Gartner Research

What to Include in ERM Frameworks, Policies, Charters and More

Gartner

What to Include in ERM Frameworks, Policies, Charters and More

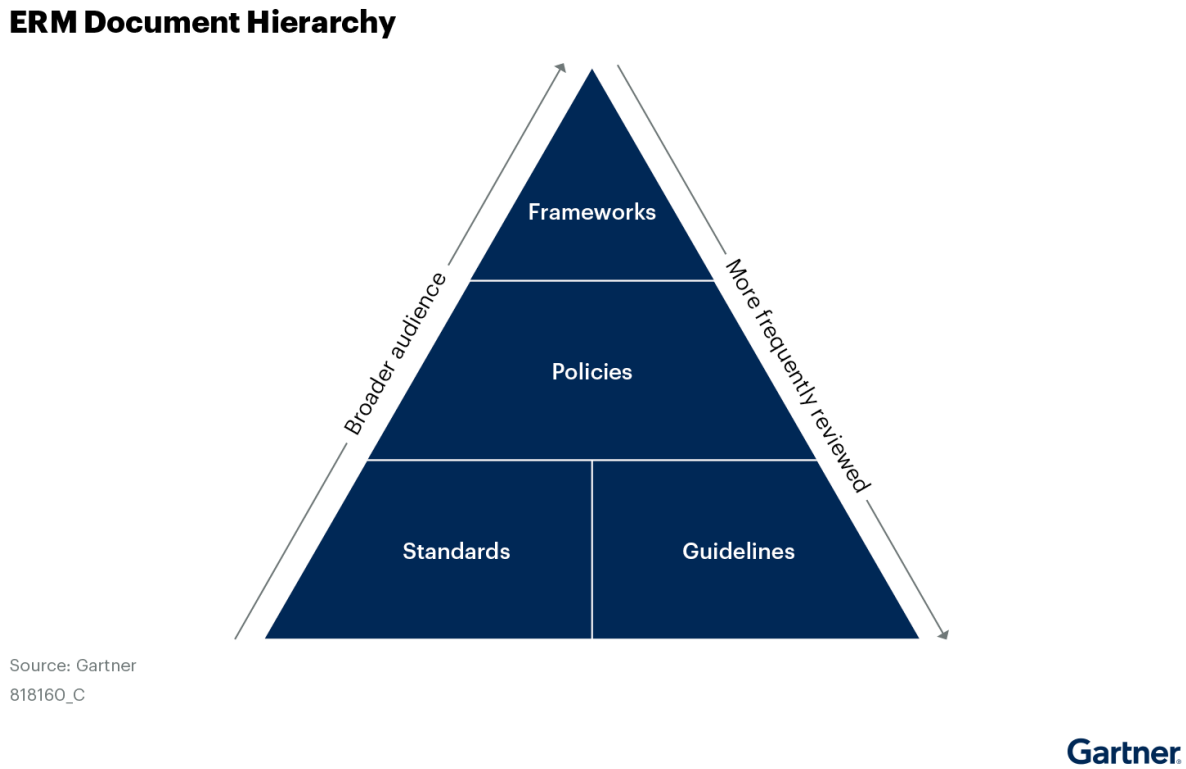
Introduction

Without a universally accepted standard on the structure of enterprise risk governance, heads of ERM have many choices to make when crafting their ERM programs' governance documentation. For example, ERM departments can be governed by various types of ERM frameworks, and many frameworks, policies, standards and guidelines can be combined into overlapping documents. The amount of choice with which heads of ERM, executives and corporate directors are confronted often leads to confusion as to what each type of document should do and how they should relate to each other.

This research directs heads of ERM on what to include in each type of document to fulfill its specific purpose and be easily consumed, based on our review of ERM governance documents and interactions with clients. Providing a clear and separate purpose for each type of document allows each to have maximum utility for varying audiences and have different review frequencies.

Figure 1 demonstrates the hierarchy of ERM governance documentation as commonly observed by Gartner. Frameworks have the broadest audience; you should anticipate that they will be reviewed by boards, executives and risk owners across the enterprise. Policies and especially standards and guidelines, on the other hand, are typically written specifically for enterprise risk owners and others with specific concerns over a risk or organizational domain.

Figure 1: ERM Document Hierarchy



Risk committee charters, also addressed in this guide, are not part of the hierarchy and are intended only for committee use.

Analysis

Use ERM Frameworks to Establish Governance and Risk Management Strategy

Heads of ERM can select an existing ERM framework to establish a high-level structure and guidance for implementing and managing risk, and customize the framework to suit organizational needs. COSO 2017 and ISO 31000 are the two best known and widely used ERM frameworks.

Comparing the COSO 2017 and ISO 31000 ERM Frameworks

	COSO 2017	ISO 31000: 2018
Scope	Most prominent in North America; able to be applied by any industry or sector. COSO is explicitly about ERM.	An international framework; able to be applied by any industry or sector. ISO 31000 is a framework for general risk management. However, it is commonly applied to ERM.
Key components	■ Governance and culture ■ Strategy and objective setting ■ Performance ■ Review and revision ■ Information, communication and reporting	■ Principles ■ Framework ■ ERM process
Orientation	COSO is linked to the Sarbanes-Oxley Act requirements for companies listed in the U.S.; it therefore has a control and compliance orientation.	ISO 31000 focuses on integrating risk management into the regular management processes of an organization.
Area of focus	Focuses on the senior levels of the organization.	Focuses on all levels of the organization.
Definition of risk management	Enterprise risk management is the culture, capabilities and practices, integrated with strategy setting and its execution, that organizations rely on to manage risk in creating, preserving and realizing value.	Risk management is a set of coordinated activities to direct and control an organization regarding risk.
Definition of risk	The possibility that events will occur and affect the achievement of strategy and business objectives.	The effect of uncertainty upon objectives.

Source: Gartner (August 2024)

Heads of ERM can then consider customizing the COSO 2017 or ISO 31000 frameworks, or building an original framework, to further clarify the governance model and risk management strategy. See below for some examples of considerations when customizing or building an ERM framework.

Considerations for Custom ERM Frameworks

Characteristic	Key considerations
Size	Smaller teams may set fewer or less comprehensive goals to avoid exceeding bandwidth.
Maturity level	Newly established ERM departments may have to expand on the importance of ERM/ERM processes.
Industry	Certain industries may be governed by specific regulation.
Goal	The impetus for the change in or adoption of a new framework can be to establish overarching principles or to prescribe or change something specific.

Source: Gartner (August 2024)

Whether implementing an external or customized framework, heads of ERM should ensure that frameworks achieve the following objectives:

- Establish a governance model.
- Define risk as it pertains to the organization and its industry.
- Establish an overarching risk management strategy for the entire organization that will guide ERM policies.
- Establish risk assessment and mitigation techniques to achieve the risk management strategy.

Heads of ERM can encourage comprehension of the ERM framework by avoiding highly technical language and department-specific instructions, instead opting for language that can be understood by both executives and business unit personnel. Ideally, heads of ERM should keep the length to a few pages to allow executives and boards to quickly understand the entire framework content.

Use ERM Policies to Document Risks, Responsibilities and Processes

ERM policies are often longer than frameworks and include more technical language to establish acceptable risk owner behavior. Policies are most effective after consultation with the risk owners, risk liaisons, and legal and compliance departments to ensure adherence to relevant regulations and alignment with other related documentation.

Comparing ERM Frameworks and Policies

	Frameworks	Policies
Audience	Entire organization	Risk owners
Length	10 to 12 pages, for example	10 to 20 pages, for example
Common authoring process	Head of ERM recommends an external framework or adapts one for organizational context, then approves with ERC and board.	Head of ERM liaises with the executive risk committee (ERC), risk owners and risk liaisons, then approves with ERC and board.
Review cadence	Commonly once every two years	Commonly once a year
Key components	■ Organizationwide goals ■ Risk governance structure ■ Overview of the risk process	■ Risk domain focus ■ Role responsibilities ■ When and how to collaborate with the ERM department

Source: Gartner (August 2024)

Detailed and instructive ERM policies help employees determine whether business activities are aligned with the organization's risk management goals. Be sure ERM policies contain the following components:

- Objective of the policy
- Definitions of relevant key terms within the policy
- Specific evaluation guidelines to make sure that business activities are aligned with desired risk strategy
- Assignment of responsibility to specific roles or teams

Use ERM Standards and Guidelines to Instruct Risk Owner Behavior

ERM standards and guidelines describe how risk owners adhere to ERM policies in their daily business activities. Heads of ERM should separate standards and guidelines from policies to allow for further detail, though they can be directly referenced within a relevant ERM policy.

Standards should specify actions that risk owners must take to adhere to the ERM policies. They can include decision matrices to aid employees in risk-aware decision making. For example, a risk assessment standard requires stakeholders to evaluate individual enterprise risks using a set of risk rating criteria.

Guidelines should explain best practices for employees to support the organizational risk culture, such as a guide to risk-informed decision making. They are not required actions, like standards.

Both standards and guidelines need to be reviewed the most frequently out of all components of the hierarchy to assess effectiveness. They include the most technical language.

Oversee the Creation of Risk Committee Charters to Define Structure and Accountability

The ERC (or its equivalent) serves as an extension of the board of directors' risk oversight function (e.g., the board risk committee [BRC] or audit committee) and is made up of executive leadership rather than board members. Risk committees should establish committee charters to clarify their agenda, scope and composition. Both executive risk committees and board risk committees should have their own charters, which can be referenced in cases of uncertainty about committee activities.

Heads of ERM can encourage risk committee members to incorporate the following guidelines to organize productive activities and avoid accountability issues among members:

- Explain the risk committee's purpose to ensure that members understand how the committee contributes to the organization's strategy and objectives.
- Include an exhaustive list of the goals and objectives of the committee.
- Include a statement on corporate responsibility, specifically regarding the obligation to protect sensitive stakeholder data, including that of customers, suppliers and employees.
- Outline the scope of the committee with respect to the functions that are included, and state the roles and responsibilities of each committee member.
- List meeting frequency and the time commitment required from members.
- Obtain sponsorship for the charter from either the CEO or the board to inform members that risk is a top priority from management's perspective.
- Keep the charter's length short to encourage members to read the complete document.
- Use business language and avoid jargon that can result in confusion or misunderstanding.
- Avoid using specific job titles, which can change as the organization evolves, since the charter should remain comparatively static.

Evidence

This research is based on over 50 interactions with ERM leaders on governance-documentation-related topics; prior Gartner research; a review of client and publicly available ERM policies, frameworks and other governance documentation and data from the Gartner ERM Budget & Efficiency Benchmark on the percentages of ERM programs that use various types of ERM frameworks (including custom frameworks).

© 2024 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. It consists of the opinions of Gartner's research organization, which should not be construed as statements of fact. While the information contained in this publication has been obtained from sources believed to be reliable, Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by Gartner's Usage Policy. Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see "Guiding Principles on Independence and Objectivity." Gartner research may not be used as input into or for the training or development of generative artificial intelligence, machine learning, algorithms, software, or related technologies.

Actionable, objective insight

Position your enterprise risk management function for success. Explore these additional complimentary resources and tools:

Webinar

Join a Virtual Event

Hear the latest insight from Gartner experts at an upcoming or recorded event.

Watch Now

Guide

Risk Reporting That Drives Executive Action

Discover best practices for risk reporting and empower leaders to make decisions quickly.

Download Now

Template

Risk Management Strategy Template

A 5-step template for heads of ERM to craft an effective risk management strategy.

Download Now

How We Help

Gartner for Legal, Risk & Compliance Leaders

Discover how we can help you tackle your mission-critical priorities.

Learn More

Already a client?
Get access to even more resources in your client portal. Log In

Connect With Us

Get actionable, objective insight that drives smarter decisions and stronger performance on your mission-critical priorities. Contact us to become a client:

U.S.: 1 855 811 7593

International: +44 (0) 3330 607 044

Become a Client

Learn more about Gartner for Legal, Risk & Compliance
gartner.com/en/audit-risk/products/gartner-for-risk

Stay connected to the latest insight

© 2024 Gartner, Inc. and/or its affiliates. All rights reserved. CM_GBS_3314271