynamic
Framework	Leadership, commitment, and organisational integration
Process	Scope and context ▯ assessment ▯ treatment ▯ monitor
Assessment	Identify, analyse and evaluate the risks

METHODOLOGY

An international consensus standard, deliberately generic and non-prescriptive.

SIGNIFICANCE AND CRITIQUE

The global reference standard, flexible across sectors and risk types. The critique: its generality means it guides rather than prescribes, and it is not a certification.

Kaplan & Mikes Managing Risks: A New Framework, 2012

Managerial reframing · categories of risk

CORE THESIS

Not all risks are alike, and a single rulebook cannot manage them all. Risks fall into **three categories**, each needing a different approach — the central failure of much risk practice is treating strategy and external risks as if they were compliance risks.

FRAMEWORK

Category	Nature and management
Preventable (I)	Internal, controllable — rules, compliance, controls
Strategy (II)	Taken for return — risk dialogue, dashboards, envision failure
External (III)	Uncontrollable — stress tests, scenarios, war games

A key implication: the independent risk function's role differs by category — enforcing rules for the first, challenging assumptions for the second and third.

METHODOLOGY

A managerial framework drawn from research and practice across firms and sectors.

SIGNIFICANCE AND CRITIQUE

The sharpest reframing of why risk management often fails — by mismatching method to risk type. The critique: it is a taxonomy and orientation rather than a detailed method.

Synthesis

Framework	Nature	Key idea	Register
COSO ERM	US standard	Integrate risk with strategy	Board / audit
ISO 31000	Global standard	Principles-based process	Universal
Kaplan & Mikes	Managerial	Three categories of risk	Reframing

FOR THE OPERATOR

The formal frameworks give risk a structure – integrated with strategy and performance (COSO), a principles-based universal process (ISO 31000), and matched to the kind of risk in play (Kaplan & Mikes). For the operator: build a risk process, but don't manage strategy and external risks with a compliance rulebook – each category needs its own method. The next paper turns to why complex systems fail, and how some stay remarkably safe.