The evolution of non-financial risk

Adapting risk management practices to prepare for future non-financial risks.

KPMG International | kpmg.com

Introduction

The vital role of non-financial risk management

The landscape of the financial services sector has changed significantly and continues to evolve. In the fifteen years since the financial crisis, there have been revolutions in how businesses deliver their services to customers, run their operations and manage their risks, underscoring the growing importance of trust. Trust from regulators, employees, customers and a growing ecosystem of distributors and alliance partners is critical to the continued existence of organizations, maintaining a license to operate, and strengthening the financial system as a whole.

The next few years is looking set to bring accelerated change against a backdrop of increasing digitization, geopolitical turbulence, large-scale artificial intelligence (AI) adoption and complex workforce dynamics. Successfully navigating this phase may be hugely dependent on organization's proficiency in non-financial risk (NFR) management and how we develop this practice to allow businesses to operate responsibly and prosper in the future.

NFR can pose a significant threat

There is often debate about what constitutes NFR, which is often defined differently depending on the organization. A simple definition is that all risk types, *excluding* credit, market, interest rate and liquidity risk, are considered to be NFR, including operational, regulatory, environmental, social and governance (ESG), strategic and business risks, to name a few.

NFR has been a pan-industry concern for some time now, with material losses frequently arising from ineffective management of these risk types. Several prolific occurrences of non-financial risk events have impacted numerous industries, including construction, finance, natural resources and technology. While most risk events incur tolerable operational costs, some more significant incidents have incurred losses valued at upwards of $1bn (often contributed to by a regulatory fine due to mismanagement of risk and related operations).

Looking ahead, NFR may certainly continue to be an area of focus for regulators and businesses alike. As stakeholders demand greater transparency and accountability, NFR will likely come under increasing scrutiny, compelling businesses to make measurable and meaningful enhancements to how they perform risk management. Organizations that fail to address these risks may face significant financial consequences and loss of consumer trust.

It is imperative that businesses be equipped with the correct tools and resources to ensure resilience and adaptability to risk events more holistically. While these events can originate from a myriad of causes and result in various impacts, regardless of internal risk taxonomies, this paper will look at the five key elements that organizations should consider when futureproofing against emerging risks and innovating their risk practices.

> **Successfully navigating this phase may be hugely dependent on organization's proficiency in non-financial risk (NFR) management and how we develop this practice to allow businesses to operate responsibly and prosper in the future.**

Five key considerations for futureproofing against non-financial risks

Click on each consideration to learn more.

01

An integrated NFR function

How to achieve efficiency through an integrated NFR function?

02

Dynamic Risk Management Frameworks (RMFs)

How to ensure RMFs are dynamic, relevant and efficient?

03

Automated management information

How automated risk management information (MI) is produced and used to quantify and report NFR?

04

Robust systems and data management

How systems and data management can accelerate effective decision-making.

05

Enhanced risk management with intelligent automation

How to elevate risk and control processes with targeted intelligent automation?

01

An integrated NFR function

Achieving efficiency through an integrated NFR function

The future of NFR is one of convergence and integration across risk types, the business and business support functions. As organizations become more complex and interconnected, so do the risks they face. This means that traditional siloed approaches to risk management are no longer sufficient. Instead, organizations need to adopt an integrated approach across all three lines of defense that considers the full range of risks they are exposed to.

One of the key components of an integrated risk management approach is an integrated risk function operating model. This model brings together all of the organizations risk management activities into a single, cohesive function.

Organizational structure and responsibilities

The size and structure of NFR teams will vary depending on the size and complexity of the organization. However, the key to success lies in integrating capabilities and close collaboration between the second line of defense (2LOD) and the business. A partnership approach is essential to connect the dots when dealing with intricate challenges. This approach ensures that risk minimization and resilience become ingrained in the organization's ways of operating. Doing so supports the business in making well-informed decisions that strike a balance between risk and reward.

To achieve an integrated operating model, the organizational structure and responsibilities for NFR management must be clearly defined and transparent. This can ensure that specialist NFR teams and business stakeholders are clear on their roles, minimize duplication and receive appropriate resource allocation:

- The NFR function should have a clear mandate and scope of responsibility that empowers them to focus on the most important risks and use resources efficiently.
- The business must have clear delegated authority to allow managers to take informed risks and necessary action to mitigate risks.
- The NFR function should have a strong relationship with the business units it oversees (risk business partnering).

People, skills and capabilities

An optimal approach for a forward-looking risk function is a blend of versatile risk professionals with a strong generalist foundation complemented by experts in specific domains. Within this framework, each significant risk category in the taxonomy should have a designated 'Risk Class Owner' in the 2LOD. These owners should possess in-depth experience and specialized knowledge of the respective risk, taking ownership of related policies and control libraries. They must remain abreast of regulatory requirements, risk appetites and external influences.

The role of Risk Class Owners should be reinforced by collaboration with NFR managers and the first line of defense (1LOD) experts proficient in NFR capabilities like operational risk, compliance, ESG and resilience. This approach ensures robust subject matter expertise for critical risks while maintaining the adaptability needed to address emerging priorities effectively.

An NFR manager of the future should have the following core capabilities:

- **Risk** — An understanding of managing risk within appetites, effective risk monitoring and reporting, implementing and inputting to risk governance, and strengthening a control framework and its operating effectiveness.
- **Leadership** — To drive the organization's values, culture and strategy and lead through change via coaching, influencing skills, strategic thinking and demonstrating integrity.
- **Commercial and innovative** — To steer business value and work towards long term strategic goals, with business acumen, critical thinking and utilizing continuous improvement and project management skills.
- **Digital** — To effectively manage risk and make decisions by utilizing technology and data, with strong capabilities in digital literacy, data analysis, and visualization.
- **Behavioral** — Be interactive and engaging, with the ability to build relationships and influence stakeholders.

NFR managers should further enhance their core skills with specific expertise, such as cyber or climate risk, to ensure comprehensive coverage and effective management of non-financial risks. It's essential to acknowledge that risks constantly evolve and arise with the rapid changes in technology, processes and markets. Consequently, organizations should adopt a flexible model that enables them to swiftly recalibrate their risk expertise to address these changes. This adaptability can be realized through re-skilling or up-skilling existing colleagues.

Alternatively, organizations can consider implementing a 'flexible resourcing' model, which empowers them to deploy the right resources promptly, enabling a proactive response to emerging threats even before they solidify into tangible risks.

Corporate culture

A strong risk culture can help with the early identification of NFRs. This will help ensure the effective management of NFRs and that the organization is equipped to deal with the risks it encounters. It's crucial to be specific about risk culture, thinking of it as the underlying behaviors needed to manage risk effectively, such as:

- **Attention to detail** — Employees apply diligence and seek facts to make sound NFR judgments.
- **Leadership** — Positive risk behaviors are actively role-modelled by leadership, with senior management prioritizing the management of current and emerging NFRs.
- **Speak up** — Employees have the ability and confidence to respond quickly to escalate potential NFRs.
- **Continuous learning** — Effective root cause analysis, knowledge sharing and read across when things go wrong.
- **Balancing risk and reward** — Risk is not a blocker but supports balanced decision-making while supporting NFR appetite and tolerance.
- **Customer care** — Customer outcomes are always front of mind when making decisions.

These behaviors will continue to be important in the future and are often at the core of the risk function. In order to fully benefit from a robust non-financial risk management system, it's important to embed the culture of risk management throughout the organization.

Management teams need to make the behavioral expectations transparent, understandable and positively incentivized, rather than just imposing negative consequences for poor behavior. By transitioning NFR management from being perceived as a policing activity to becoming a partner of the business and an integrated value-adding activity, an organization can fully unlock its benefits.

Benefits of an integrated NFR operating model

There are several potential benefits to taking an integrated approach to the NFR operating model. By considering the factors outlined in this section, organizations can create a function well-positioned to support the business in achieving its strategic objectives in the future. This can lead to improved:

- **Risk identification and assessment** — Brings all the organization's risk management activities into a single cohesive function.
- **Decision-making** — Provides a more comprehensive and holistic view of the organization's risks.
- **Efficiency** — Reduces duplication and helps ensure that risk management activities are conducted consistently.
- **Flexibility** — Enables faster response and more effective management of new and emerging risks.

02

Dynamic Risk Management Frameworks (RMFs)

Ensuring RMFs are dynamic, relevant and efficient

RMFs provide the guardrails for managing risk and outline the 'rules of engagement' for dealing with emerging threats. Current frameworks are often rigid when responding to shifts in the external or internal environment, resulting in challenges when embedding and enforcing frameworks into the broader business.

RMFs can be perceived as servicing regulatory requirements, adding little practical value and often becoming outdated. By ensuring that frameworks are dynamic and efficient, organizations provide their risk community with optimal conditions to practice effective risk management.

Dynamic tailoring of RMFs

So, how do we help ensure risk frameworks are dynamic? Firstly, our RMFs need to be more responsive to internal and external changes. In order to provide sound guidance to employees regarding current and emerging risks, all factors should be taken into consideration when making risk-based decisions. These factors may include economic, environmental, geopolitical or cyber trends, as well as internal factors such as business performance, funding, staff turnover or third-party dependencies.

While monitoring of internal risk events is typically well covered, too often, there is a secluded first-line response to external risk developments with little thought given to how these trends can influence organizational risk strategy, appetite and metrics. The focus for organizations should be to utilize all available information to guide improvements and adjustments within the RMF, to realize optimal risk management approaches at an organizational level, rather than in isolated pockets of the business.

Businesses should be looking to get ahead of risk events by predicting them before solidifying and proactively implementing mitigation strategies. Successful identification of emerging risk trends or precursor events enables companies to avoid unnecessary losses and pre-emptively adjust their risk strategies and control processes and focus their resourcing. These adjustments can be made decisively via the RMF, if successfully embedded.

Technology will naturally play a large part in this evolution, and the use of emerging technologies, such as machine learning (ML) and artificial intelligence (AI) can support the analysis of unstructured data which can inform changes to the RMF.

Businesses can dynamically tailor frameworks by accessing and understanding available NFR data sets and factoring current and expected exposures into the RMF in real-time or as near as possible. A top-down RMF-led approach to risk management enables much closer alignment to business strategy and goals, tighter calibration of appetite and tolerance, and purposeful downstream monitoring and measuring of risk exposures across all business lines.

Effective dissemination

The RMF is a communication tool that allows the central risk function to align risk processes and methodologies across the organization. As with all communication, timeliness and currency are critical — the quicker everyone is aligned the more cohesively risk is performed and the more in line with strategy those processes will be.

With many businesses beginning large-scale adoption of automation across their risk functions, we need to explore similar opportunities to innovate and modernize how we govern our frameworks. By digitizing the RMF (and associated standards and policies), companies can aim for faster modification, near-instant adoption and enforcement of the framework across the business, with a clear opportunity to leverage current and emerging technologies.

An emerging technology with potential in technology and governance is 'Policy-as-Code' (PAC), which can help enhance Governance, Risk, and Compliance (GRC). PAC is a concept whereby the framework (or equivalent compliance document) is translated into code as a set of rules, conditions and parameters that can be embedded into current GRC systems.

This can augment today's technology-enabled risk activities by reflecting real-time changes in policy and frameworks into automated processes, such as risk workflows, monitoring, alerting and management information. It also enables better enforcement of the RMF and easier identification of non-compliant areas or exception management.

Another compelling advantage of digitizing frameworks, along with the underlying standards and policies, is its scalability. Once a certain level of maturity is achieved in centralizing automation and incorporating technology into the foundational risk processes, the effective digitization of the overarching governance should remain unimpacted by the organization's scale. This means that even large Global Systemically Important Banks (GSIBs) with over 100,000 employees should see changes in their frameworks reflected in downstream processes at a pace similar to agile FinTech companies.

By making RMFs dynamic and incorporating digitization, we can encourage:

- Rapid and better-informed calibration of the RMF to cater to internal and external factors.
- Swift adoption and enforcement of RMF processes via technology enablers.
- Enhanced risk management through a standardized and integrated RMF, fostering improved understanding and collaboration.

03

Automated management information

Producing automated risk management information (MI) to quantify and report NFR

How much time are your risk experts spending on detailed analysis and decision-making, versus inefficient data sourcing and aggregation? How long do teams spend manually updating Excel spreadsheets and PowerPoint presentations in each reporting cycle?

NFRs are inherently difficult to quantify. However, organizations that aim to identify and prioritize risks effectively should have an element of automated risk MI to support efficient assessment of the likelihood and impact of risks — enabling the effective development and implementation of risk mitigation strategies.

Many organizations have dedicated teams solely responsible for the aggregation, analysis and formatting of MI for regular governance meetings creating significant overhead costs. The resulting MI is often outdated (sometimes over a month old) and does not provide sufficient or accurate information for management to make informed decisions. For example, in the financial services industry, it takes, on average, nine days from identifying a control violation until it is reported and communicated to the control or process owner.[1]

To improve the efficiency of these activities, automation can be utilized to capture, analyze and present data in a more useable and understandable way. However, there are some challenges organizations need to address to effectively use automated risk MI to quantify and report on NFR, including:

- **Investment decisions** — Automated risk MI can require significant investment. An objective cost-benefit analysis should be able to identify where the investment yields the most substantial returns.
- **Lack of expertise** — Automated risk MI can be complex to implement and use, and risk functions may need to reshape their talent profile.

Despite these challenges, automated risk MI can be a valuable tool for organizations by making timely and informed decisions based on near real-time information to protect their operations, finances and reputation.

Here are some of the potential benefits of using automated risk MI to quantify and report on NFR:

- More objective and consistent evaluation, variable 'expert judgment' where necessary.
- Increased accuracy and efficiency compared to manual methods of reporting, which are often resource-intensive and prone to human error.
- Improved visibility, with a more comprehensive view of the NFR landscape.
- Predictive or faster response to risks and compliance with regulation.
- Tracking the effectiveness of risk mitigation strategies.

[1] APQC OSBsm Data

04

Robust systems and data management

Using systems and data management to accelerate effective decision-making

Tech Stacks

To ensure improved risk mitigation and operational efficiency objectives are met, businesses need an Integrated Risk Management (IRM) ecosystem that harmonizes solutions across one or more platforms. This ecosystem should cover all three lines of defense using a common set of integrated policies, technology and data.

Most systems architecture today lacks the necessary tools for effective data aggregation and reporting. While policies and procedures are firmly in place, the organization of these systems remains somewhat disorganized, with each operating in isolated silos. There is a clear need for improved collaboration and insights across different business areas, but there is no 'one size fits all' approach to achieving IRM with technical solutions. The right approach depends on several factors, including an organization's key reporting needs, existing assets, licensing agreements, centralized versus decentralized governance approaches, investment ability and willingness to challenge its current ways of working.

Here are three approaches organizations can consider depending on their needs:

- **Interoperable** — An integrated risk system prioritizing data between loosely aligned systems with basic automation interfaces. The system requires alignment between departments and can be complex to maintain if systems are not fully connected.
- **Shared** — A multi-vendor risk system prioritizing centralized reporting and can be achieved with minimal changes to existing solutions. However, the lack of connection between data sources reduces integration.
- **Consolidated** — A fully integrated risk ecosystem that combines interoperable and shared methods. Data is directly related, with operations focusing on user experience, simplicity and full technical integration. This is considered the most innovative approach for the organization that aims to be truly fit for the future; it is, however, associated with considerable costs and overheads.

Interoperable

Multi-vendor with integrations

- Tight technical integrations
- Loosely aligned processes
- Data feeds aligned
- Specialist solution offerings
- Focus on organic growth and optimization

Ideal for organizations who want to maintain their existing systems and invest in integrating them.

Shared

Multi-vendor with pooled data

- Limited technical integration
- Loosely aligned processes
- Data models aligned
- Specialist solution offerings
- Focus on oversight

Ideal for organizations who are more interested in joint reporting outcomes than aligned procedures or complex integrations.

Consolidated

Single vendor/platform

- Full techinical integration
- Intimately aligned processes
- Data directly related
- Broad solution offerings
- Focus on consistency, user experience and simplicity

Ideal for organizations keen on leveraging an existing vendor with a broad solution set they can slowly expand into.

GRC systems

The future of managing NFR will heavily rely on putting technology at the center of the risk function strategy. Organizations are increasingly investing in GRC systems, resulting in improved risk management, heightened compliance and reduced costs. GRC systems look to unify risk management, governance and regulatory compliance within an organization, promoting transparency, efficiency and accountability across business activities.

Businesses that continue to rely heavily on spreadsheets to track data and manage risks will struggle to adapt to evolving regulations and industry best practices. Difficulties will be faced in maintaining risk MI integrity and availability, governance and data reporting will be cumbersome, and the cost implication of manual and inefficient tooling will be increasingly uneconomical.

By prioritizing the development of a robust, centralized GRC system, organizations can better prepare for unforeseen circumstances. As a result, GRC systems need to focus on:

- **Centralizing controls** — Transparent, centralized control repositories (e.g. libraries showing the standard controls for each risk class) are more important than ever, promoting consistency and better data management.
- **Automating workflows** — Automated workflows reduce the risk of human error and ensure tasks are completed efficiently (see section 5).
- **Customizing reporting to meet business needs** — Quick access to MI is invaluable, allowing for informed decision-making using up-to-date and reliable data.

These advancements enable organizations to significantly enhance other fundamental risk processes such as risk assessments, scenario analysis and read-across activities.

05

Enhanced risk management with intelligent automation

Elevating risk and control processes with targeted intelligent automation

Intelligent automation (IA) is the combination of automation and artificial intelligence (AI), which has emerged as a game-changer in the business world. Its transformative potential is highly useful in addressing NFRs, not by replacing human resources, but rather by collaborating between people and technology, to achieve the best possible risk management outcomes.

According to KPMG 2023 CEO Outlook, business leaders across sectors are focused on investing heavily in disruptive technology and financial services CEOs are no exception, with 72 percent agreeing that generative AI is the most important investment opportunity for their company.[2]

The age of IA is here, and there is no turning back. Organizations implementing IA have reported significant returns on investment (ROI) and efficiency gains. Forrester Research predicts that IA will significantly impact the global financial services industry, increasing revenue by up to 15 percent and reducing costs by up to 20 percent. The research indicates that AI and IA can automate up to 40 percent of tasks currently performed by humans in the financial services industry. This will free employees to focus on more strategic work.[3]

Automation, at its core, removes human intervention and enables organizational efficiency, streamlining repetitive and manual operations, enhancing the accuracy of process execution and reducing costs. However, the advent of IA has introduced a paradigm shift by integrating AI capabilities into automation frameworks, enabling systems to operate with increased cognitive abilities and adaptability.

Contrary to concerns about the replacement of human roles, the true essence of IA lies in augmenting human capabilities and expertise. It empowers organizations to leverage the strengths of both humans and machines to address NFR more effectively. Through the integration of AI technologies like machine learning, natural language processing and robotic process automation, IA systems can efficiently analyze extensive datasets. This enables the recognition of patterns and identification of anomalies, contributing to the early detection of potential NFR.

[2] KPMG 2023 CEO Outlook, KPMG International, 2023.
[3] Forrester Research, "The Future of Jobs in the Age of AI and Robotics," 2018

Example use cases of IA include:

Increased use of synthetic data:

Synthetic data is proving invaluable in the rapidly evolving world of financial services, especially when managing non-financial risks. As an artificially generated alternative to real data, it provides a secure and cost-effective means to navigate sensitive information challenges. Financial institutions can utilize synthetic data for risk scenario simulations, compliance testing, anti-money laundering, and fraud detection, bolstering their resilience against potential threats. Additionally, it facilitates employee training, cybersecurity testing, and modeling of operational risks, fostering adaptability. While synthetic data holds great promise, its best application lies in conjunction with real-world data for comprehensive risk assessment and management. By leveraging its potential, financial services can proactively address non-financial risks and lead risk management practices in the digital era.

Cybersecurity and data privacy:

With the proliferation of connected devices and smart machines, the risk of cyber threats and data breaches increases. Financial institutions need to bolster their cybersecurity measures to protect sensitive customer information and financial data from potential attacks. IA can enhance cybersecurity by continuously monitoring and analyzing network activities, identifying potential threats and responding in real-time to cyber incidents. AI-powered security solutions can detect and mitigate sophisticated cyber-attacks, reducing the risk of data breaches and protecting customer information.

Operational resilience:

The transition from fixed to interchangeable assets implies a shift in how financial institutions manage their operational risks. They need to be prepared for disruptions caused by technology failures or cyber incidents and ensure business continuity and resilience. IA can enhance operational resilience by automating critical processes and reducing the reliance on manual interventions that may introduce errors or delays. Workflow automation can help streamline incident response and disaster recovery procedures, ensuring faster recovery from operational disruptions.

Customer trust and experience:

The move from global to personal and the rise of connected humans and devices emphasize the importance of building and maintaining customer trust. Financial institutions need to prioritize customer data protection and provide transparent and reliable services to retain customer confidence. IA can improve customer trust and experience by delivering personalized and efficient services. AI-powered chatbots and virtual assistants can address customer queries in real-time, enhancing customer engagement and satisfaction.

IA represents a dynamic interplay between processes and people. While automated processes enhance efficiency and accuracy, human intervention remains critical for decision-making, judgment and creativity. The collaboration between humans and machines harnesses the strengths of each, ensuring a robust risk management framework that combines technological prowess with human ingenuity to minimize the impact of NFR incidents on the organization's operations and reputation. By implementing this optimization, senior managers can allocate resources to higher-risk areas and emerging threats. Skilled professionals can then concentrate on more strategic and intricate risk management activities, leveraging their expertise to make well-informed decisions and devise comprehensive risk mitigation strategies.

Conclusion

A sharp focus on non-financial risk is now imperative

Looking at the scale and depth of emerging risks that the market faces in today's hyper-competitive and fast-changing global landscape, it's valid to question whether the responses this report has examined will be adequate.

Can banks become agile quickly enough? Can a supervisory balance be struck that continues to stimulate innovation while protecting customers and markets? Will technology platforms create as many problems as they solve?

Simply put, financial markets today stand at an inflection point. They are on the cusp of deep and positive transformation — while also facing potential instability and risks to customers, banks and the markets themselves. What's now important is to ensure that the questions raised in this report are actively and constructively debated. The wider and deeper the discussion, the better the opportunity for financial services to be future-proof and poised for growth.

As noted in this report, non-financial risk will certainly remain in sharp focus among businesses and regulators alike. As stakeholders demand greater transparency and accountability, NFR will likely come under increasing scrutiny, compelling businesses to make measurable and meaningful enhancements to how they perform risk management.

Businesses need to be equipped with the correct tools and resources to ensure resilience and adaptability. As we stress in this report, success will likely demand:

- An integrated NFR function;
- Dynamic risk-management frameworks;
- Automated management information;
- Robust systems and data management;
- Enhanced risk management with intelligent automation.

Businesses may drive and accelerate change against a challenging backdrop of increasing digitization, geopolitical turbulence, large-scale AI adoption and complex workforce dynamics. Therefore, businesses should be equipped with the correct tools and resources amid evolving risks and global challenges.

Successfully navigating the journey ahead will likely demand innovative non-financial risk management that positions businesses to operate responsibly and prosper in the future. Organizations that fail to address these risks may face significant financial consequences and loss of consumer trust. Change is inevitable. And the time to act is now.

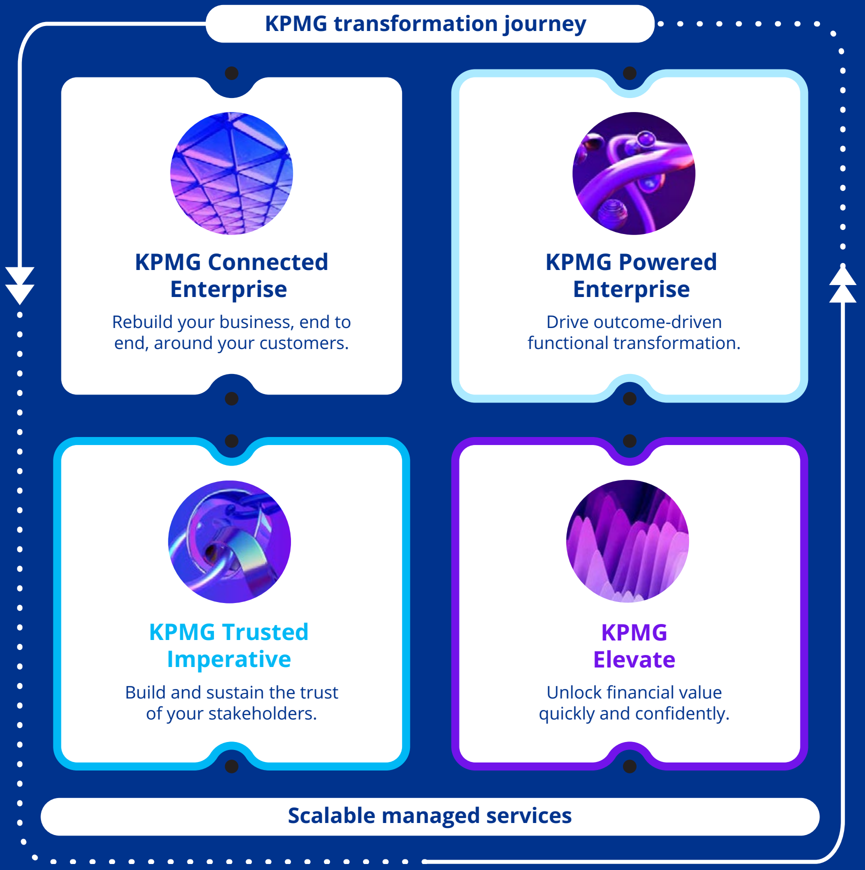
How this connects with what we do

In the contemporary business landscape, the need for transparency in managing non-financial risk and controls is steadily increasing. At KPMG, we fully acknowledge the paramount significance of robust non-financial risk management practices. Our global team of risk professionals offers a wealth of experience, specializing in optimizing the efficiency and effectiveness of your non-financial risk processes, free from subjectivity.

An efficient non-financial risk management process is the foundation of effective risk mitigation. Our approach leverages cutting-edge technology, facilitating real-time data collection and analysis, enabling you to make well-informed, risk-based decisions. KPMG risk professionals are dedicated to working alongside you, fostering trust, reducing risks, and unlocking new value, helping ensure your readiness for the future.

Collaborating with KPMG can not only enhance the effectiveness of your non-financial risk management but also help ensure its alignment with your strategic business objectives. We work closely with you to help you develop an understanding of your non-financial risk landscape and its active and proactive management. Our proficient team of risk professionals can transform your non-financial risk processes into a robust and invaluable tool for comprehensive risk management, fortifying your organization's resilience with secure and trusted risk management practices.

In addition, KPMG firms' suite of business transformation technology solutions can help you engineer a different future — of new opportunities that are designed to create and protect value.



KPMG transformation journey

KPMG Connected Enterprise

Rebuild your business, end to end, around your customers.

KPMG Powered Enterprise

Drive outcome-driven functional transformation.

KPMG Trusted Imperative

Build and sustain the trust of your stakeholders.

KPMG Elevate

Unlock financial value quickly and confidently.

Scalable managed services

Contacts

Fabiano Gobbo
Global Leader, Risk and Regulatory Advisory
KPMG International
fgobbo@kpmg.it

Cameron Burke
Principal, Risk and Regulatory Advisory
KPMG in the US
cburke@kpmg.com

Narinder Singh
Partner, Risk and Regulatory Advisory
KPMG in the UK
narinder.singh@kpmg.co.uk

Roger Acton
Director, Risk and Regulatory Advisory
KPMG in the UK
roger.acton@kpmg.co.uk

Matt Tottenham
Partner
KPMG Australia
mtottenham@kpmg.com.au

Andrea Antonio Colombo
Associate Partner, Risk and Regulatory Advisory
KPMG in Italy
andreacolombo@kpmg.it

Matthias Degen
Partner
KPMG in Switzerland
mdegen@kpmg.com

Markus Quick
Partner
KPMG in Germany
markusquick@kpmg.com

We would like to acknowledge the contributions of Benjamin Lemon, Benjamin Morrison, Lisa Widdows and Joel Kibirige.

kpmg.com

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG refers to the global organization or to one or more of the member firms of KPMG International Limited ("KPMG International"), each of which is a separate legal entity.
KPMG International Limited is a private English company limited by guarantee and does not provide services to clients. For more details about our structure please visit kpmg.com/governance.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

Throughout this document, "we", "KPMG", "us" and "our" refers to the global organization or to one or more of the member firms of KPMG International Limited ("KPMG International"), each of which is a separate legal entity.

Designed by Evalueserve.

Publication name: The evolution of non-financial risk | Publication number: 139156-G | Publication date:January 2024