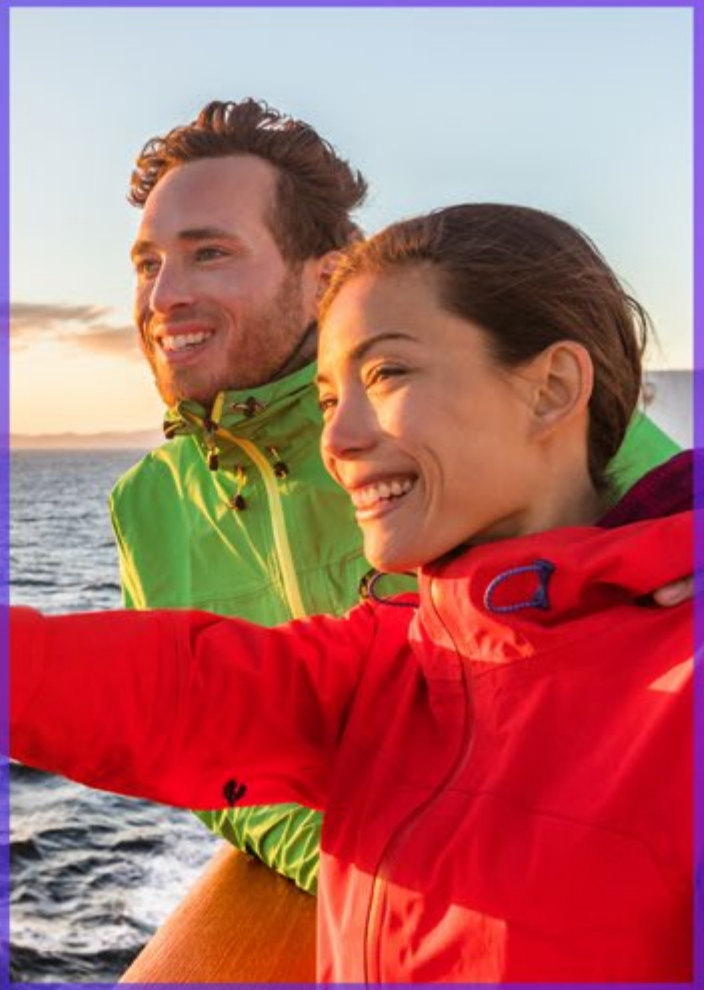
KPMG

Taking risk management to the next level in banking



The journey to modern risk infrastructure is inevitable

Whitepaper

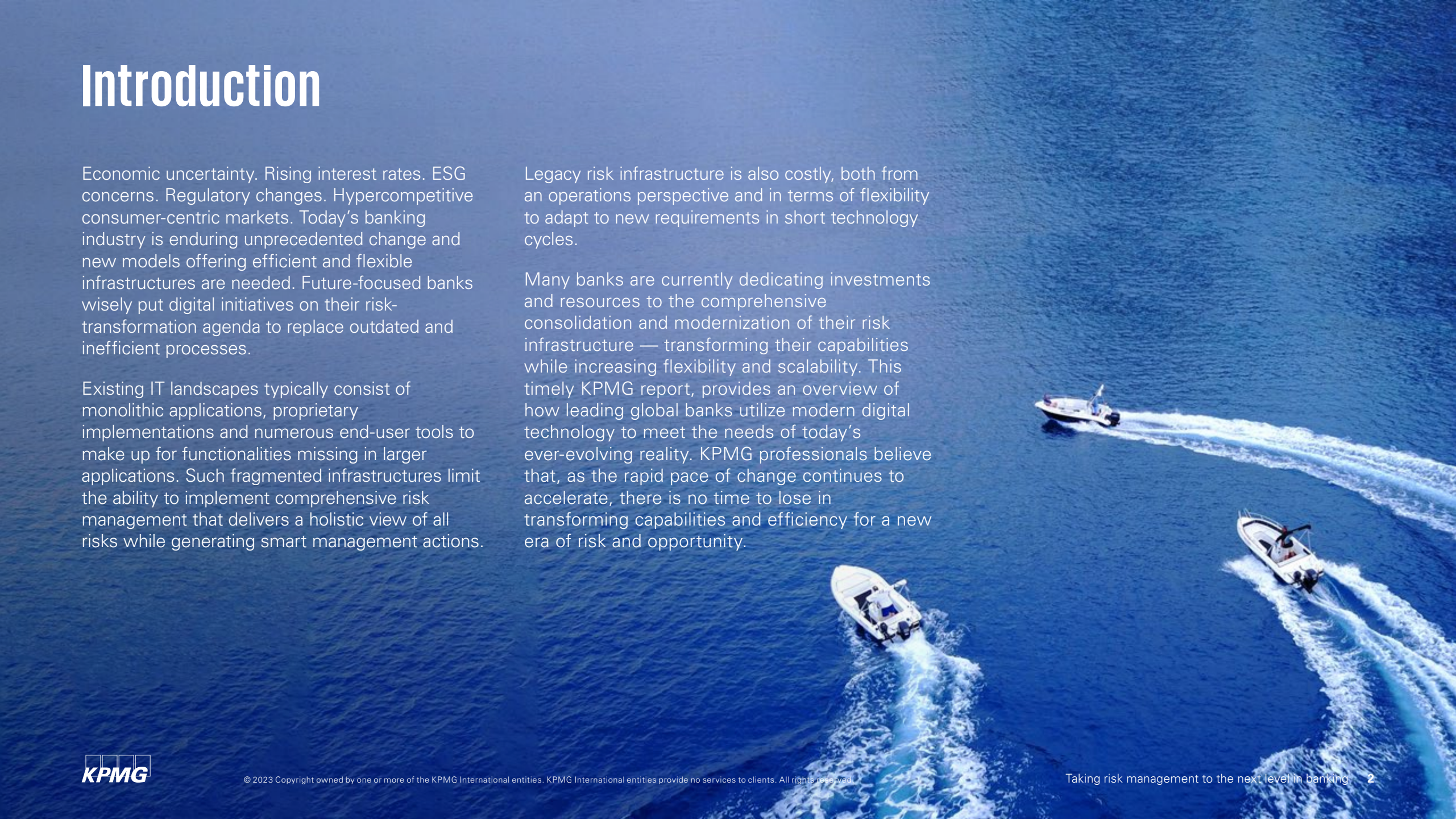
Introduction

Economic uncertainty. Rising interest rates. ESG concerns. Regulatory changes. Hypercompetitive consumer-centric markets. Today's banking industry is enduring unprecedented change and new models offering efficient and flexible infrastructures are needed. Future-focused banks wisely put digital initiatives on their risk-transformation agenda to replace outdated and inefficient processes.

Existing IT landscapes typically consist of monolithic applications, proprietary implementations and numerous end-user tools to make up for functionalities missing in larger applications. Such fragmented infrastructures limit the ability to implement comprehensive risk management that delivers a holistic view of all risks while generating smart management actions.

Legacy risk infrastructure is also costly, both from an operations perspective and in terms of flexibility to adapt to new requirements in short technology cycles.

Many banks are currently dedicating investments and resources to the comprehensive consolidation and modernization of their risk infrastructure — transforming their capabilities while increasing flexibility and scalability. This timely KPMG report, provides an overview of how leading global banks utilize modern digital technology to meet the needs of today's ever-evolving reality. KPMG professionals believe that, as the rapid pace of change continues to accelerate, there is no time to lose in transforming capabilities and efficiency for a new era of risk and opportunity.



Contents

01 The ‘make or buy’ balancing act for banks

The ‘make or buy’ balancing act for banks

When choosing risk architecture components, a key consideration is whether to ‘make or buy’ — deciding on a vendor tech solution or proprietary development of new capabilities. The decision typically involves a balancing act between standardization and individual needs. Vendor tech solutions provide standardization while maintaining a certain degree of flexibility, while proprietary software initiatives can be easily tailored to specific business requirements.

Vendor tech solutions and adherence to standards will likely reduce costs

Many of today’s medium-sized banks are embracing vendor solutions, partly because they incentivize a “bank follows standard” approach. On one hand, vendor tech solutions do not offer the complete flexibility of proprietary developments, but allow some customization through lobbying of the client base. On the other hand, the complexity of architecture and the headcount needed to run it can be reduced and serve to lower costs.

Most importantly, the vendor can implement regulatory-driven changes without needing a specific client request. And since associated costs for such changes are shared by the total client base, the cost baseline is further reduced. Many vendors offer managed services or similar outsourcing agreements that provide additional strategic advantages for the risk function.

But specialized business models may require a deviation from standards

The advantages of vendor tech solutions don’t make proprietary initiatives obsolete, far from it. These use cases typically stem from highly individualized business models or specialized functionality needs that traditional vendor tech solutions don’t offer. For example, a bank specializing in corporate or project finance and structuring complex credit deals requires sophisticated credit-risk management to enhance regulatory capital and economic exposure. In this context, a proprietary digital solution with a customized technical architecture is likely the right choice.

“The rising cost of risk architecture is expected to continue to increase if nothing changes. Often, a complete modernization of the outdated systems is required to help remain profitable in the long term.”

Heiko Carstens
Partner, Risk and Treasury
KPMG in Germany

Institutions can benefit from vendor solutions

The market for vendor systems for risk management is vast, spanning various financial and non-financial risk management functions and ranging from very specialized solutions to comprehensive platforms servicing not only risk, but also financial controls, accounting and reporting needs. This diverse offering corresponds to today's multifaceted needs regarding risk architecture modernization. Some vendors have clear aspirations to extend their platforms over the coming years. Even large-tier banks are introducing or expanding their coverage of vendor tech solutions for specific areas of their risk management functions. This trend is likely to continue, with cost efficiency being the number one priority, in addition to creating productive synergies in finance and the front office.

"In many banks, infrastructures have been developed with provisions and manual processes. To be able to react to fluctuating market developments and regulatory changes, these need to be modernized."

Heiko Carstens
Partner, Risk and Treasury
KPMG in Germany

02
Look to the cloud for critical new advantages

Look to the cloud for critical new advantages

Leaving outdated processes behind

Traditional risk IT and data architectures are no longer up to the task of meeting current and evolving business needs. Risk calculations can take several hours amid numerous individual steps and human intervention. This dated approach makes risk management costly, inefficient, error-prone and high-maintenance — and it overlooks the revolutionary advantages of modern digital solutions.

Modern architecture is fast and flexible

Risk managers in banks need an architecture that is both standardized and flexible. Standardized risk calculations that banking supervisors regularly require need to be activated with the simple push of a button that produces results within seconds. Equally important are rapid risk calculations amid ever-changing market conditions.

A cloud-native architecture turns hours into minutes

Highly scalable cloud infrastructure enables risk management to save considerable time on risk calculation, ideally allowing risk managers to focus on other business needs. Not surprisingly, calculation-intensive areas of risk management are typically the first movers to cloud-native implementations that provide: the valuation of financial instruments, cash flow generation, traded market risk, net interest income simulations and counterparty risk simulations.

Reduced maintenance due to a modular design based on microservices allows individual program modules to be revised or replaced independently. Therefore, maintenance and adaptation to new regulatory requirements are flexible and easy to manage. Ideas can be tested on short notice without additional costly infrastructure and lengthy processes.

With the pay-per-use model, unused or overbooked resources don't need to be kept idle and paid for if no risk computations occur.

A paradigm shift is required to leverage the expected benefits of the cloud — bringing IT and the business closer together to enable continuous deployment and innovation.

One thing is clear: cloud computing is inevitable for banks that want to modernize their risk architecture and tap into the advantages of state-of-the-art technologies.

"The cloud has potential to transform the Risk function. In an interconnected world, where risk now has many dimensions, cloud-based architecture and practices will enable you to connect-the-dots, manage, and mitigate risks intelligently."

Bharat Bhushan
Partner
KPMG in the UK

03
The data-driven future is here

The data-driven future is here

The innovation agenda among today's organizations focuses on cloud services, process automation and digital reporting. But none of this is sustainable if timely, accurate data is not available, traceable and subject to instant analysis.

Modern data management is critical

As with risk architecture, data management is typically structured in diverse ways. Inconsistent and unreconcilable data consumes valuable time among risk managers and leads to difficulties evaluating risk information. How often are different values for the same risk metric in other data marts? This results in conflicting reporting statements that can be recognized, but rarely remain reconcilable.

Most banks strive for a single point of truth for risk data that can be mapped via a reporting data mart (RDM) for various purposes. The RDM forms the basis for all evaluations — a single correct value for all employees, with no end-user computing or workarounds. Silos can be abolished, and data consistency can be ensured.

In addition, the RDM can be extended with specific external or individual data using a data lake for ad-hoc analysis. This database is used for all internal reporting and analysis — reaching far beyond the risk function.

Data governance is a culture, not a theory

Data that's available in an RDM is not automatically accurate. Far too often, data is manually corrected during the last steps of the reporting process — rather than at the source. Usually, this is done on aggregate values, making consistent analysis of the source data and traceability impossible.

Any corrections must always be performed at the source of the process and system. In the future, workarounds to cure data quality 'just before the risk report' should be eliminated. Unfortunately, what sounds logical is still not common practice.

The future demands active data governance that is enterprise-wide. All employees should be clear on who their data customers are and how data-driven insights can enhance services and operations. This can be supported by data analytics tools such as automated correction of data records.

Risk officers need a clear view

Transparency of the data flow from the source to the risk report can be ensured via a data lineage and data glossary. What seems like a common practice, according to Basel Committee on Banking Supervision 239 (BCBS), is still proving to be a work in progress when it comes to implementation. Quite often, parts of the data flow are documented, but a view of the total data flow is missing, resulting in an exhausting exercise of clicking through various data trees. The report may deliver a 'best guess.' Offering a starting point to the data lineage via reports, precise descriptions and suggestions can enable effective and easy data shopping for employees.

Data within an organization is key to unlocking insights. Start with setting up processes and systems to extract, manage, and share appropriate data safely. This will allow the entire organization to make data-led decisions."

Bharat Bhushan
Partner
KPMG in the UK

04
A new reality of reporting and data insights

A new reality of reporting and data insights

Dynamic reporting is an imperative

With an RDM in place, it's now a matter of evaluating it in a targeted and efficient manner to produce impactful risk reports. Developing static reports that need to be manually adjusted frequently is an obsolete approach today. The goal for every CRO should be to create efficient, dynamic, low-effort risk reporting that enables simple, fast and individual analysis. It's, therefore, crucial to align the organization and reporting infrastructure accordingly.

The need to comply with targeted reporting goals

A dedicated team for RDM development and operation is essential amid the large flow of data and the system's complexity. In addition, there should also be a team independent of any specific department and acting as a 'business integrator' — converting various data requirements into views within the central RDM. Multiple departments can then access and use the data flexibly for their reports.

Business intelligence tools are the new PowerPoint

The risk team should perform the development of analytical and reporting dashboards used for risk reporting with the help of business intelligence (BI) tools. These tools typically offer accessible user interfaces and the ability to make templates for individual users, leading to easy entry for team members. BI tools make reporting much more mobile and adaptable. Static reports can still be generated, but are expected to become extinct over time. At the heart of these plans is the ability to respond quickly and flexibly to ad-hoc requests such as a stress test or other what-if analyses.

Automation is delivering breakthroughs

There's a trend toward integrating BI components into tools for workflow-based reporting. Workflow automation of reporting processes allows businesses to focus on analyzing data and responding. They're not distracted by formal processes, and the report can be generated much faster.

For example, KPMG in Germany worked with a banking client that saw report creation accelerated by seven days — a significant 35 percent reduction — by building and implementing a workflow-based reporting platform. In addition, the number of employees required for report preparation was reduced to eight from 20.

"Advancements in technology allow banks to carry out ad-hoc analyses quickly and effectively. A realignment of reporting is required to take advantage of new modernized technologies and digital solutions."

Jeffrey Dykstra
Principal, Advisory
KPMG in the US

“In today’s environment it is critical for CROs to retain the ability to analyze data effectively — flexible reporting is essential to act in a timely and efficient manner.”

Jeffrey Dykstra
Principal, Advisory
KPMG in the US

05 Keeping non-financial risks in focus

Keeping non-financial risks in focus

Governance, risk, compliance (GRC) software for non-financial risks

Although there is no universally agreed-upon definition of non-financial risks (NFR), it's widely used across the financial industry. Depending on the financial institution and its risk profile, NFR encompasses a broad range of risks: operational risk, reputational risk, IT or cyber risk, third-party risk, conduct risk and more.

Governance of NFR is indeed complex and includes many second line-of-defense (LoD) functions that are often widely dispersed across a bank's operations. Combined with varying regulatory requirements and standards, this typically leads to a silo-based organization with different methodologies and processes for identifying, assessing, monitoring, reporting and steering NFRs. Although the central role naturally falls to the CRO function, efficient NFR management implies significant alignment efforts with information security, compliance and outsourcing management professionals. Due to the number and diversity of stakeholders, all with their own requirements, agreeing upon a commonly used software solution for NFR can be very challenging compared to financial risk — but the effort can certainly be worthwhile.

Harmonizing methods and processes

Implementing a common tool can harmonize methodologies and processes, produce efficiency gains, and leverage synergies between lines of defense. The first LoD, which in the past was consumed by the activities imposed by the second LoD, can benefit from the elimination of outdated redundancies. A GRC solution establishes a joint database by implementing common data storage and management standards. The collection of redundantly collected data can be eliminated and common data can be leveraged for monitoring and reporting. This can help improve efficiency and consistency across the organization.

GRC software can fail to satisfy all needs

Software vendors have recognized the diverse needs of their customers and strive to develop overarching GRC digital solutions that cover and integrate the functionality of various stakeholders. Many vendors have developed GRC solutions with standard modules that successfully incorporate the functionality of the process-driven second LoD functions — information security, business continuity and outsourcing management. However, GRC standard software often fails to meet operational risk management needs, as some requirements, such as categorization of data loss, are seldom met.

The implementation of GRC software often proves more cumbersome than initially anticipated when the existing methodology of the second LoD functions can only be applied to a customized standard functionality. This customization is more costly in the initial implementation and requires regression testing in future software releases.

Holding on to existing methodologies is also why promised efficiency gains fall behind expectations. Banks often underestimate the effort needed to harmonize methodologies and processes or the compromises required for individual functions. The common tool can only be the incentive for harmonization — not the solution itself.

Vendor tech solutions for smaller players

Vendor solutions for GRC software are more often seen among smaller and medium-sized institutions. Since fewer stakeholders need to be involved and the methodology of the respective functions tends to be less complex, standard functionality is more likely to suffice. Larger banks tend to rely on their digital solutions, as they require more alignment and customization, and they can make IT capacity available for tailor-made tech solutions.

Build on a foundation of technology and data

Regardless of an in-house or vendor solution, the same holds for financial risk as for NFR: the ability to take advantage of digital technology and a solid data foundation can be critical as addressed earlier.

The future is now

It's clear that the future is digitally enabled and data-driven. Today's revolutionary technology is opening the door to remarkable new possibilities for NFR management. As the rapid pace of change continues to accelerate and rewrite the rules for growth and success in today's global banking industry, banks need to be efficient, flexible and fit for the future. Achieving this requires reassessing a bank's risk architecture. This begins with data and ends with reporting. CROs, together with other relevant bank functions, should rethink and potentially radically transform their risk architecture — utilizing modern digital technology to meet the needs of today's ever-evolving reality.

To ready themselves for NFR challenges — today and tomorrow — banks should to invest in modern IT infrastructure and data-management capabilities.

"For years, banks have tried to integrate their NFR frameworks. The introduction of GRC software can provide the incentive to find a common solution."

Jeffrey Dykstra
Principal, Advisory
KPMG in the US

GRC tech solutions can under-deliver on initial expectations once they have been implemented. This is due to stakeholders failing to harmonize and adapt their methodologies beforehand, as well as the lack of a one-size-fits-all digital solution for everyone in the market."

Jeffrey Dykstra
Principal, Advisory
KPMG in the US

06 How KPMG professionals can help

How KPMG professionals can help

In various sectors, organizations have a real opportunity to define a different future through digital transformation — and stakeholder trust is an indispensable ingredient. KPMG professionals strive to understand how you feel about the opportunities and challenges because they have encountered many of them in their own digital transformation. They know firsthand the importance of creating and retaining stakeholder trust. Their business depends on it.

Meeting you wherever you are on the journey, KPMG professionals combine deep business, industry, and technical knowledge to integrate risk and regulatory discipline within your digital transformation. They can provide holistic support, from the evaluation of options through to implementation — helping you walk the tightrope between standardization and flexibility.

Whether you're optimizing a single function or connecting the entire enterprise, you can inspire stakeholder trust throughout. As a business enabler, trust can lead to responsible growth, bold innovation, confident decision-making, and sustainable advances in performance.

To be efficient, flexible, and ready for the future, the risk architecture of every bank must be fundamentally reassessed — this begins with data and reporting. Time is pressing, and CROs must rethink their approach when looking to transform their risk architecture. KPMG offers support to CROs in key decision-making, from evaluating options through to implementation by developing agile solutions for standardization and flexibility.

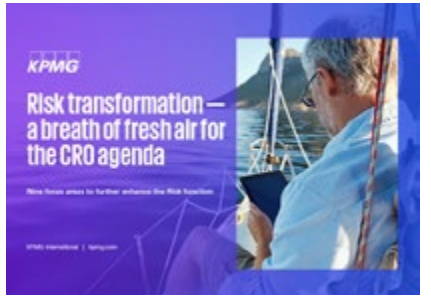
Related publications

ESG risks in banks

Closing the disconnect in ESG data (Part 2)

Risk Transformation — Driving Value in Risk Management

SSM beyond COVID-19: ICLAAP



Risk Transformation CRO agenda

Contacts

Heiko Carstens
Partner, Risk and Treasury
KPMG in Germany
hcarstens@kpmg.com

Jeffrey Dykstra
Principal, Advisory
KPMG in the US
jdykstra@kpmg.com

Bharat Bhushan
Partner
KPMG in the UK
bharat.bhushan@kpmg.co.uk

Fabiano Gobbo
Leader and Partner
KPMG in Italy
fgobbo@kpmg.it

Justin Malta
Partner
KPMG in the UK
justin.malta@kpmg.co.uk

Matthias Mayer
Leader
KPMG in Germany
matthiasmayer@kpmg.com

Brian Hart
Principal, Advisory
KPMG in the US
bhart@kpmg.com

Koen De Loose
Partner, Head of Risk & Regulatory
KPMG in Belgium
kdeloose@kpmg.com

François Delcourt
Principal, Advisory
KPMG in Belgium
fdelcourt@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia

Designed by Evalueserve.

Publication name: Taking risk management to the next level in banking | Publication number: 138609-G | Publication date: March 2023