KPMG

# Transforming technology risk

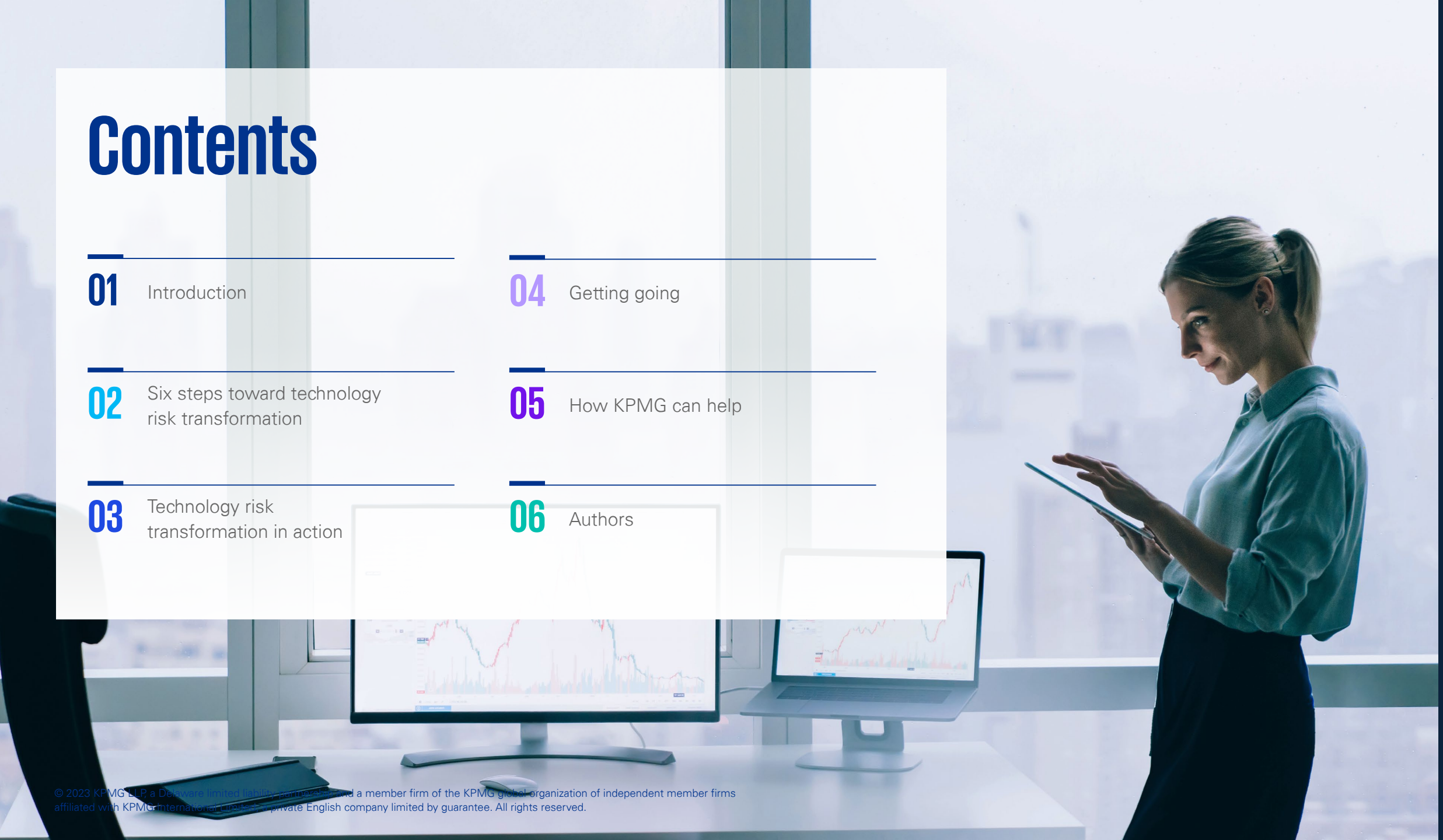
Managing technology risk to build stakeholder trust

**The future of technology risk**

kpmg.com

# Contents





# Introduction

Most organizations are modernizing their critical information technology—to improve the customer experience, replace aging software, shift work to the cloud, or adopt artificial intelligence systems. Adding to the challenges are evolving regulations, changing customer behaviors, the concept of data as an asset, and employee expectations for flexible technology tools to use in a more virtual workplace.

Technology risk and compliance need to adjust to this new reality. Among attendees of a recent KPMG webcast, only 11 percent of risk executives said their organization was "very mature" in its ability to assess and respond to changes in risk posture.[1] Consider these trends:

Businesses are transforming and modernizing the technology stack. Therefore, technology risk approaches and controls must adapt, too.

Threats to technology are becoming more complex and more sophisticated, so risk management approaches must transform and be multilayered and agile.

Increasing technology trust and transparency with stakeholders are becoming the new normal in the marketplace.

Automation, technology, and data can help build technology risk capabilities, but organizations must be willing to change and invest in these areas.

However, in many organizations technology risk knowledge remains limited or may not be keeping pace with innovation.

The future of risk is shifting away from a regulatory-driven "protect agenda" to one where organizations leverage risk to enable firmwide growth and optimization. That means becoming closer to the business and driving towards an environment with more proactive monitoring and automated controls to address risk events as close to real-time as possible. Boards and shareholders want the technology risk teams to be a strong partner to the business and want to leverage regulatory-focused investments to further business results.

Based on our experience with clients, we have identified key areas where technology risk leaders should focus their efforts to shape their organizations for the business challenges of today—and tomorrow.

**These key areas are:**

1. Taking a fresh look at the technology risk operating model
2. Gaining a competitive advantage by increasing technology trust and transparency with stakeholders
3. Making better use of data, analytics, and insights; invest in digital acceleration
4. Upskilling and embracing new ways of working
5. Pursuing digital acceleration
6. Accelerating technology risk transformation.

In the following pages, we share our insights into how companies can take these steps toward technology risk transformation.

[1] Source: Participant survey, KPMG webcast, "Risk transformation in the digital world," October 31, 2022.

# Six steps toward technology risk transformation

# 01. Taking a fresh look at the technology risk operating model

Businesses continue to prioritize digital investment. They have digitized business processes, modernized IT infrastructure, moved work to multiple cloud environments, and connected to customers, suppliers, employees, and partners. In the KPMG 2022 CEO outlook survey, 72 percent of respondents indicated that they have an aggressive digital investment strategy, intended to secure first-mover or fast-follower status in their businesses.[2] To keep up, compliance programs must scale and map to layers of internal, external, and regulatory control requirements.

It's no surprise then that the expanding scope of technology risk can seem overwhelming. The velocity and range of technology change have made traditional technology risk models obsolete and antiquated, exposing institutions to greater risk. There are also emerging technology risk and regulatory mandates to deal with.

At the same time technology risk is no longer just a technology problem—it is an essential part of the overall operational risk framework. That means technology risk managers need to take a fresh look at their current IT operating model and determine how to manage technology changes while attending to the day-to-day running of the department. In our webcast survey, nearly 71 percent of respondents said that they were either planning a technology risk transformation or the transformation was under way.[3]

Corporations require a holistic risk approach that deals with growing technology risk challenges and accelerates strategic value realization and competitive advantage. The goal is an operational risk model built for the accelerated rate of technology change that addresses an organization's appetite for risk while offering increased opportunities for value creation.

Technology risk also needs to be able to adapt quickly and effectively to keep up with the company's evolving strategy, business, and operating models. That requires that risk maintains an open business and technical architecture that enables it to adapt to this changing business, regulatory and operating environment quickly, meaningfully, and commercially.

Given the pace and scope of change, some risk teams will face challenges if they continue to perform tasks as they always have—manually and with limited technology for risk analysis.

**To be agile and adaptable, technology risk needs to ask:**

- Do we know what our critical services are?
- Do we know what our critical assets are?
- What are our risks related to these processes?
- Is there a risk committee to stay aware of the organization's strategy and tactics?
- Do we know what new technologies are being deployed?
- Do we know what acquisitions are being planned?

[2] Source: KPMG 2022 CEO outlook, KPMG International, 2022

[3] Source: KPMG webcast survey, op. cit.

## 02. Transparency, stakeholder engagement, and trust

As risk transformations advance, risk leaders will need to consider the increasing need for transparency to meet stakeholder expectations and build trust. Customers, for example, expect organizations to communicate how they plan on protecting their data and how they have implemented meaningful information security and controls. Regulators are also planning new information security rules that will require greater due diligence, external supervision, and audits.

Organizations can build trust through technology risk transformation by enhancing risk management, reducing the likelihood and severity of adverse outcomes, and promoting transparency. To achieve these objectives, the risk function must change the way it is perceived by the rest of the organization. Here are some essential steps that the risk function should undertake to be perceived as a trusted, strategic partner in decision making:

- Become a trusted and valuable partner in strategic decision making by fostering strong relationships and developing a deeper understanding of the organization's goals and objectives.
- Offer data-driven insights of the organization's risk posture proactively, so that stakeholders can make informed decisions.
- Act as a strategic partner that supports dynamic and proactive decision-making through the identification and prioritization of risks.
- Strive for continuous improvement and become more effective, efficient, and agile to better manage and mitigate risks.

With these capabilities, the risk function will move beyond a defensive, reporting-centric role to a trusted partner that delivers proper safeguards and improves the likelihood of successful implementation and execution of a strategy in line with investor risk appetite.

## 03. Using data, analytics, and insights in the risk function

When it comes to analytics, a wide range of maturity exists among companies. Often, people think using analytics implies highly advanced programs with sophisticated dashboards. In our webcast survey, respondents were evenly split over whether their companies use data effectively.[4] This suggests that many technology risk leaders should be looking at ways to use the data they are gathering. People may assume that data analytics means using highly advanced programs with sophisticated dashboards. But there's a spectrum and several practical ways to use data to better diagnose the health of an organizations risk and control environment.

Utilizing metrics to measure technology risk maturity can be an advantageous strategy for risk leaders. By exploring data and analytics, organizations can evaluate their processes and identify areas of improvement. This helps them address friction points in the process, and refine security and compliance checkpoints. These insights can empower risk leaders to make data-driven decisions that enhance efficiency, security, and compliance measures.

Digital applications provide tremendous amounts of data. And, increasingly, many small applications are generating a lot of data. While in the past the challenge for analytics was not being able to get enough data to work with tools such as GitHub, GitLab, and Jenkins, etc., there is almost an overload of data. The challenge becomes making sense of it all.

From a risk perspective, the benefit of having all this structured data is that you can move beyond monitoring controls once or twice a year to monitoring them continuously and quickly uncover anomalies that need attention. This data can help risk understand where in the environment issues are arising and deploy resources to help manage them.

**Data and analytics in action**

Measuring technology risk maturity can be an important step for risk leaders. By exploring data and analytics, organizations can evaluate their processes and identify areas of improvement. This helps risk leaders address friction points in the process, and refine security and compliance checkpoints. These insights can empower risk leaders to make data-driven decisions that enhance efficiency, security, and compliance measures. As modern technology tool sets are deployed, organizations can leverage the information derived to monitor control environments and scale compliance efforts.

[4] Source: KPMG webcast survey, op. cit.

# 04. Upskilling and embracing new ways of working

Technology risk requires professionals with deep insight into business processes, technology, and compliance. It also requires data scientists, engineers, and even experts in change management, who can help with risk transformation. Building the skills to meet evolving technology risk challenges is a top priority. In our webcast survey, when asked how they envision their service delivery model keeping pace with change, 33 percent of respondents said upskilling existing talent; 25 percent indicated that they are targeting specific skill sets.[5]

Risk teams are challenged to find employees with the right skill sets, including expertise in modern architecture, cloud, and emerging technologies. In addition to recruiting new talent, risk should provide training opportunities to develop skills of existing employees.

Leaders should determine what skills reside on their teams, build a plan to fill in the gaps, and provide training to encourage professional growth and advancement, including rotations in the risk department. For example, employees should learn and be able to harness the emerging technology such as: artificial intelligence, machine learning, and DevOps. Equally important is making sure employees are cared for so they don't burn out. Give them opportunities to develop, but allow them to balance their workload. Technology risk can become a trusted provider of the right subject matter expert with the right skill set when the organization needs it.

Finally, intelligent automation is an option that is gaining traction in risk functions. Technology has advanced tremendously, and digital or virtual agents can carry out increasingly sophisticated tasks. There are many compelling use cases for digital workers to supplement the risk team.

Upskilling talent can take time and comes with its own set of challenges. Achieving flexibility may mean creating a co-sourcing operating model using partnerships that can be called upon to get you through the peaks and valleys.

[5] Source: KPMG webcast survey, op cit.

# 05. Enabling digital acceleration

Digital acceleration drives foundational, emerging, and innovative technologies that embed risk management closer to the point of risk origin while reducing the need to rely on manual efforts. Digital acceleration ultimately enables the business to drive effective risk management into the first line while allowing the second line to deploy enhanced oversight.

During digital transformation, companies typically see new risks as they shift more work to the cloud, and adopt 5G, AI, the internet of things, and the metaverse. According to the 2022 KPMG global tech report, 61 percent of tech leader respondents said that they expect to have embraced most key new tech platforms in the next two years, including Web3 and the metaverse.[6]

Adoption of new technologies can be an opportunity for the business to take a step back and reassess controls and environments to ensure their knowledge of emerging technology is keeping up. Do you have the right controls to mitigate these new risks, and are you taking advantage of pervasive controls across these new technologies?

Making these determinations will, of course, require the right talent with the knowledge and capabilities to make these assessments. But as these technologies become more pervasive, having the right talent alone won't be enough. Organizations will need to better manage risk technologies to also manage controls. One reason: boards want more data. As they become more sophisticated, directors want better reporting on key indicators and various metrics that can now be captured through risk-management technical solutions.

[6] Source: KPMG global tech report 2022, September 2022

# 06. Accelerating technology risk transformation

Technology risk must adapt quickly and effectively to keep up with the organization's evolving strategy, business, and operating models. When looking to modernize the risk function, consider the following:

| | |
|---|---|
| Start small | Launch a pilot with limited scope to get a quick win and gain internal support. |
| Leverage agile approaches | Complete work in sprints to provide flexibility in scope coverage and allow for more real-time reporting and response. |
| Understand the strategic technology modernization and digitization efforts that are under way | Prioritize the technology risk program around these critical success areas. Understand your vision and business objectives before designing new operating models and adopting new risk technologies. |
| Understand which customers and partners are prioritizing digital trust and transparency | Understand the ecoysystem of stakeholders: sales engineering, and product teams, as well as customers and suppliers—The traditional tech risk stakeholder group is evolving and expanding. |

*Client success stories*

# Technology risk transformation in action

Case study

# Protecting software development and operations

A global leader in cloud-based services launched an initiative to assess its software development and operations practices across the product portfolio.

This assessment offered an understanding of the software development lifecycle across many development teams and provided visibility to the organization. The company found that although it had defined change-management standards and established a centralized change management system, several application-level change-management practices were in use across the portfolio and could lead to non-compliance with centralized standards.

KPMG worked with the client's global risk and compliance group, engineering organizations, and application teams to develop a monitoring system to provide visibility into the change-management processes. This was achieved by establishing a codified system of centralized control requirements and working with first-line engineering teams to develop and implement these automated control compliance checks into development processes and pipelines to report on real-time control compliance information.

**This initiative:**

- Generated a prioritized set of change-management design and effectiveness improvements to enhance compliance and code quality.
- Defined a codified, standardized, and machine-ready set of standards, controls, and systematic checks for key controls applicable across the environment throughout the software development life cycle.
- Created a dashboard to allow change managers, auditors, security professionals, and executives to review (in real-time) their teams and product compliance with centralized controls, reducing the risk of unauthorized or unapproved changes being migrated to production environments.

**To achieve these results, KPMG:**

- Worked closely with the client's stakeholders across risk management and application teams to establish a set of criteria to assess and address risk. They reviewed documentation and collected evidence across applications to fully understand current change management processes and effectiveness of controls to build a comprehensive risk assessment with actionable improvement recommendations and efficient monitoring ingestion points.
- Leveraged leading practices, an understanding of advanced change management processes, and deep knowledge of key controls required within change management processes to help the company develop a system to support compliance of these activities real-time, greatly increasing visibility into change management processes and reducing risk for all stakeholders.

Case study

# Harnessing risk quantification insights

For a large foreign banking organization that deals with complex transactions, protecting sensitive data and other enterprise and customer assets is paramount to serving its markets and competing in international finance. However, the processes this organization used to aggregate data and calculate enterprise-wide technology risks were disparate and difficult to industrialize.

The bank wanted to reduce the most risk for the least dollars. But without strong data-driven insights, the organization had only a general understanding of its technology risk exposure and couldn't determine which risk mitigation investments would deliver the greatest returns.

The company turned to KPMG technology risk professionals, who helped the organization leverage deeper risk analysis, improve risk decision-making, and optimize risk reduction activities.

By aggregating the relevant data, the KPMG team saw that the business unit was already mitigating 55.3 percent of its technology risk by simply executing its control portfolio and processes for risk reduction. However, that left an additional 44.7 percent in residual technology risk exposure.

Using the KPMG Tech Risk Intelligence solution, additional risk and control activities were prioritized through the tool's optimization engine by simulating over 100,000 risk reduction scenarios and their financially backed risk decisions. If undertaken by the business unit, the priority activities would reduce the most risk for the least investment.

Based on these initial results, the organization was able to further develop its risk quantification capability, which will enable it to consistently prioritize and optimize its risk reduction investments and improve future enterprise-wide risk decision-making.

After the additional risk and control activities were prioritized through the KPMG Tech Risk Intelligence tool's optimization engine during the business unit pilot, the company was able to realize the following benefits:

- Technology risk mitigated by existing controls and processes: approximately 55 percent
- Residual technology risk: nearly 45 percent
- Investment in existing processes and controls: nearly $4 million
- Technology risk mitigated by investment: more than $13 million
- Risk reduction return: 242 percent.

Case study

# Cloud migration and assessments, monitoring, and testing

A commercial bank was one of the first financial institutions to adopt a cloud environment. As the first adopter, the company faced unique risks and challenges to the organization to maintain SOX compliance. Specifically, it was unclear how the cloud migration would affect the organization's ability to maintain SOX compliance. Moreover, the company's professionals lacked the subject matter expertise to translate the on-premises control to the cloud provider. An added complication was that the migration timing necessitated a control strategy and project management.

KPMG assisted the company in developing data migration and systems development lifecycle controls specific to each unique application migration strategy and supporting on-premises to cloud migration of SOX applications through the translation of on-premises control coverage to the cloud's unique infrastructure, as well as migration timing impacts on stub period testing.

As a result of these efforts, the company migrated SOX applications to a third-party cloud with minimal disruption. It established formalized and tested controls within the cloud to mitigate emerging risk. After deployment, the bank faced numerous challenges and regulatory action (MRA/MRIAs), which were the result of heightened regulatory scrutiny. The bank continued to struggle with a knowledge gap due to constant employee turnover as well as an inconsistent application of controls testing methodology and due diligence.

KPMG worked collaboratively with the client to improve the efficiency of obtaining information and setting up parallels across various workstreams. Our team leveraged institutional knowledge to translate legacy control objectives into evolving processes, policies, and infrastructure as code. We analyzed the client's IP ranges, VPCs, and high-risk API actions to identify inconsistently-applied restrictions. Additionally, we performed MRA/MRIA compensating controls and impact analyses to aid in responding to regulators. Our ongoing cloud assessments included evaluating governance, identity and access management, cryptography, key management, and data protection measures within the organization. Through these efforts, KPMG helped improve the client's overall cloud security.

**The actions yielded the following benefits to the bank:**

- Adherence to regulatory requirements through demonstration of control effectiveness
- Identification of an undetected SSH key cyber event within the bank's environment and the redesigning of controls to mitigate SSH key risk and data loss risk within the cloud
- Identification and remediation of systematic issues within the bank's core utility to monitor and enforce compliance across cloud services/resources, and concise action plans were created to close gaps within their cloud risk and controls portfolio.

# Getting going

# Getting going

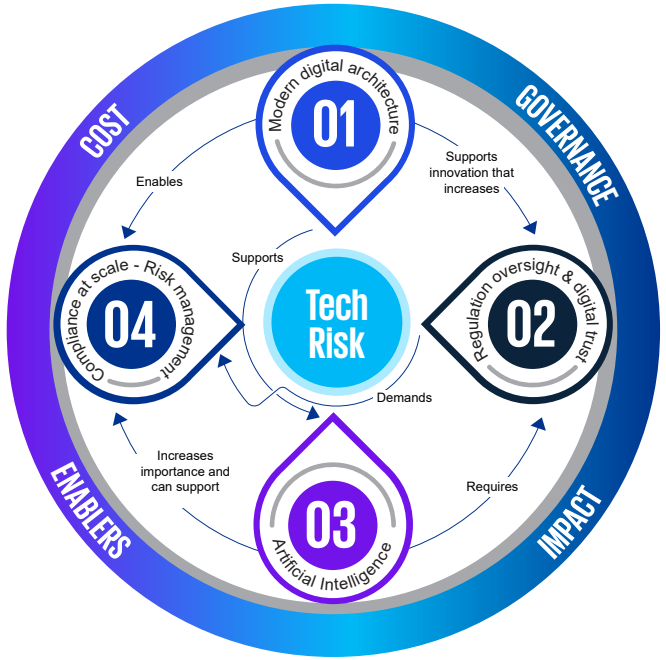
With technology transformation, digitization, and cloud migration, businesses continue to move forward.

Tech risk must keep up with modernization (business transformation, digitization, and cloud migration), while facing new and continuing challenges. AI bias is becoming increasingly concerning with the rise of new AI tools. Managing technology transformation projects is still a significant challenge, while tech compliance is also a concern with new regulations on the horizon.

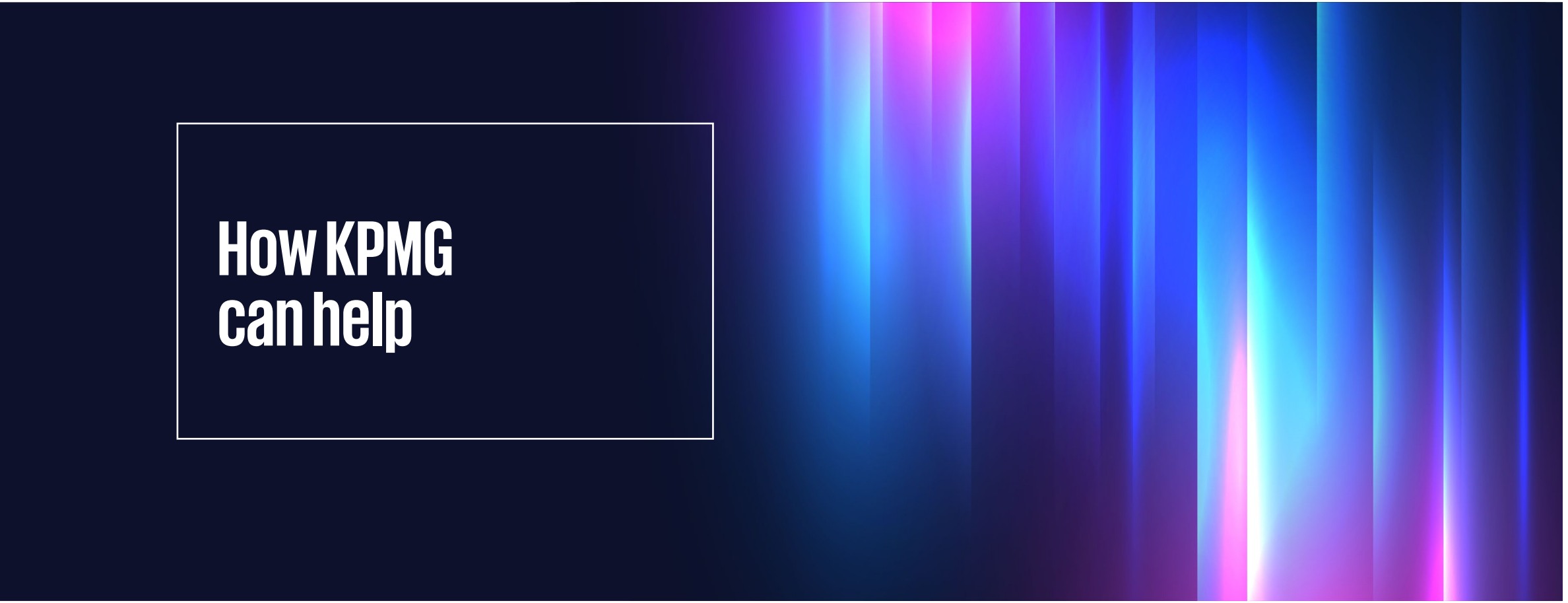
Keeping pace will require a transformation within technology risk to align it with the business's modernization. Better tools and technology, greater use of data and analytics, as well as automation and digitization, will be essential to manage risk and create value.

Underlying this transformation must be a renewed focus on transparency and trust among stakeholders, which is now a competitive necessity. And attracting and retaining the right talent to bring about and maintain this transformation will require risk management to accommodate the new ways of working, like remote workforces and other benefits.

While the challenges facing risk management in an increasingly complex business environment can seem daunting, they can also motivate your team. A measured and planned approach will result in a risk organization that is proactive, strategic, and an increasingly essential partner with the business.



# How KPMG can help



# How KPMG can help

Technology adoption is critical to any organization's competitiveness, but also exposes the organization to risk. KPMG can help turn that risk into opportunity and help build stakeholder trust.

Our Technology Risk services team has deep experience supporting organizations in managing technology risk in the most complex, fast-changing, and global business environments.

With more than 6,000 global practitioners, we deliver technology risk services to hundreds of client organizations with our network of member firms worldwide.

We also help organizations build compliant, effective, efficient, and scalable technology risk services with technology and automation to enable the technology risk program.

## The trusted imperative

In every sector, and in every transformation initiative, stakeholder trust is an indispensable ingredient. Whether you are optimizing a single function or connecting the entire enterprise, you can inspire stakeholder trust at every turn. As the ultimate business enabler, trust is your ticket to responsible growth, bold innovation, confident decision-making, and sustainable advances in performance.

# Forces of risk for modern technology

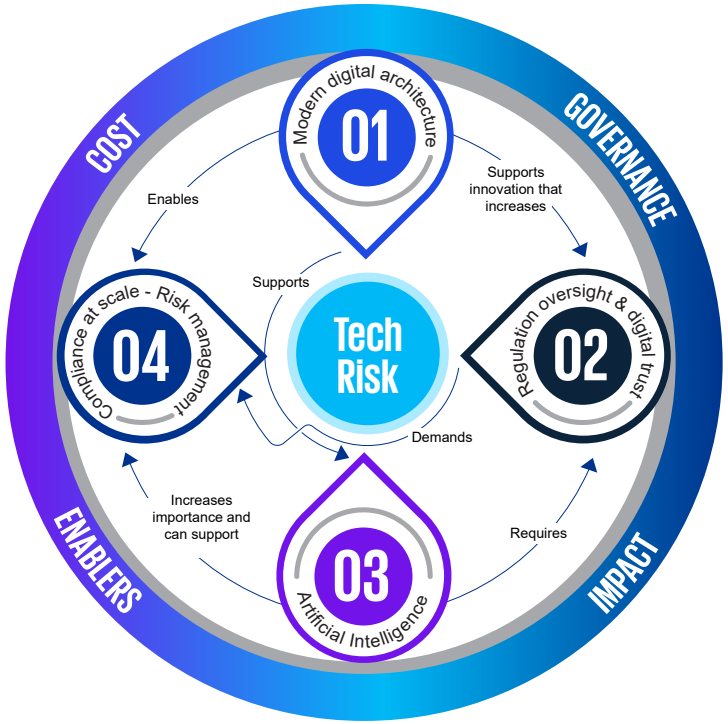
Evolving changes in the business landscape can create vast opportunities for the risk function to provide insights into revenue generation and new business models, but these forces may also introduce new challenges such as regulatory compliance and unique risk mitigation considerations.

To overcome these obstacles, businesses can harness cutting-edge technologies in line with cloud platforms, artificial intelligence, and digital architecture to scale and meet regulatory mandates while maintaining stakeholder trust.

**1**

Digital tools, solutions, and processes that introduce new revenue streams, optimize operations, and demand cutting edge risk treatment. Cloud platforms combine with loosely coupled services to scale on demand. These advances demand cutting-edge risk treatment and create the opportunity to treat compliance as code.

- DevSecOps (controls observability)
- Cloud governance
- APIs and microservices
- Move to cloud




**2**

The evolving global regulatory landscape mandates new requirements regarding digital technology. Customer and public trust rely on safeguarding data and privacy. Businesses can "assess once and report many times" to address layers of regulatory and third-party risk.

- Regulatory readiness
- Security standards and certifications
- Technology risk management
- Digital trust culture

**3**

Artificial intelligence is changing the art of what's possible through simulated human intelligence making abstract decisions.This powerful technology can transform how businesses operate, innovate new consumer products, and create new security challenges. It can also be an ally in managing the risk landscape but requires unique risk mitigation and compliance considerations for use.

- Low code and automation
- Artificial intelligence
- Quantum computing
- Big data

**4**

Compliance programs must scale and map to layers of internal, external, and regulatory control requirements. Businesses can tap into digital architecture and automation to provide sweeping coverage across the risk landscape. Compliance programs can adopt engineering principles to deploy a tech-enabled risk management program.

- Unified control frameworks
- Risk workflow tools
- Continuous controls monitoring
- KRI and KPI libraries

# The technology risk management team

Our multidisciplinary teams have deep risk management and technology skills, with specialization in key industry and functional areas, including:

**Technology Risk Modernization**

- Technology risk capability transformation
- Digital transformation governance, risk and control

**Technology Trust**

- Technology audit
- Technology controls
- Technology risk assessment and Intelligence
- Technology regulatory response
- Technology compliance at scale

Learn more here

# Authors


**Jill Farrington**
*Partner, Technology Risk Service Network Leader*
KPMG LLP
jfarrington@kpmg.com

Jill has over 20 years of experience providing information technology consulting and assurance services to clients across a variety of industries.

**Emily Frolick**
*Partner, US Trusted Imperative Leader*
KPMG LLP
efrolick@kpmg.com

With a focus on risk and regulation powered for the digital era, Emily helps clients reframe the way they look at risk management by thinking through strategic, proactive ways to build trust and generate value across their entire business ecosystem.

**Beth McKenney**
*Principal, Technology Risk Modernization COE Leader*
KPMG LLP
bmckenney@kpmg.com

Beth is an effective leader with over 17 years of experience helping clients manage risk, deliver value through IT internal audit, and strengthen their governance capabilities.

**Vivek Mehta**
*Partner, Technology Risk Solutions Leader*
KPMG LLP
vivekmehta@kpmg.com

Vivek assists clients in IT Risk Management specifically IT Regulatory management, IT Governance & Strategy and IT controls implementation.


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**