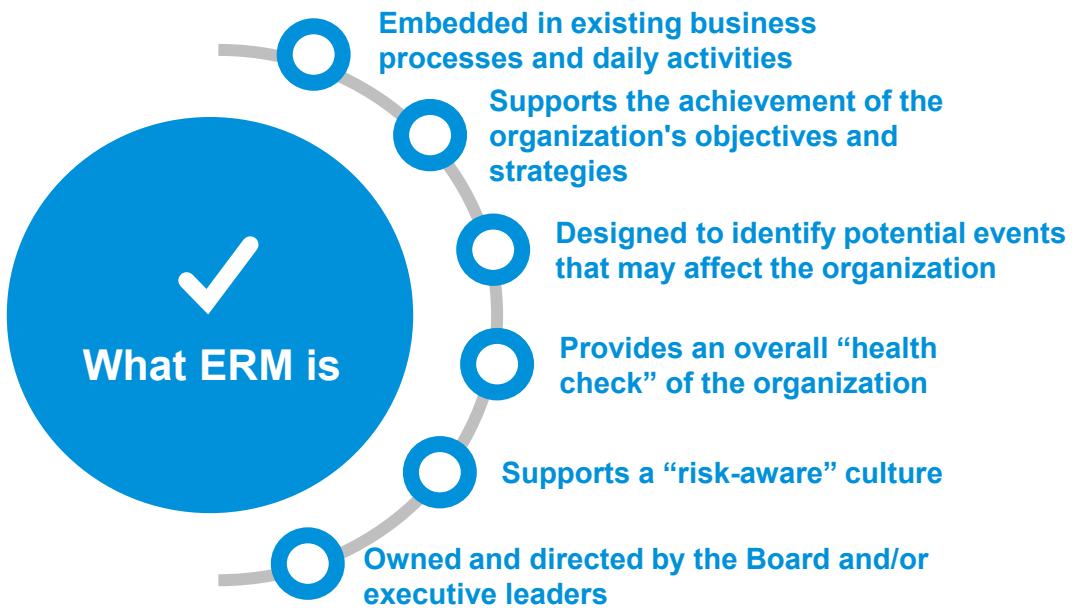
KPMG ERM Perspectives

April 2025

ERM OVERVIEW

When properly embedded within business operations and appropriately empowered, an ERM program can support and enable:

- Deeper insight and understanding of *risks* AND *opportunities*
- Consistent performance and reduced “surprises”
- Delivery of high quality products and services
- Achievement of strategic objectives and priorities
- A more proactive and predictive risk posture
- Strengthened competitive advantage



The enterprise risk journey

Organizations that succeed will be the ones that can transform and continue to adapt to ongoing change.

ENTERPRISE RISK PROGRAM PRINCIPLES

01 Business-relevant enterprise risk content

Maintain the right risk content, while keeping it relevant and dynamic. Identify those risks and vulnerabilities that could threaten the organization's overall business strategy or model.

02 Tailored, proportionate enterprise risk process

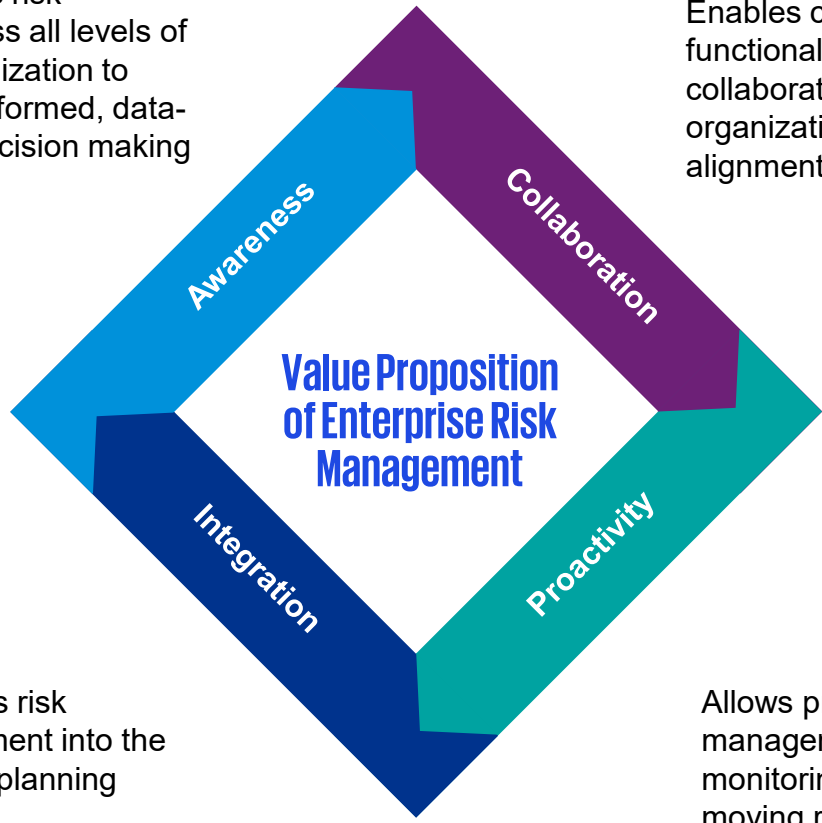
Adopt a unified vision and clear objectives of ERM – processes built with a clear view of the potential benefits of ERM as a strategic tool.

03 Aligned governance, risk, and compliance activities

Recognize the opportunity to coordinate often fragmented risk assessment and assurance work streams, simplify reporting, and streamline oversight to provide better risk coverage across their activities.

Promotes risk awareness all levels of the organization to enable informed, data-driven decision making

Enables cross-functional collaboration and organizational alignment



Integrates risk management into the strategic planning process

Allows proactive management and monitoring of fast-moving risks

Guiding principles of risk management

To navigate opportunities, successful programs need to:

01 **Connect risks** across the enterprise and functions to enable strategic risk reporting

02 Improve **collaboration and prioritization** of initiatives to improve resource allocation

03 Enhance **risk awareness and ownership** at the appropriate levels of the organization

04 Drive alignment through a **simplified risk governance structure** and common tools

05 Provide guidance for **efficient and effective** risk related activities across the enterprise

Enterprise Risk Management Framework

Note: KPMG's ERM framework aligns to COSO ERM 2017 and ISO 31000.

Governance & Strategy

Board Oversight & Expectation	Governance & Committee Structure	Lines of Defense / Responsibilities	Risk Strategy	Linkage to Corporate Strategy	Risk Appetite	Governance Documentation	Risk Taxonomy & Structure	Issues Definition & Classification

Framework Execution Components

Identification & Classification	Assessment & Measurement	Management & Monitoring	Issue Management & Remediation	Reporting & Insights
Risk Identification Process	Assessment Process	Risk Analysis / Deep Dives	Root Cause Analysis	Reporting Process & Structure
Risk Sources & Level	Assessment Scope / Target	Risk Response & Documentation	Remediation & Plan Development	Report Aggregation & Dashboards
Emerging & Evolving Risks	Risk Criteria, Scoring & Aggregation	Metrics / Tolerances	Risk Acceptance	Reporting by Level
Risk Inventory / Library	Risk Connectivity	Control Inventory / Library	Issue Identification & Management	External Reporting
	Risk Prioritization	Control Validation & Assurance	Issue Escalation	
		Risk Escalation & Breach Protocol		

Framework Enablers

Risk Culture	Effective Challenge
Training & Development	Risk Data & Technology Strategies
Roles & Responsibilities	Data Governance & Management
Communication / Stakeholder Management	Technology Enablement

KPMG

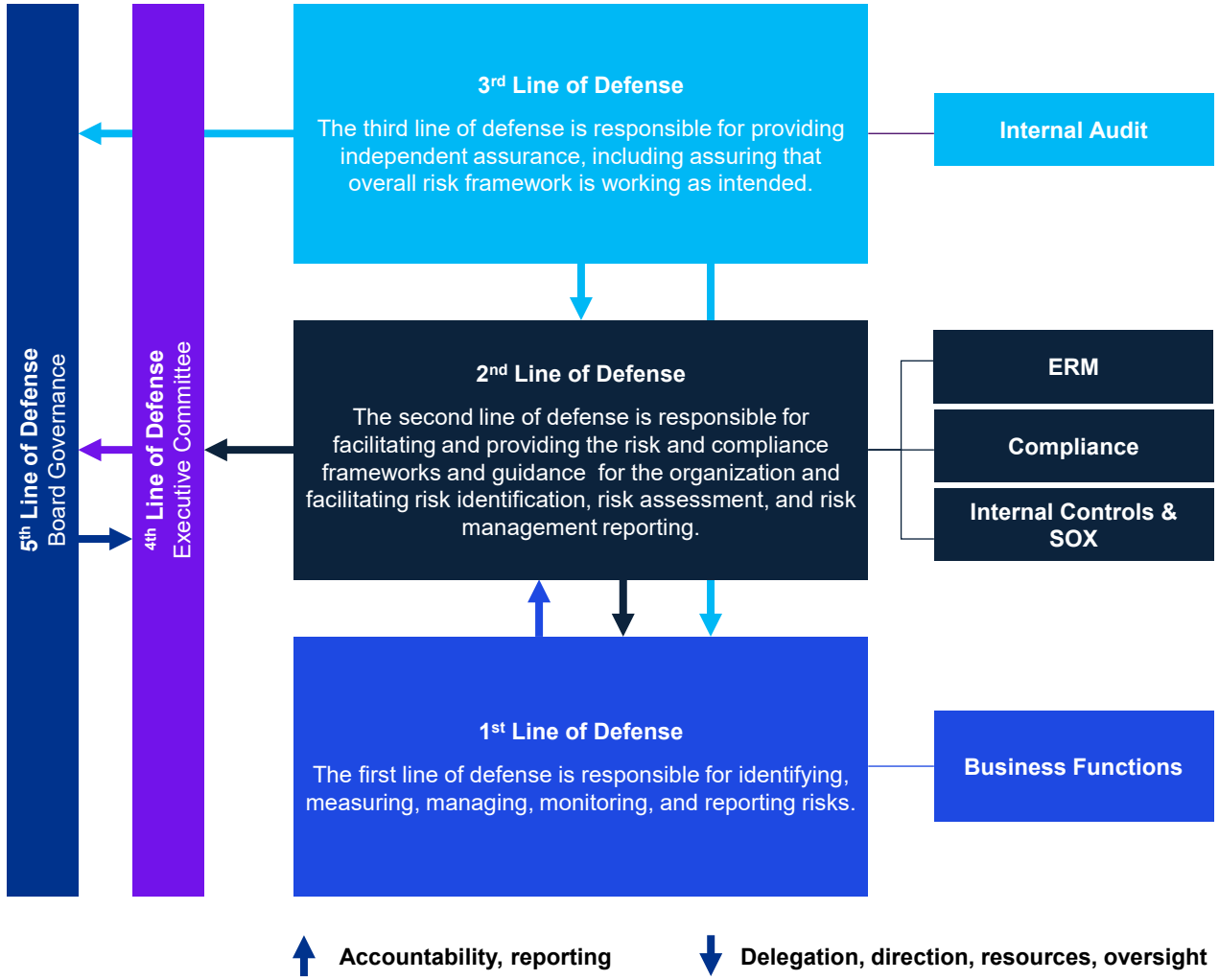
Path Forward: Risk governance and operating model considerations

How does ERM fit into the organization structure?

1st Line | 2nd Line | 3rd Line | 4th Line | 5th Line

ERM functions reside in the 2nd line of defense with Compliance. Internal Controls / SOX functions have varying “placements” within organizations but are still managing risk. An appropriately designed and placed ERM function will enable the following:

- Alignment between organizational structure and strategy within the three lines of defense
- Centralized compliance programs with integrated processes to eliminate redundancy cut across organizational boundaries
- Common and consolidated view of risk across the organization
- Support the value of a common technology and a “single source of truth” for risk and compliance data to facilitate improved transparency and information sharing

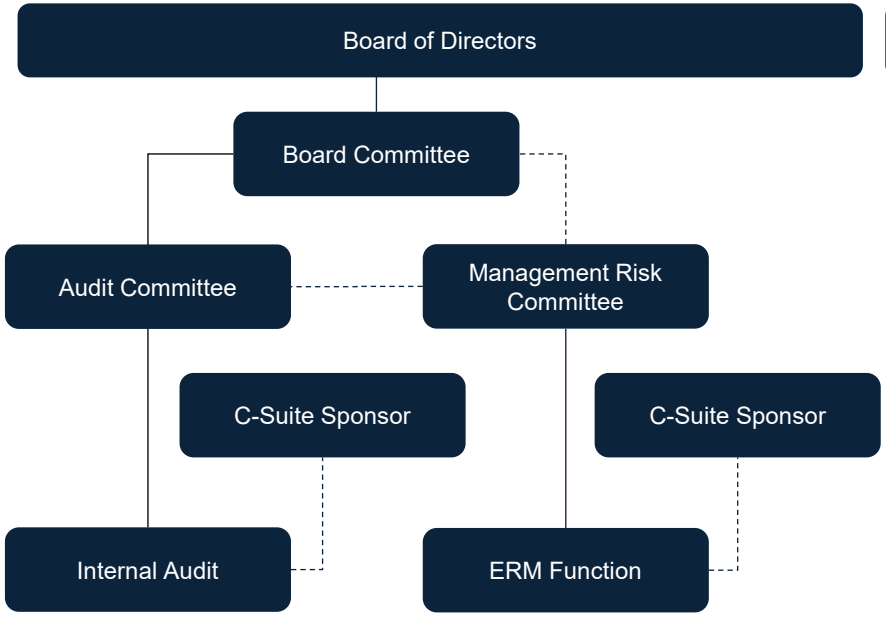


Example risk governance structures

Observed governance structures & reporting lines:

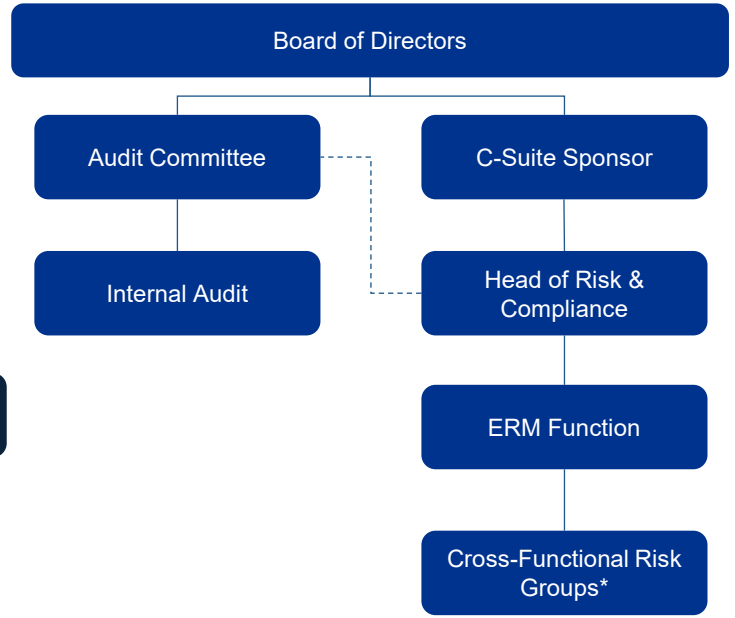
Reporting lines:

- The ERM Function and Internal Audit Department are separately overseen by a C-Suite Sponsor.
- The ERM Function reports to a Management Risk Committee, which reports to the Board.



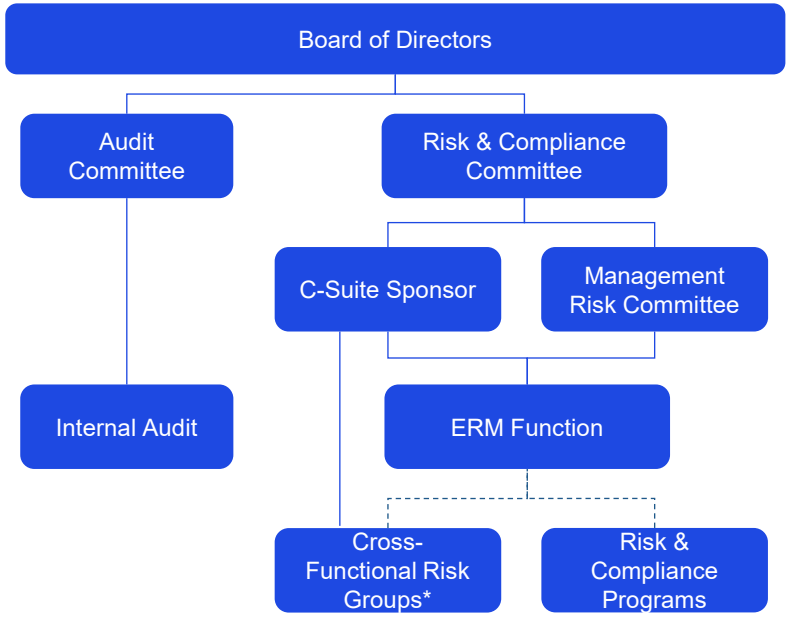
Reporting lines:

- The ERM Function consists of shared FTEs and reports to the C-Suite Sponsor.
- The Head of Risk & Compliance has a reporting line towards the designated C-suite Sponsor and a dotted line to the Audit (or Risk) Committee.
- Cross-Functional Risk Working Groups cover risks related to technology, people, operational, strategic, and legal and compliance risks.



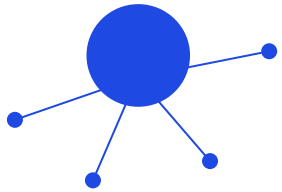
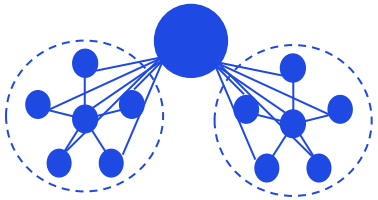
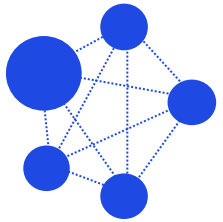
Reporting lines:

- The ERM Function reports to the C-Suite Sponsor and the Management Risk Committee.
- The Management Risk Committee receives input from other risk groups, programs, and committees, as appropriate.
- Reporting may be delivered to select committees or subcommittees of the Board or Management.



* Cross-functional risk groups may include multiple risk and compliance functions and capabilities (e.g., third party risk management, business resiliency / continuity, internal controls, data risk management, information security, privacy).

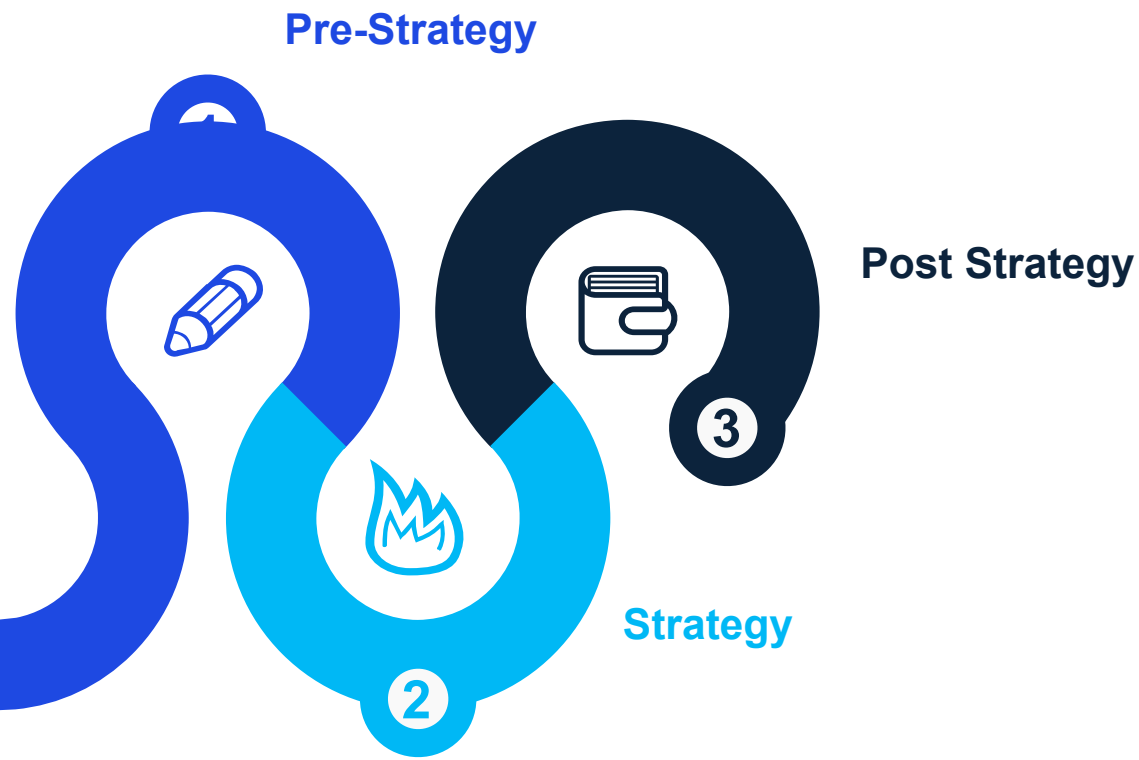
Operating model structures for managing risk

	Centralized (dedicated team)	As-A-Service (limited or partial team)	Decentralized (reliant on other risk functions)
			
Description	• The function is organized under an ERM leader supported by a core team while drawing on additional subject matter experts / risk owners • Responsibility for enterprise risk management is centrally managed	• The function is organized under an ERM leader supported by a limited team • ERM relies heavily on SMEs / risk owners • Creates accessibility to risk information with tools and methodology enabled by a limited, central team	• Responsibility for ERM is owned by multiple owners / business leaders • This option requires defined coordination and collaboration
Advantages	• Clear accountability, reporting lines and structure, including Board reporting • Enables faster pace of change and adoption • Reduces duplication of ERM-like activities • Can encourage cross-functional collaboration • Ability to support the business in a responsive manner	• Reporting lines and structure defined, including Board reporting • Facilitates sharing of skills and expertise • Ability to set company-wide standards with limited resources	• Specialized knowledge in different risk areas • Delegated responsibility to SMEs can increase speed to delivery when addressing specific risks
Disadvantages	• Commitment to investing in a team of dedicated resources • Requires change management	• Lines of authority and accountability less defined • Non-dedicated resources may reduce ability to advance ERM agenda due to reliance on other leaders • Requires change management	• Risk managed in silos • May reduce accountability as functions report to multiple authorities • May slow down decision making due to requirement for consensus • Separate departments may create conflicting agendas related to risk

KPMG

Path Forward: Risk to Strategy Linkage

ERM Within the Strategic Process Overview



Risk Assessment

- Identify Risks
- Apply Rating Criteria
- Prioritize Risks

Strategy Development

- Develop Assumptions
- Set Appetite / Risk Limits
- Identify Emerging Risks

Application

- Deep Dives
- Risk Mitigation
- Emerging Risks
- Risk Tolerance Metrics

Initiatives

- New
- Existing

Performance Initiatives

ERM Within the Strategic Process - Pre-Strategy

Defining Risk – The What, Why and Who?

The Enterprise Risk Assessment process is linked to ERM Strategy Development:

1. What are the short and long-term strategic objectives of the organization?

2. What are the potential roadblocks to meeting those objectives (i.e., threats/risks)?

3. What is the potential impact of those risks based on magnitude of impact and likelihood?

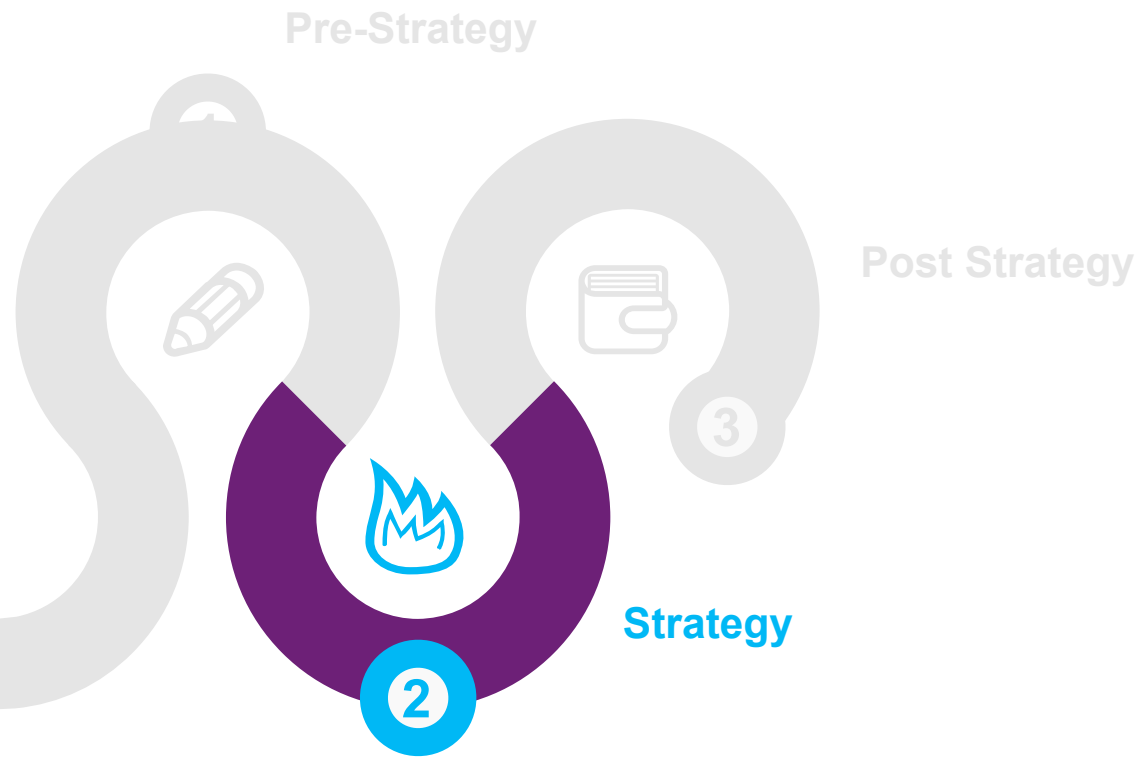
4. How well does the organization currently manage those risks?

5. Where do the biggest needs for improved risk management exist in terms of identified risks?

6. Who owns the prioritized risks (overall and day-to-day)?

ERM Within the Strategic Process – Strategy

Aligning ERM to Business Strategy



The ERM Strategy Development process reconciles the Enterprise Risk Assessment results to Business Strategy:

1. What assumptions should be layered onto identified risks that may affect strategic objectives (e.g., market conditions, competitive landscape, political and regulatory environment)?

2. What level of risk is the organization willing to absorb in order to achieve its strategy?

3. What level of risk impact would require a fundamental change in strategic direction?

4. What are the emerging risks on the horizon that should be continually monitored?

5. What is the potential for a “perfect storm” of multiple risks occurring at once?

ERM Within the Strategic Process - Post-Strategy

Embedding ERM in Strategy Execution

Business Strategy dissemination across the organization must also include an expectation for risk-aware business decision-making:

1. How are organizational strengths being leveraged and harnessed across business units/functions to share the wealth and reduce redundancies?

2. Is the process for escalating issues and key business risk decisions defined and being applied?

3. What reporting mechanisms are in place to monitor KRI/KPIs against the strategic roadmap?

4. How do existing initiatives align to strategy?

5. What new initiatives are being rolled-out to further promote strategy?

6. Are organizational incentives tied to strategic objectives and risk-aware decision making?

KPMG

ERM Journey – Enterprise Risk Assessment to Management and Monitoring

Journey to an Optimized ERM Program

Creating a mature and effective ERM program is an evolution. Our journey (as depicted below) balances meeting your key requirements and avoiding undue stress and cost ramifications, while achieving a scalable and optimized ERM program.

Phase 1 Program Foundations

Primary Objectives

- Build ERM foundational elements
- Define ERM Framework, Roadmap, and Policy
- Draft / update risk rating criteria
- Conduct strategic risk interviews
- Document risk inventory / risk listing
- Prioritize risks via enterprise risk assessment survey

Phase 2 Grow Presence

Primary Objectives

- Integrate ERM into strategy and business decisions
- Create risk profiles to further understand the risks identified including but not limited to:
  - Sub-risks
  - Risk mitigation activities
  - Risk Ownership
  - Risk Metrics
- Establish Management Risk Committee (MRC)

Phase 3 Mature Program

Primary Objectives

- Based on the risk profiles, identify metrics and create reporting dashboards
- Determine risk tolerances and begin reporting
- Define risk appetite statements
- Perform emerging risk analysis
- Establish ongoing monitoring via metrics reporting and trending
- Conduct 2-3 risk deep dives

Phase 4 Enhance Program

Primary Objectives

- Conduct risk Culture Survey
- Enhance your ERM toolkit to more forward-looking techniques
- Perform scenario analysis for disruptive risks
- Develop automated and interactive dashboarding and analytic capabilities

Phase 1: Program Foundations - Enterprise Risk Assessment

An enterprise risk assessment will provide a continuous focus on the risks that matter most and establish risk prioritization efforts enterprise-wide. KPMG has outlined our approach for effectively implementing our risk management leading practices below:

Planning & Interviews

- Review existing strategy and governance documents
- Launch project and conduct interviews with senior leadership to identify top risks that could impact your ability to achieve strategic objectives
- 6-10 interviews (30-45 minutes)

Risk Validation

- Leverage existing processes, procedures, and content, as well as information gather from interview to draft risk themes
- Present risk themes which emerged from interviews and validate risks
- Collectively select top ~15 risks

Survey & Analysis

- Distribute survey via Qualtrics to solicit SME views on:
  - Severity
  - Likelihood
  - Velocity
  - Mitigation Effectiveness (ERA)
  - *Optional: Connectivity (DRA)*
- Analyze collective results and create detailed report
- Expected commitment for senior leaders to complete the ERA assessment is ~45 minutes

Report Out

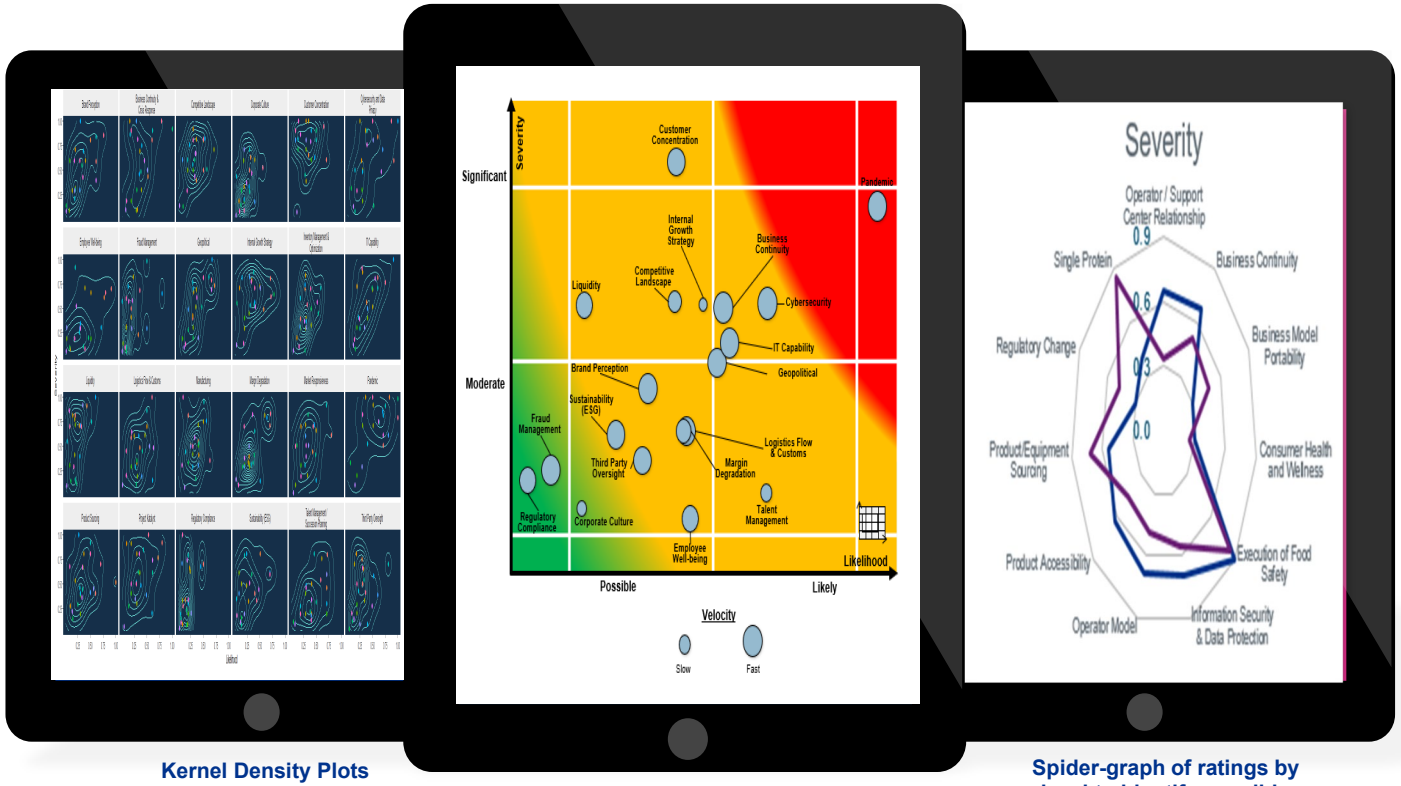
- Collectively review and evaluate the results
- Assign risk ownership
- Consider action plans to mitigate identified risks (focusing on root causes)
- 1 workshop with key stakeholders (1-2 hours)

Phase 1: Program Foundations - Enterprise Risk Assessment & Key Outputs

Organizational Benefits of an ERA:

- **Provides a consistent approach to risk prioritization**
- **Enables a collaborative method of brainstorming relevant risks, based on proven scientific methodologies**
- **Identifies the greatest systemic risk exposures to help inform a risk mitigation plan**
- **Encourages overarching consensus building to ensure results are broadly accepted among stakeholders**

Key Outputs



Kernel Density Plots demonstrating level of consensus among survey participants

Data-driven Top Risk Prioritization

Spider-graph of ratings by level to identify possible areas of disconnect

Phase 2 – Grow Presence

In order to grow the ERM presence across the organization, we suggest populating enterprise risk profiles. Profiles exhibit an organized summary of risk information that includes identified sub-risks (key risk areas), key mitigation activities, and metrics.

Risk Profiles... Refresh results can be leveraged to develop profiles to help establish a common understanding of risk ownership

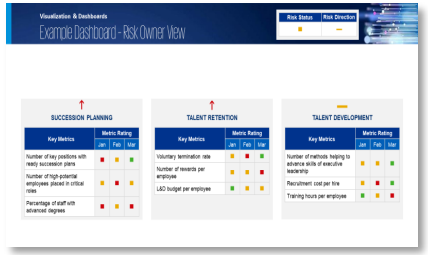
Risk Profile Benefits

- ✓ Provide meaningful, relevant and actionable recommendations to mitigate risk
- ✓ Basis for developing ongoing monitoring and mitigation plans
- ✓ Improve awareness of risk information and insights into potential risk drivers

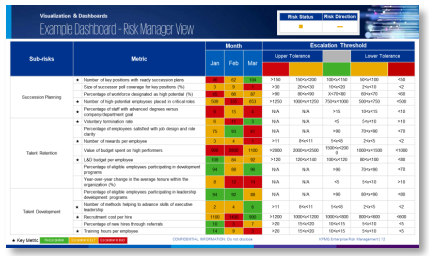
Phase 3 – Mature Program

After you have built out its ERM program foundations and grown presence, the company can begin to fully mature its risk management capabilities. Some additional ERM content that can be developed and implemented is included below:

Risk Metrics and Reporting

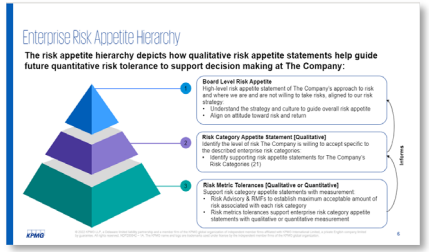


Individual Risk Dashboard



Executive Risk Dashboard

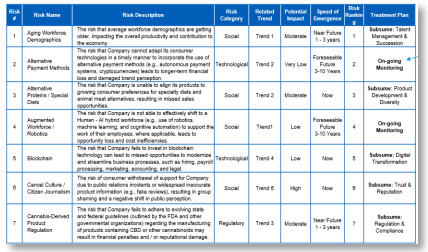
Risk Appetite



Risk Appetite Guidance

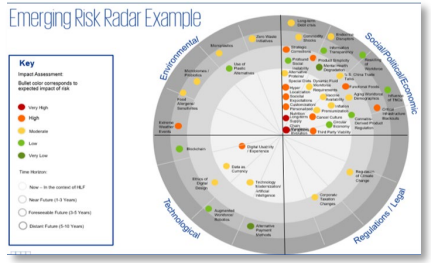
Risk Appetite Statements

Emerging Risk Analysis



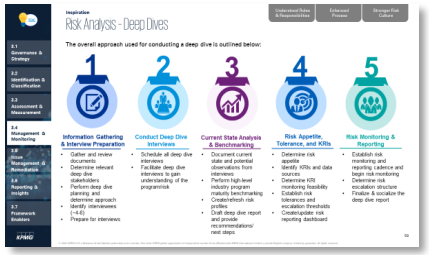
Risk #	Risk Name	Risk Description	Risk Category	Related Trend	Potential Impact	Speed of Emergence	Risk Number	Treatment Plan
1	Aging Workforce Demographics	The risk that average workforce demographics are getting older, impacting the overall productivity and contribution to the economy.	Social	Trend 1	Moderate	Near Future 1 - 3 years	1	Subsume: Talent Management & Succession
2	Alternative Payment Methods	The risk that Company cannot adapt its consumer technologies in a timely manner to incorporate the use of alternative payment methods (e.g., autonomous payment systems, cryptocurrencies) leads to longer-term financial loss and damaged brand perception.	Technological	Trend 2	Very Low	Foreseeable Future 3-10 Years	2	On-going Monitoring
3	Alternative Proteins / Special Diets	The risk that Company is unable to align its products to growing consumer preferences for specialty diets and animal meat alternatives, resulting in missed sales opportunities.	Social	Trend 2	Moderate	Now	3	Subsume: Product Development & Diversity
4	Augmented Workforce / Robotics	The risk that Company is not able to effectively shift to a Human - AI hybrid workforce (e.g., use of robotics, machine learning, and cognitive automation) to support the work of their employees, where applicable, leads to opportunity loss and cost inefficiencies.	Social	Trend1	Low	Foreseeable Future 3-10 Years	4	On-going Monitoring
5	Blockchain	The risk that Company fails to invest in blockchain technology can lead to missed opportunities to modernize and streamline business processes, such as hiring, payroll processing, marketing, accounting, and legal.	Technological	Trend 4	Low	Now	5	Subsume: Digital Transformation
6	Cancel Culture / Citizen Journalism	The risk of consumer withdrawal of support for Company due to public relations incidents or employees' responsible product information (e.g., fake reviews), resulting in group shaming and a negative shift in public perception.	Social	Trend 6	High	Now	6	Subsume: Trust & Reputation
7	Cannabis-Derived Product Regulation	The risk that Company fails to adhere to evolving state and federal guidelines (outlined by the FDA and other governmental organizations) regarding the manufacturing of products containing CBD or other cannabinoids may result in financial penalties and / or reputational damage.	Regulatory	Trend 3	Moderate	Near Future 1 - 3 years	7	Subsume: Regulation & Compliance

Emerging Risk Listing



Emerging Risk Report

Deep Dives



Deep Dive Report

Phase 4: Enhance Program – ERM Tools, Techniques, & Accelerators

Not all risks are created equal – and various ERM techniques may be applied to appropriately address the issue or opportunity at hand based upon varying degrees of uncertainty, time horizons, and levels of quantification to enable risk-informed decision making and a fit for purpose business solution.

Deep dives

Gathering in depth insights into strengths, vulnerabilities, and response strategies for top risks or corporate focus areas.

Wargaming

Tactical exercise to evaluate the results of various decision alternatives in relation to counterparty responses, e.g., contract negotiation.

Scenario analysis

Evaluating various alternative future scenarios and the impact on your strategy and business model.

Pre mortem

Imagine that a future product launch or market entry decision you undertake has failed – work backward beforehand to determine what could have led to the failure.

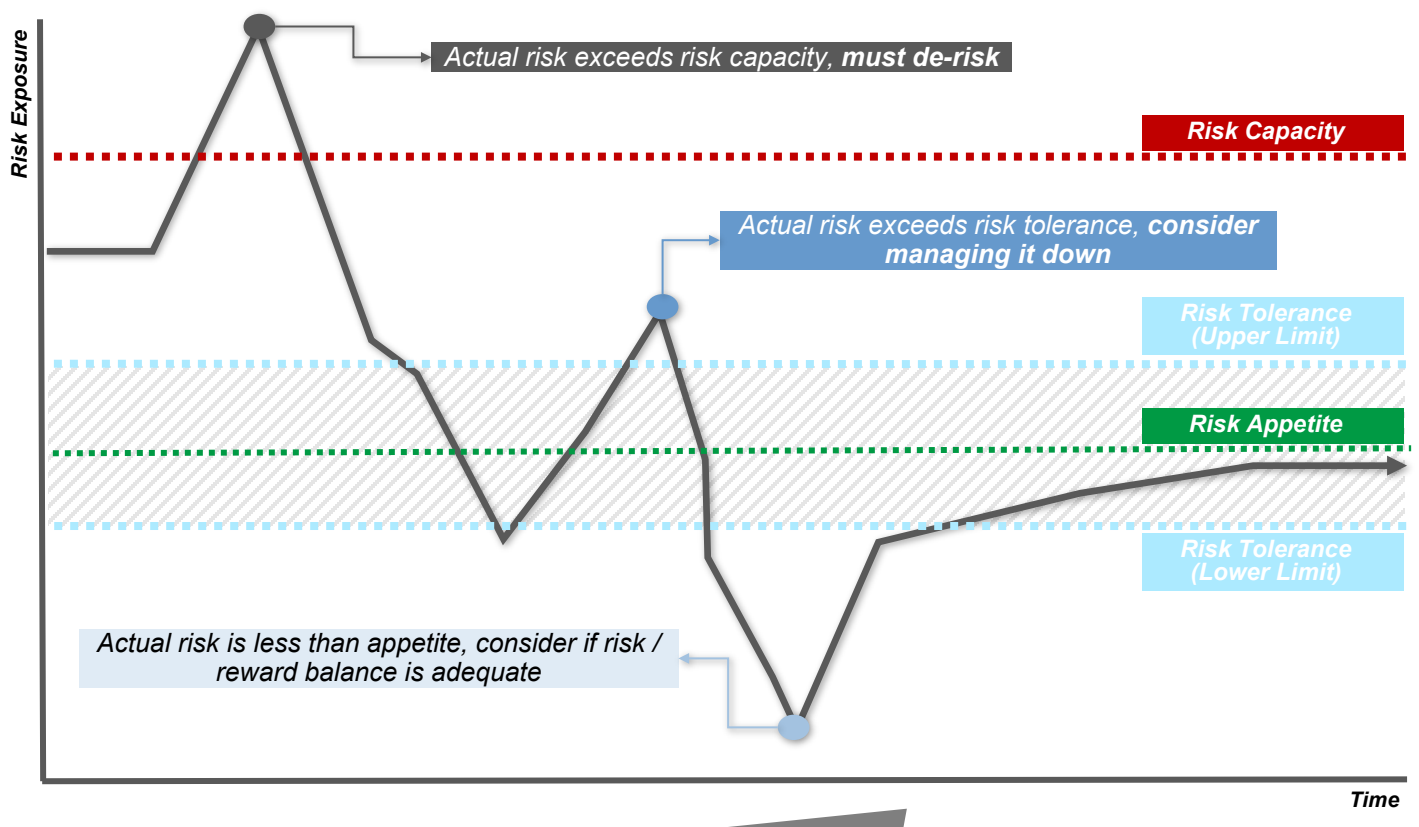
Phase 4: Enhance Program – ERM Tools, Techniques, & Accelerators

Deploying ERM techniques and solutions to support the business in understanding, evaluating, and acting upon real-time situations through a risk-informed lens can help drive value creation and enhance business performance.

ERM Solution	What it is	Where it can be used	Value to the Business
Scenario planning 	Business driven exercise intended to evaluate potential impacts and corresponding management response strategies for a defined set of situations.	• Strategic planning process • Partnering with the business • Annual or semi-annual strategy setting with management	• Promote open dialogue and consideration of risk and opportunities in decision-making • Proactive understanding and plan for uncertainties • Focus on value creation (“accelerate in straightaways”)
Pre mortem 	Strategic planning exercise that assumes a future-planned strategy has failed and examines potential reasons why, before it actually occurs.	• Technique deployed before strategy has been implemented • Annual workshops conducted with management and/or working groups	• Challenges business assumptions to consider what could threaten strategy, existence or business model • Combines business and risk inputs with management planning/decision making
Wargaming 	Business exercise that simulates the potential movements of customers, competitors or markets to help management proactively consider competitive strategies.	• ELT team members and working groups • Distinct exercise embedded within the strategic planning process	• Considers new and outside (i.e. competitor) perspectives • Converts disparate information (strategies, data, etc.) into business insights to help inform strategy
Deep dives 	In-depth exercise focused on a specific enterprise risk designed to comprehensively examine the contributing factors (root causes), potential impacts and existing strategies in place (including potential gaps).	• Select risks conducted annually • Facilitated by ERM, works with the business and risk ownership group	• Improves management awareness and seeks to address root causes • Supports enhanced monitoring and reporting • Developed action plans guide future improvements

Appendix: Risk Appetite

How Does Risk Appetite Work?



Risk capacity
Maximum level of risk the organization can assume given its current level of resources before breaching constraints

Risk tolerance
The maximum acceptable amount of risk associated with each risk-taking activity or risk category, e.g. operational risk KRIs, etc.

Risk appetite
The aggregate amount of risk a company is willing to accept relative to its resource capacity to assume losses, to align with and support its strategic and financial objectives

Plan and execute activities in gray "Risk Appetite zone" and avoid the breach of limits.
Once the organization breaches the Risk Capacity trigger, its resources may not be able to absorb any resulting losses.

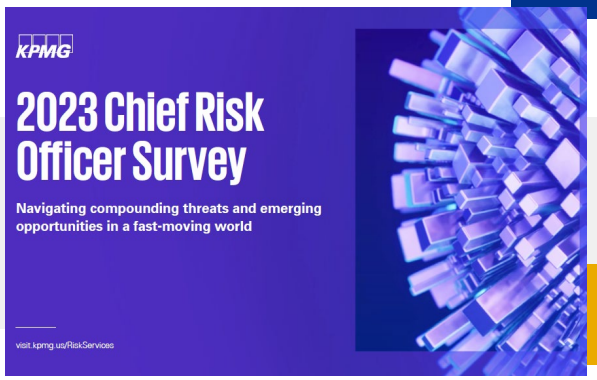
Risk Appetite Hierarchy

A step-by-step approach to establishing and maintaining a Board-level risk appetite, enterprise risk appetite statements, and supporting risk tolerance statements; operationalized through a comprehensive Enterprise Risk Management program.

Appendix: ERM Thought Leadership

Our ERM thought leadership

KPMG ha a proven track record in driving valuable business insights through Enterprise Risk Management.

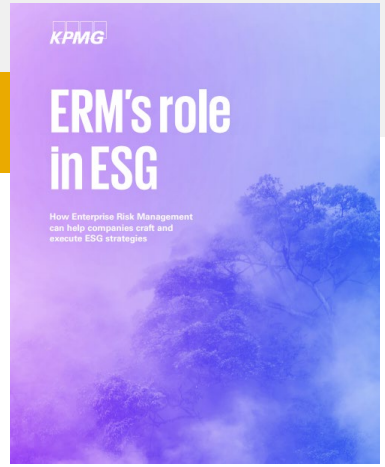


2023 Chief Risk Officer Survey

The KPMG 2023 CRO Survey draws on perspectives from 390 Chief Risk Officers (CROs) representing the largest companies across six industries.

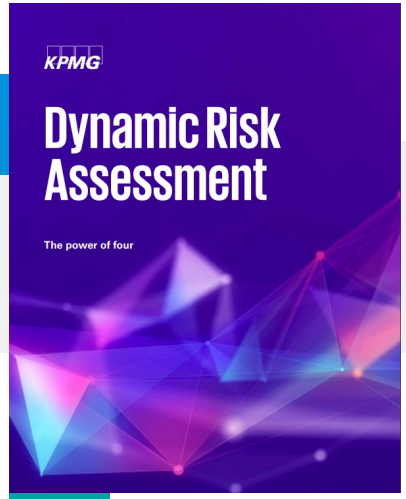
KPMG Risk Intelligence

Navigate complex risks with a comprehensive, automated solution for confident, informed decision-making.



ERM's Role in ESG

How Enterprise Risk Management can help companies craft and execute ESG strategies



Dynamic Risk Assessment

Dynamic Risk Assessment provides insights into risk that can enhance capital allocation, decision-making, resilience and agility.