MOODY'S

# Unified Risk Management

## The connected future of risk

moodys.com/maxsight

# Table of contents

**CHAPTERS**



SECTION 1

# Executive summary

As I reflect on the conversations and insights gathered for this report into unified risk management, what stands out is the candor of contributors and the scope and urgency today's risk landscape creates for them, their teams, and the global businesses they run.

Across the 50 interviews with C-suite leaders in risk, compliance, finance, and procurement, a clear message emerged: risk is not a series of isolated events, but a fast-moving, interconnected force that challenges assumptions about how organizations operate as a whole.

What struck me was the vividness with which contributors described the nature of risk, not as a theoretical construct, but as a lived reality. Leaders spoke of cyber incidents rippling through supply chains, operational failures triggering regulatory scrutiny, and reputational shocks that have the potential to upend markets. The old boundaries between risk domains appear to be dissolving; as one board director put it, "Risks don't respect our org charts anymore."

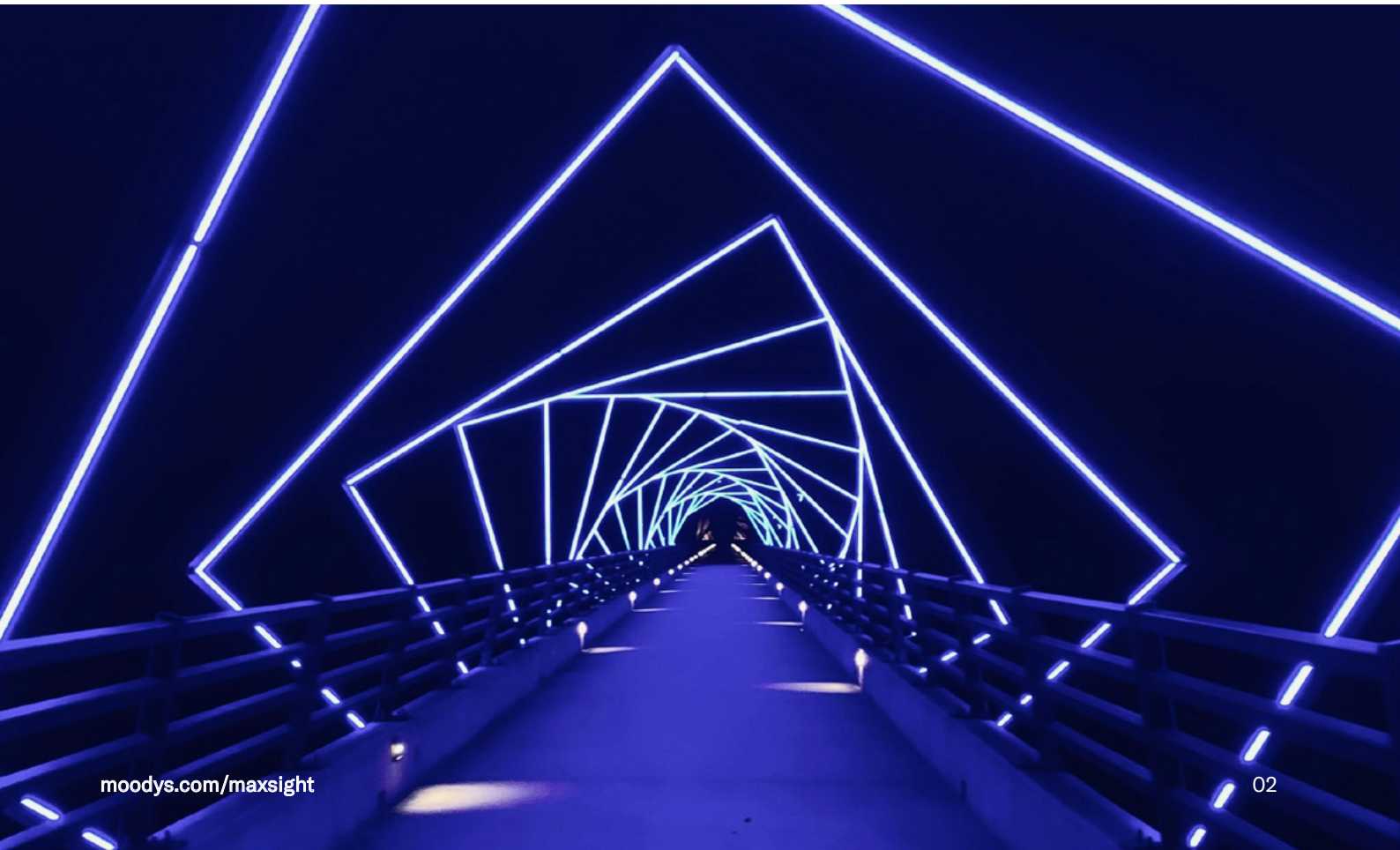
Yet, amid this complexity, I was inspired by the vanguard organizations who are redefining what 'good' looks like in risk management. These pioneers are treating risk as a strategic enabler, embedding it in boardroom discussions and leveraging data-driven approaches to anticipate and absorb shocks. Their stories reveal that unified risk management is not just an aspiration, but a new direction of travel for global organizations - one that asks for clarity, collaboration, and a willingness to rethink legacy systems.

Contributors were frank about their challenges: fragmented ownership, tool fatigue, and the struggle to turn data into actionable insight. But they also saw promise in a unified approach, recognizing its potential to create visibility and empower smarter decisions.

This report is shaped by the voices of those living and adapting to the changing nature of global risks each day. Their experiences and ambitions point to a future where agility, strategic engagement, and holistic oversight are the essentials to resilience and growth.

I would like to thank everyone who took the time to participate in this study.

**Keith Berry**
Head of Corporates and Government Solutions, Moody's



SECTION 2

# About the study

## Context and objectives

### A WORLD DEFINED BY COMPLEXITY AND INTERCONNECTION

Today's global businesses operate in an environment of heightened volatility and compounding risk. Economic uncertainty, digital acceleration, geopolitical disruption, and escalating regulatory expectations are converging to create an environment where risk events rarely occur or can be treated in isolation.

Technology has amplified both interdependence and exposure. Supply chains stretch across continents; data travels instantaneously, and operational resilience now determines competitive advantage. In this context, risk is changing too.

As organizations digitize core processes and adopt AI-driven tools, new forms of algorithmic, privacy, and reputational exposure have emerged. The lessons of **'Moody's From reactive to proactive: How AI is transforming risk and compliance study'** are relevant here. Leaders are no longer asking whether technology introduces risk; they are asking how to govern it holistically, to support innovation, integrity, and resilience in each step.

### PURPOSE OF THIS RESEARCH

Against this backdrop, Moody's initiated the Unified Risk Management (URM) study to understand how global businesses are evolving their approach to risk.

The study explores:

- → How leaders perceive and prioritize risk in an era of exponential connections.
- → What 'good' looks like in risk management today, including how data, culture, and governance interact to drive resilience.
- → How the concept of URM, an integrated and organization-wide approach to risk, can help businesses move from fragmented control to unified insight.

### METHOD

The findings in this report draw on 50 in-depth qualitative interviews with senior executives responsible for risk, compliance, finance, procurement, and operations across three regions: EMEA, Americas, and APAC.

Each 45- to 60-minute interview was conducted under confidentiality and analyzed thematically to surface both shared challenges and regional nuances.

Participants represented a broad mix of industries and maturity levels, so the research could capture the diversity of real-world experiences. The sample included financial institutions with sophisticated risk infrastructures, as well as corporates and professional services firms managing complex, human-driven exposures.

## SAMPLE COMPOSITION

| Region | |
|---|---|
| Europe, the Middle East, and Africa | 21 |
| Americas | 21 |
| Asia-Pacific | 8 |

| Subsector | |
|---|---|
| Corporates | 15 |
| Professional services | 12 |
| Fintech | 8 |
| Banking | 7 |
| Insurance | 4 |
| Wealth and asset management | 4 |

| Business size | |
|---|---|
| 0-99 | 2 |
| 100-499 | 6 |
| 500-999 | 8 |
| 1,000-4,999 | 11 |
| 5,000-9,999 | 9 |
| 10,000+ | 14 |

| Role | |
|---|---|
| Risk, compliance & regulatory | 19 |
| Technology & data | 6 |
| Procurement & supply chain | 6 |
| Executive leadership | 5 |
| Finance | 5 |
| Commercial & revenue | 5 |
| Operations | 2 |
| Consulting / fractional leadership | 2 |

## ANALYTICAL APPROACH

Interviews were transcribed and coded to identify recurring themes, tensions, and differences across cohorts.

The findings were then synthesized into a framework that maps how risk perceptions, practices, and priorities are shifting, and where unified risk management offers the most strategic value.

Throughout the report, direct quotations from participants bring these findings to life, illustrating both the challenges of legacy approaches and the promise of a unified model.

SECTION 3

# The changing state of risk

## A new playing field

### A RISK LANDSCAPE TRANSFORMED

Global risk has entered a new phase of speed, interdependence, and unpredictability.

The conversations in this study highlight that risk today is no longer a collection of discrete events. It is a web of interlinked forces that can amplify one another in unexpected ways. A cyber incident can trigger supply chain disruption, regulatory intervention, and reputational fallout within days. Economic volatility and geopolitical shifts can ripple through financial markets and consumer trust in equal measure.

### THE PACE OF CHANGE AND ITS IMPLICATIONS

The majority of organizations in this study described their exposure to risk as **accelerating**.

## 46/50 said that Cyber Risk has grown in the recent years.

Indications from participants are that digital dependency has outpaced digital control; organizations have migrated critical operations, data, and decision systems into cloud environments and third-party platforms faster than their governance frameworks have adapted. And the expansion of hybrid-work and connected supply chains have multiplied potential entry points for attack.

At the same time, the threat landscape has become more sophisticated, with cyber incidents now intersecting with factors like fraud, data privacy, and geopolitical tensions.

For many, the challenge is not awareness but capacity: they have more data on threats than ever, yet fewer coordinated mechanisms to detect, prevent, and recover at speed.

**"The barrier to entry for malicious cyber threats has really decreased in the last few years, they are extremely prolific now in a way they weren't previously."**

**Lead Director of Third-Party Security & Risk Management, Americas, Major Healthcare brand**

## 41/50 said that Third-party/Operational Risk has grown in recent years.

Third-party and operational risk have also grown as organizations have become more dependent on — and responsible for — extended, multi-tiered networks of suppliers and partners.

Digital transformation has multiplied the number of external interfaces and service providers on which business continuity depends. This complexity can create new points of failure: a single vendor outage can disrupt operations, breach compliance rules, or expose data across multiple regions.

Many described a widening gap between how much operational activity sits outside their direct control and how limited their oversight remains.

**"Operational risk has taken on a whole new dimension because of how connected everything is. A disruption in one vendor, one data center, one logistics partner, and it cascades instantly. You can't separate operations from third-party anymore, they're the same ecosystem."**

**COO, Americas, Financial Institution**

This acceleration has shifted risk from being a compliance issue to a **strategic business challenge.** Risk teams are now expected to anticipate disruptions, not just respond to them. Yet most organizations acknowledged that their systems, data, and governance structures were not designed for this level of complexity.

## FROM SILOS TO SYSTEMS

What emerges is a consistent tension between the **interconnected nature of modern risk and the fragmented way in which it continues to be managed.**

Across industries, we found that risk functions remain divided between IT, compliance, finance, procurement, and operations. Data is siloed, processes can be inconsistent, and accountability diffuses. This often results in a growing "execution gap" between recognizing that risk is interconnected and being able to act on that insight.

> **"We know what the future looks like, but we're still operating like it's 2005. Everyone owns a piece of risk, but no one owns the whole."**
>
> **Chief Risk Officer, EMEA, Global Bank**

## A TURNING POINT FOR BUSINESS RESILIENCE

The changing state of risk has created both urgency and opportunity for organizations. Across every sector, leaders describe an environment where risk feels faster, broader, and harder to contain. The escalation of cyber and third-party threats has exposed the limits of current systems, and the speed of change has left even the most advanced organizations struggling to keep up.

This moment presents an **urgent inflection point**. The growing web of interconnected risk types and events is forcing organizations to confront a difficult reality: existing frameworks, processes, and hierarchies were not built for the world they now operate in. The challenge is not a lack of awareness, but a lack of coherence.

Yet, within that tension lies opportunity. As risk becomes more integrated into strategic decision-making, organizations have the chance to redefine how resilience is built. Those who can connect data, people, and governance into a single, transparent view of risk will not only manage volatility more effectively but also find new sources of trust and competitive advantage.

This is where the next chapter begins — with understanding how risk thinking diverges across industries, and what it might take to move toward a more connected future.

SECTION 4

# Diverging risk worlds

## The path forward

### RISK MATURITY DEPENDS ON WHERE YOU SIT

Although all organizations spoken to face accelerating, interconnected risks, their experience of risk was shaped by what they do, where they operate, and how they are regulated.

The study revealed five key drivers that determine risk maturity:
**1) Scale and complexity**
**2) Regulatory intensity**
**3) Digital dependency**
**4) Geographic reach**
**5) Sector culture**

These create a fragmented landscape in which the sophistication of risk management can vary widely.

### Drivers of difference

| | | |
|---|---|---|
| **Financial services** Systemic, model-based, credit/market focussed | SECTOR FOCUS | **Corporate & professional services** Supply-chain, reputation focussed |
| **Local / regional** Manageable, fewer third parties | SCALE & COMPLEXITY | **Global / multinational** Sprawling vendor based, higher exposure |
| **Lightly regulated** Agile but inconsistent | REGULATORY INTENSITY | **Heavily regulated** Disciplined but rigid |
| **Manual / fragmented systems** Reactive, siloed | DIGITAL & DATA MATURITY | **Automated / integrated system** Data-driven, predictive |
| **Compliance-owned** Risk as a policing function | LEADERSHIP CULTURE | **C-suite sponsored** Risk seen as a strategic enabler |

Together, these drivers create a spectrum of risk maturity, from highly regulated and data-driven to relational and adaptive.

### FINANCIAL VS NON-FINANCIAL INSTITUTIONS

Financial institutions are grounded in decades of formal risk infrastructure, (frameworks, appetite statements, and regulatory oversight), but many of the ones we spoke to appear to struggle to connect financial and non-financial domains such as cyber, sustainability, and operations.

Corporates and professional-services firms, by contrast, tend to have lighter formal frameworks yet clearer visibility into day-to-day vulnerabilities. Both recognize that integration is the missing piece needed to achieve greater resilience and agility.

**SUBSECTOR NUANCES**

## Banking

Mature in financial risk management but constrained by regulation and legacy systems.

**Tension:** Sophistication without agility. Banks struggle to connect speed and control.

## Wealth & asset management

Broadening the lens from market exposure to enterprise risk including sustainability, data, and reputation.

**Tension:** Rising investor expectations for transparency create pressure to demonstrate integrity and control.

## Insurance

Rich in data but fragmented across underwriting, actuarial, and enterprise functions.

**Tension:** Abundance of information without integration limits efficiency and resilience.

## Fintech

Fast-moving and innovation-led, with governance that often lags growth.

**Tension:** Agility continually outpaces assurance and oversight.

## Corporate

Wide operational and reputational exposure from complex supply chains and sustainability scrutiny.

**Tension:** Global visibility desired, but accountability remains fragmented and reactive.

## Professional services

People- and reputation-driven, reliant on judgment and trust rather than formal systems.

**Tension:** Inconsistency and informality make risk hard to standardize across networks.

> **"We've got some of the most advanced models in the world for credit and capital, but we still run some of our core processes on legacy systems that can't talk to each other. We can measure risk to four decimal places but still can't get a single real-time view."**
>
> **Chief Risk Officer, EMEA, Global Bank**

## REGIONAL NUANCES

While the core risk challenges are shared globally, each region brings its own emphasis and operating realities. Market context can subtly shape how these risks are experienced and prioritized; differences in regulatory focus, supply chain exposure, and pace of digitalization that influence how organizations approach risk management.

### Americas

More focused on agility amid policy shifts, sanctions, and supply chain volatility; faster decision cycles but often fewer formal frameworks.

### EMEA

Leans toward regulatory harmonization and data transparency; supplier oversight and auditability are ongoing priorities.

### APAC

Balances rapid digital growth with multi-country supply chain complexity and diverse data-privacy regimes.

> **"Every few months it feels like the rules change — new tariffs, new sanctions, new restrictions. You plan a quarter ahead and suddenly the whole supplier map is obsolete."**
>
> **VP Procurement, Americas, Corporate**

> **"We spend half our time reconciling what the EU wants versus what the UK now requires."**
>
> **Head of Compliance, EMEA, Financial Services**

> **"In APAC you're managing ten versions of digitalization at once - from advanced AI to paper forms - and ten different sets of rules about what you can do with the data."**
>
> **Regional Director of Risk, APAC, Professional Services**

These contrasts underscore a central truth: **resilience can look different depending on context,** but integration is the common frontier. Regardless of sector, leaders agree that managing risk in isolation can weaken a business. The challenge now is not identifying risks, but connecting them into one coherent picture of exposure, performance, and opportunity.

SECTION 5

# The vanguards of risk management

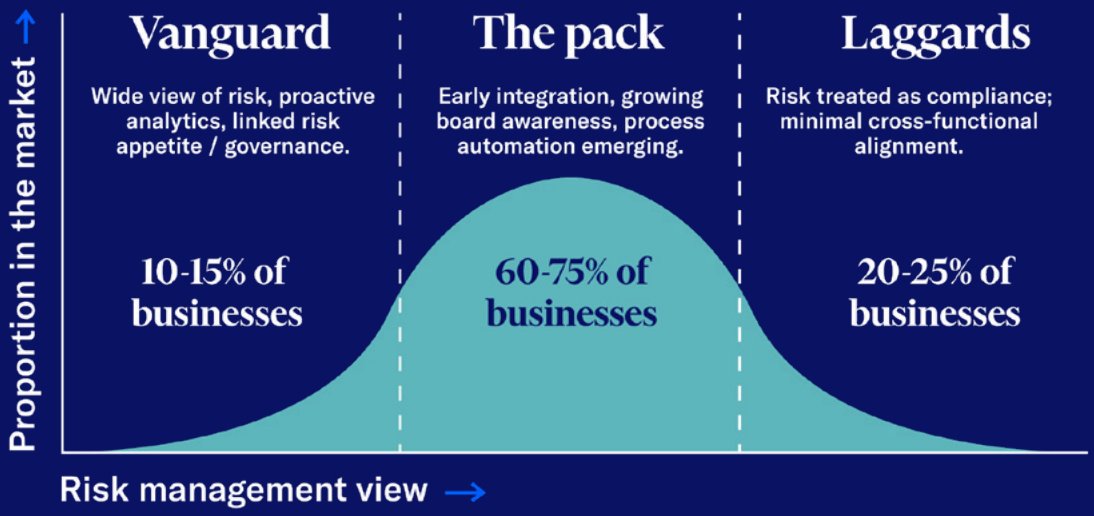
## The mature risk management framework

### RISK MATURITY DEPENDS ON WHERE YOU SIT

Across these differences, a small cohort are redefining what 'good' can look like.

Organizations sit along a clear maturity curve, from fragmented and reactive risk management to unified and strategic.

Some still manage risk through siloed spreadsheets and post-incident reviews; others are building integrated, data-enabled frameworks. The majority sit in the middle: aware of the need to unify, but unsure how to operationalize it.




### VANGUARDS

Amid the complexity and fragmentation described in earlier sections, a smaller group of organizations is moving differently. These are the vanguards: leaders who no longer view risk as a compliance burden, but as a strategic capability that underpins performance, trust, and resilience.

Where most organizations still manage risk within functional silos, vanguards are breaking those boundaries. They are replacing fragmented processes with shared frameworks, treating risk data as a business asset, and embedding risk insight directly into operational decision-making.

> **"We've reached a point where every material risk is visible in one framework. Financial, cyber, operational, reputation - they're all linked, and we can model how one shock plays through the rest of the system. It's not perfect, but it's a living, breathing view of the enterprise."**
>
> **Chief Risk Officer, EMEA, Financial Services**

## FROM RISK MANAGEMENT TO RISK INTELLIGENCE

What defines these vanguards is not simply better controls or stronger governance. It is their ability to translate complexity into foresight. The focus is less on static frameworks and more on creating **risk intelligence** — the ability to anticipate disruption, absorb shocks, and adapt quickly.

Their approach blends three qualities that set them apart:

### 1. Connected data.

They integrate data across systems, partners, and geographies, creating visibility that supports faster, coordinated responses.

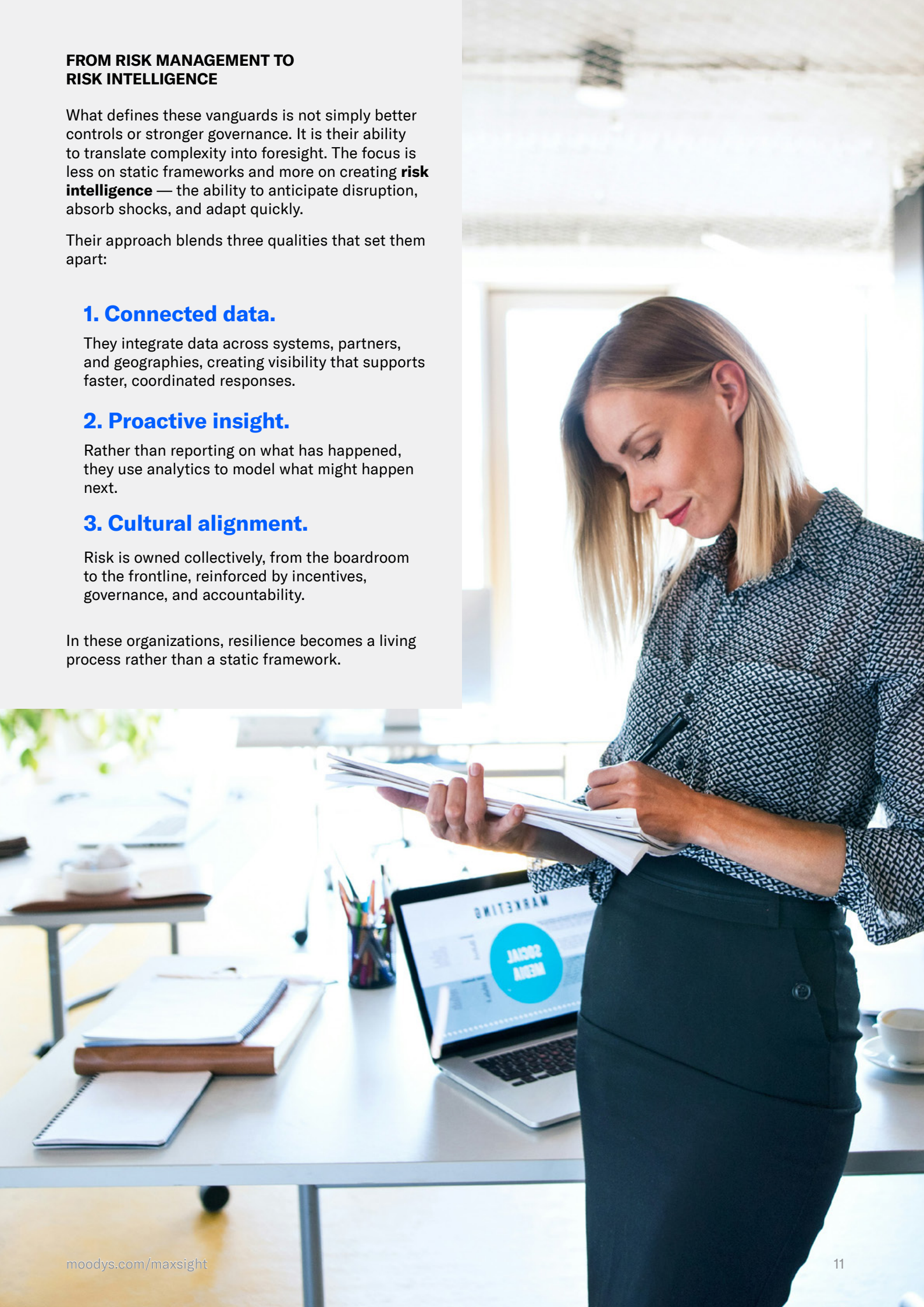
### 2. Proactive insight.

Rather than reporting on what has happened, they use analytics to model what might happen next.

### 3. Cultural alignment.

Risk is owned collectively, from the boardroom to the frontline, reinforced by incentives, governance, and accountability.

In these organizations, resilience becomes a living process rather than a static framework.



# Five defining shifts

Across interviews, five mindset shifts distinguish the vanguard group from the mainstream:

| | | |
|---|---|---|
| Isolated → | Interconnected | The vanguards are building cross-domain visibility; others still manage in silos. |
| Defensive → | Strategic | Advanced firms treat risk as a lever for growth; others still see it as protection. |
| Compliance → | Resilience | Leaders focus on agility and recovery; others remain checklist-driven. |
| Manual → | Data-driven | Pioneers automate and integrate; most still rely on spreadsheets. |
| Tactical → | Boardroom level | Risk is now a leadership language for the most mature; others are just beginning to elevate it. |

## 1. From isolated to interconnected risk management

They recognize that financial, operational, and reputational risks aren't best when separated. Their structures and tools are built to connect insights across a business.

## 2. From defensive to strategic

Risk is treated as a source of value and differentiation, not just protection. It informs investment decisions, innovation, and customer trust.

## 3. From compliance to resilience

Controls are still essential, but the emphasis has moved toward adaptability, preparedness, and continuity under pressure.

## 4. From manual to data-driven

Technology underpins their advantage. Automation, AI, and integrated analytics turn risk monitoring into a dynamic capability.

## 5. From tactical to cultural

Risk awareness extends beyond risk teams to become part of everyday leadership and decision-making.

Each of these shifts requires more than new technology. It requires a different mindset, one that treats risk as a shared strategic language across the organization.

**WHY THIS MATTERS**

The vanguards show what is possible when risk is unified, digitized, and embedded in leadership thinking. They are not immune to disruption, but they are positioned to respond and recover faster.

Their example also sets out a challenge for the rest of the market: to move from managing risk in isolation to managing it as a system.

For many, that would mean confronting long-standing barriers in structure, culture, and technology. But the alternative is falling behind in a world where operational resilience defines competitiveness.

**"Risk isn't a department anymore. It's part of every strategic conversation — product launches, partnerships, even hiring. We don't talk about 'owning' risk; we talk about how we manage it together."**

**Head of Risk and Compliance, Americas, Multinational Consulting and Advisory Firm**

SECTION 6

# The new league table of risk

## Managing interconnected risks

### RETHINKING THE HIERARCHY OF RISK

The study shows that risk priorities have shifted from what is most visible to what is hardest to manage. Leaders now evaluate exposure by two criteria: **1) impact on the business and 2) ease of management.**

This view creates a new "league table" of risk, in which the most severe risks are not always the newest or the biggest, but the ones least within organizational control.

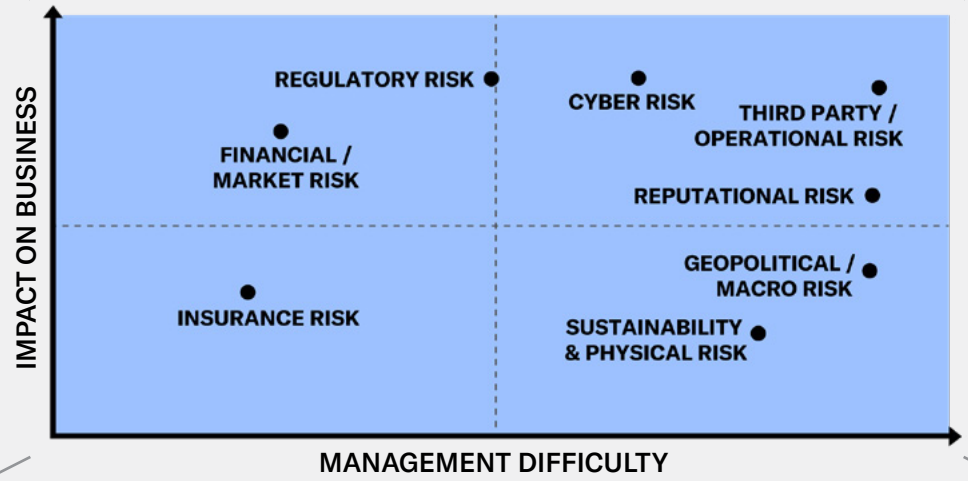
When mapped by **impact on business** (low → high) and **management difficulty** (low → high), four distinct groups of risk emerge.

## Risk types

### BY IMPACT AND DIFFICULTY OF MANAGEMENT

**Structured core**
While their direct day-to-day impact may be limited, these risks require ongoing monitoring, scenario planning, and contingency modelling to mitigate external shocks.

**Hard-to-manage criticals**
Risks that feel most unpredictable and uncontrollable: fast-moving, cross-functional, and often externally triggered.




**Weakly governed emerging**
Long-established frameworks, regulatory oversight, and embedded governance make these risks predictable, modelled, and well-understood.

**Mature and managed**
Their frameworks are often mature but static - important when needed but rarely seen as a source of transformation or competitive advantage.

## Cyber risk

Sitting at the heart of the “Hard-to-manage/ criticals” quadrant.

Cyber combines the highest perceived impact with some of the lowest perceived controllability. Leaders described a dichotomy between defensive capability and threat sophistication, where resilience now depends on speed and cross-functional response.

> “We have more monitoring tools than ever, but the speed of attacks has overtaken our ability to respond.”
>
> Chief Information Security Officer, North America, Global Bank

## Third-Party / operational risk

Risks which have become existential concerns, amplified by complex supply chains and digital dependencies.

Executives spoke of visibility gaps across vendors and partners, and of risk being “inherited” from outside the organizational perimeter.

> “We can audit suppliers, but we can’t manage them daily. Our risk surface is only as strong as their weakest link.”
>
> Chief Procurement Officer, EMEA, Multinational Corporate

## Financial risk (credit, market, liquidity)

Risks which remain among the most mature and systematized.

They are the foundation of traditional risk management, supported by deep modelling and regulatory oversight. Leaders see them as high impact but also highly manageable. Well-defined, measurable, and integrated into reporting.

> “We’re good at measuring financial risk, but less good at seeing what’s around it.”
>
> Chief Risk Officer, Americas, Global Bank

## Regulatory / compliance risk

Sit firmly in the “Structured core”.

These are stable yet dynamic, shaped by continual changes in reporting standards and oversight. While control mechanisms are robust, executives acknowledged that compliance demands can consume resources that could otherwise be applied to proactive risk insight.

> “We have plenty of controls, but not enough coordination.”
>
> Head of Compliance, EMEA, Professional Services Firm

## Reputational risk

The amplifier of all other risks.

Reputational risk  is often triggered indirectly by failures in cyber, third-party, or compliance domains. Leaders see their brand reputation as both fragile and intangible — difficult to quantify, yet decisive in market and stakeholder confidence.

> “You don’t need to be wrong to lose trust; you just need to be slow to respond.”
>
> Chief Communications Officer, EMEA, Financial Institution

## Geopolitical / macroeconomic

Risks which exemplify the Mature and managed quadrant: difficult to manage, yet not always directly operational.

Their unpredictability and scale make them reliant on foresight and agility rather than direct control. Scenario modelling, diversification, and resilience planning are the primary levers.

> **"You can't control trade wars or elections, but you have to plan as if they'll hit tomorrow."**
>
> **Head of Strategy, APAC, Global Corporate**

## Sustainability / physical risk

Challenging to manage, spanning regulation, investor pressure, and reputation.

While the immediate operational impact may be limited, the long-term implications are strategic. Companies are investing in data transparency, emissions reporting, and governance reform, but maturity varies widely among the cohort we spoke to.

> **"The intent is there, but the metrics aren't yet catching up."**
>
> **Sustainability Director, APAC, Global Corporate**

### A SHIFT IN THE CENTER OF GRAVITY

Across markets and sectors, there is a clear transition: the central risk concern is no longer liquidity or credit but continuity.

Cyber, supply-chain, and system disruptions are now what keep executives awake at night.

Financial stability remains essential, but it's seen as the outcome of resilient operations, not the foundation.

While each of these risks presents challenges in their own right, what emerged most strongly was that it is the co-existence of these diverse risk types, and their increasingly interconnected nature that is most impactful, and amplifies the overall scale of the challenge.

### EXPONENTIAL RISK: MAKING SENSE OF INTERCONNECTED THREATS

Exponential risk is a term Moody's used to describe a shift in the nature of global risk.

Threats are no longer isolated or linear but are deeply interconnected, compounding, and cascading.

In this era, risks like geopolitical tensions, cyberattacks, weather events, and supply chain disruptions interact and amplify one another — often triggering domino effects that span industries, geographies, and sectors.

### WHY DOES IT MATTER?

The concept of exponential risk is not just a diagnostic; it is a learning tool.

It gives leaders a vocabulary to describe the reality they already face: the collapse of boundaries between financial, operational, and non-financial domains.

Cyber, supply chain, sustainability, and reputational risks move in concert, creating ripple effects that test resilience across every layer of a business.

By framing this dynamic, organizations can begin to move from reaction to readiness. Understanding exponential risk helps shift focus from the probability of single risk events to the interdependencies that magnify impact.

> **"This finally gives language to what we experience daily - the domino effect when one weak link fails."**
>
> **Head of Operational Resilience, APAC, Financial Institution**

SECTION 7

# Practical challenges in modern risk management

## The factors holding businesses back

### THE EXECUTION GAP

The growing complexity of risk management was well understood by leaders interviewed for this study but translating that awareness into coordinated action highlighted a gap.

Across industries and regions, organizations described the same underlying problem: they know what needs to change but cannot always execute at the required speed or scale.

This "execution gap" is widening as risks become faster, more interconnected, and more dependent on the latest data. Four categories of challenge emerged repeatedly from the study.

## 1. Data and technology challenges:

**36/50 cited this as a key challenge**

### VOLUME WITHOUT INTEGRATION

Data is abundant, but connectivity to create insight can remain elusive.

Risk information is often scattered across systems that do not talk to one another, leaving teams dependent on manual reconciliation and retrospective analysis.

Excel and PowerPoint still dominated board reporting, despite widespread investment in risk platforms.

> **"We've got more data than ever, but none of it talks to each other. By the time we've stitched it together, the risk has already moved on."**
>
> **Head of Data and Analytics, Americas, Global Manufacturing Firm**

Leaders described tool fatigue — too many point solutions solving isolated problems but not building a coherent picture.

This lack of orchestration appears to prevent organizations from transforming data into dynamic, actionable intelligence.

## 2. Capability and execution challenges:

**34/50 cited this as a key challenge**

**Systems don't match the speed of change,** even where structures and data exist, execution can lag behind ambition.

Many organizations struggled to move from analysis to action, citing integration fatigue and the operational burden of past transformation projects.

Predictive capabilities remain rare, and most businesses were still focused on reporting after events occur.

> **"We talk about foresight, but most days we're firefighting. The ambition's there; the systems and speed just aren't."**
>
> **Chief Operating Officer, APAC, Regional Financial Institution**

The result is a widening gap between aspiration and ability. The leaders who felt most confident of success were those who focused on agility, investing in people and processes that make risk intelligence usable, not just on systems.

## 3. Cultural and behavioral challenges:

# 31/50 cited this as a key challenge

### RISK AS COMPLIANCE, NOT STRATEGY

For many, the greatest barrier is not technical but cultural.

Risk is still viewed as a compliance function rather than a source of strategic insight.

This can limit engagement outside traditional risk and audit teams and foster a reactive mindset that prioritizes control over adaptability.

> **"We've built all the governance in the world, but people still see risk as someone else's job."**
>
> **Director of Risk Culture, EMEA, Professional Services Firm**

Governance frameworks exist, but they often overwhelm rather than empower.

When a culture lacks shared accountability and risk literacy, processes remain rule-bound and slow to adapt.

## 4. Structural challenges:

# 29/50 cited this as a key challenge

### FRAGMENTATION AND MISALIGNED OWNERSHIP

Many organizations still managed risk through functional silos rather than integrated frameworks

Ownership was often divided between IT, procurement, compliance, and finance, each using different taxonomies, systems, and reporting methods.

This fragmentation highlighted risk of duplication, slow escalation, and limited business-wide visibility.

> **"Everyone's got their own risk framework - IT, finance, procurement - but no one's connecting the dots."**
>
> **Chief Risk Officer, EMEA, Global Bank**

The absence of a single, holistic view meant leaders were left managing "pockets" of risk, without a consistent sense of how they interact or accumulate.

### THE BIGGER PICTURE

Across all four dimensions, one theme stands out: risk management has outgrown its old architecture.

Legacy systems, functional boundaries, and cultural habits built for a slower, more predictable world appear to be constraining progress.

The opportunity is not just to modernize but to unify, bringing structure, data, behavior, and execution into a shared operating model.

This is where **Unified Risk Management** (URM) begins to take shape, offering a path from fragmented awareness to integrated insight and action.

SECTION 8

# Unified Risk Management: A path forward

## From fragmentation to unification

Unified Risk Management (URM) represents the next stage of maturity in how organizations understand and respond to risk.

It moves beyond functional silos and fragmented tools, creating a connected ecosystem where data, people, and processes interact dynamically.

Interviewees were presented the following definition of Unified Risk Management before being asked to reflect on how this aligned with their experiences.

> Unified Risk Management is an integrated approach organizations can use when assessing and managing risk across third-party relationships, supply chains, and compliance processes.
>
> It consolidates data, automates workflows, and supports cross-functional teams in accessing shared risk intelligence.
>
> URM aims to support more consistent, data-driven decision-making by uncovering both threats and opportunities.

Many of those we spoke to told us that rather than managing risk in isolation, URM has the potential to bring it together under one framework, turning insight into foresight and supporting faster, more confident decisions.

**"We used to spend weeks reconciling reports from different teams. Now we can finally see the whole picture at once."**

**Chief Risk Officer, EMEA, Financial Services**

establishing a shared language of risk that means compliance officers, finance leaders, operations teams, and the board are positioned to see the same information for different purposes and act on it collaboratively.

### WHY URM MATTERS NOW

The case for integration has never been clearer.

As risks accelerate and converge, organizations need systems that can connect data across sources, functions, and geographies.

URM can do this by providing a single pane of glass — a unified view that helps leaders identify interdependencies and prioritize action based on risk impact, not ownership.

For many, the appeal of URM lies in its ability to close the "execution gap":

- → Turning analysis into action
- → Converting fragmented insight into shared intelligence
- → Embedding risk management directly into daily decision-making

**"URM makes risk everyone's responsibility, not just the risk team's."**

**Chief Operating Officer, Americas, Global Corporate**

## THE PRINCIPLES OF UNIFIED RISK MANAGEMENT

Across interviews, four design principles emerged that define what good looks like in a URM model:

### 1. Connected data and systems

Integrate risk signals across platforms to eliminate duplication and provide dynamic intelligence.

### 2. Configurable governance

Move away from rigid policies toward adaptable frameworks that reflect each organization's appetite, thresholds, and obligations.

### 3. Collaborative culture

Empower functions to contribute to risk identification and response, supported by common tools and consistent definitions.

### 4. Continuous insight

Shift from periodic reporting to ongoing monitoring and early warning analytics, supporting proactive intervention.

Together, these principles can replace fragmentation with flow: information moves freely, governance adapts dynamically, and accountability becomes shared.

## LEARNING FROM THE LEADERS

Among the most mature organizations in this study (the "vanguards"), URM thinking is already embedded.

They have not simply implemented new systems; they have redefined what risk means across the organization. Their leaders described risk as a source of resilience and value, not an administrative burden.

These organizations are using URM to:

- → **Anticipate risk through AI and automation**
- → **Unify oversight across regulatory, operational, and strategic domains**
- → **Align performance, resilience, and reputation as part of a single narrative**

> "The real power of URM is visibility. When everyone can see the same risks, we stop arguing about data and start acting on it."
>
> Chief Compliance Officer, APAC, Global Manufacturing

## A ROADMAP FOR TRANSFORMATION

Implementing URM does not require starting from scratch.

The journey begins by mapping the connections between existing risk domains and asking three questions:

### 1. Where are our biggest blind spots?

### 2. What information do we already have but cannot see?

### 3. Who else should be part of the decision loop?

Progress starts with alignment, not overhaul. By identifying shared pain points, particularly around data, visibility, and accountability, organizations can build their own integrated model of control and confidence.

URM is not a single product or platform. It is a philosophy: one that **redefines risk as a unifying force for performance, resilience, and growth.**

SECTION 9

# Conclusion

## Key findings and implications

This study has shown that risk management is entering a defining phase. The pace, interconnectedness, and scope of modern risks have outgrown traditional models of control, but they have also created new opportunities for organizations to rethink resilience.

Across 50 senior leaders in risk, compliance, finance, and operations, **five key takeaways** emerged that define where risk is heading and what organizations may do next.

**01**

### RISK IS NO LONGER SILOED; IT IS SYSTEMIC.

The old boundaries between financial, operational, and non-financial risks are dissolving. Cyber, supply chain, sustainability, and reputational risks are now interconnected drivers of business continuity.

Organizations are now moving from managing events to managing ecosystems.

**02**

### THE CENTER OF GRAVITY HAS SHIFTED TOWARD CONTINUITY.

The new priority is operational resilience — the ability to withstand and recover quickly from disruption.

Financial and regulatory risks remain crucial, but stability now depends on the integrity of systems, suppliers, and data.

**03**

### THE HARDEST RISKS TO CONTROL ARE NOW THE MOST CRITICAL.

Cyber, third-party, and operational risks dominated executive agendas because they combine high impact with high difficulty.

And their interconnected nature means containment is no longer enough; resilience must be built into networks, workflows, and culture.

**04**

### THE BIGGEST CHALLENGE IS EXECUTION, NOT AWARENESS.

Organizations understand what needs to change, but legacy systems, fragmented data, and siloed cultures hold them back.

The challenge now is to operationalize agility and to make insight actionable and risk intelligence continuous.

**05**

### UNIFIED RISK MANAGEMENT OFFERS A BLUEPRINT FOR PROGRESS.

URM appears to provide the structure for integrating data, culture, and governance into one coherent model. It means leaders can better see across their organizations, prioritize what matters most, and build resilience as a shared responsibility rather than a functional burden.

For many, URM represented not just an evolution in risk management, but a foundation for sustainable growth.

GET IN TOUCH

# Contact information

To find out how Moody's can help you unlock the potential of unified risk management, please visit **www.moodys.com/maxsight**


**AMERICAS**
+1.212.553.1653
clientservices@moodys.com

**EUROPE**
+44.20.7772.5454
clientservices.emea@moodys.com

**ASIA (EXCLUDING JAPAN)**
+852.3551.3077
clientservices.asia@moodys.com

**JAPAN**
+81.3.5408.4100
clientservices.japan@moodys.com


MOODY'S