KPMG

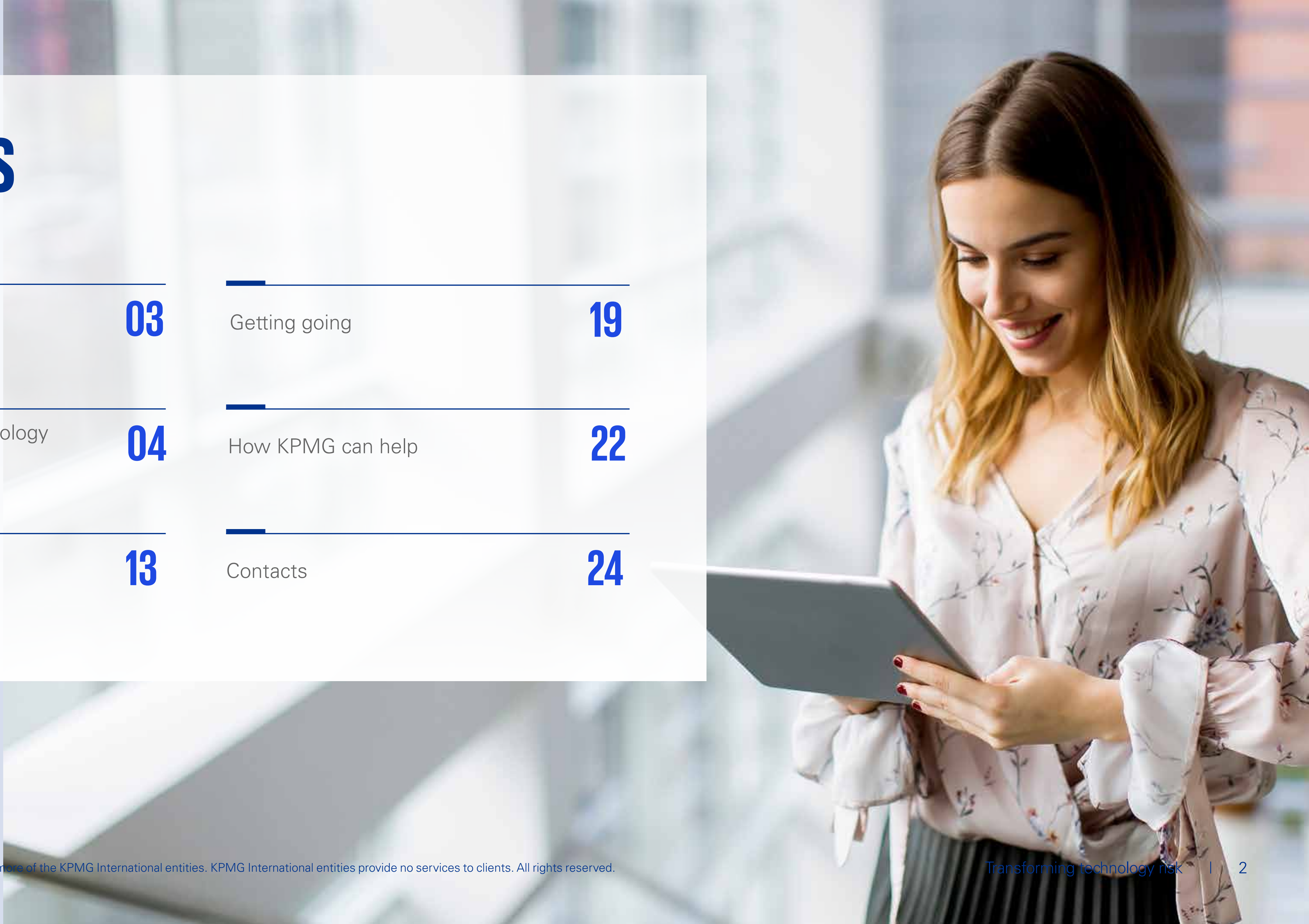
Transforming technology risk

Managing technology risk to
help build stakeholder trust

KPMG International

kpmg.com/technologyrisk

Contents



Introduction

Most organizations are modernizing their critical information technology — to help 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. The KPMG 2023 Global CCO Survey reveals that 56 percent of CCOs are planning to increase technology budgets for the ethics and compliance function.[1] However, in many organizations technology risk knowledge remains limited or may not be keeping pace with innovation. With that in mind, the following trends should be considered:

- Businesses are transforming and modernizing the technology stack, which means that technology risk approaches and controls should also adapt.
- Threats to technology are becoming more complex and sophisticated, so risk management approaches must transform and be multilayered and agile.
- Increasing technology trust and transparency with stakeholders is 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.
- Technology risk knowledge is limited or not keeping pace with innovation; how companies manage technology risk must adapt to the new ways of working to close the talent gap.
- Technology is crucial for sustainability, covering areas such as reducing carbon footprint, promoting inclusiveness and achieving balanced governance. It can speed up the transition by providing new sources of innovation, but also creates risks to tackle.

The future of risk is shifting away from a regulatory-driven ‘protect agenda’ to one where businesses leverage risk to enable organization-wide growth and optimization. Boards and shareholders are looking for technology risk teams to be strong partners with the business, leveraging regulatory-focused investments to drive business results. 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.

Based on KPMG member firms 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. This report explores each step and shares key insights into how organizations can transform their technology risk.

These key steps 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; investing in digital acceleration.
4. Reducing technology risk in ESG transformation.
5. Upskilling and embracing new ways of working.
6. Enabling digital acceleration.
7. Accelerating technology risk transformation.

[1] 2023 Global CCO Survey, KPMG International, 2023.

Seven steps toward technology risk transformation

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

Businesses continue to prioritize digital investment, with generative AI (genAI) being a top priority. Business leaders are recognizing the immense potential of genAI and are keen to explore this technology. In the KPMG 2023 CEO Outlook, 70 percent of respondents indicated that they are investing heavily in genAI as their competitive edge for the future, with most (52 percent) expecting to see a return on their investment in three to five years. In fact, increased profitability was cited as the number one benefit of implementing genAI within an organization (22 percent).[2]

To keep up, compliance programs must scale and map to layers of internal, external and regulatory control requirements. It's no surprise 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's 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. Especially as 96 percent of digital leaders say their technology function can help the enterprise to confidently explore the potential of emerging technologies, according to the KPMG Global tech report 2023.[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 increased 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 likely 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 should ask:

- Do I have a clear understanding of critical services?
- Do I know what my critical assets are?
- What are the risks associated with these processes?
- Is there a risk committee in place to monitor the organization's strategy and tactics?
- Am I aware of any new technologies being implemented?
- Do I have knowledge of any planned acquisitions?

[2] KPMG 2023 CEO Outlook, KPMG International, 2023.

[3] KPMG Global tech report 2023, KPMG International, 2023.

02. Transparency, stakeholder engagement and trust

As risk transformations advance, risk leaders should consider the increasing need for transparency to meet stakeholder expectations and build trust. The KPMG Global tech report 2023 reveals that nine in ten digital leaders believe they must be more proactive about integrating trust, security, privacy and resilience into technology roll-outs.[4]

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 likely require greater due diligence, external supervision and audits.

Organizations can build trust through technology risk transformation by enhancing risk management, working to reduce 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 help be perceived as a trusted, strategic partner in decision-making:

Foster strong relationships and develop 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 active 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 can be positioned to 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.

[4] KPMG Global tech report 2023, KPMG International, 2023.

Artificial Intelligence Act

The European Union Artificial Intelligence Act (AI Act), which sets out regulations for artificial intelligence, serves as an example of how regulators are addressing customer demands for data security through increased transparency. Its objective is to ensure trustworthy and ethical AI systems. The act introduces measures such as mandatory due diligence, external supervision and audits for high-risk AI applications, contributing to the secure handling of customer data. The AI Act is currently in the legislative process and is expected to be finalized and implemented in 2026.

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

Companies vary widely in their level of analytics maturity. Most organizations have recognized the value of data and are well on their way in executing their data strategies. But they still have more to achieve, especially around the integration issue of data sets not working together across an organization.

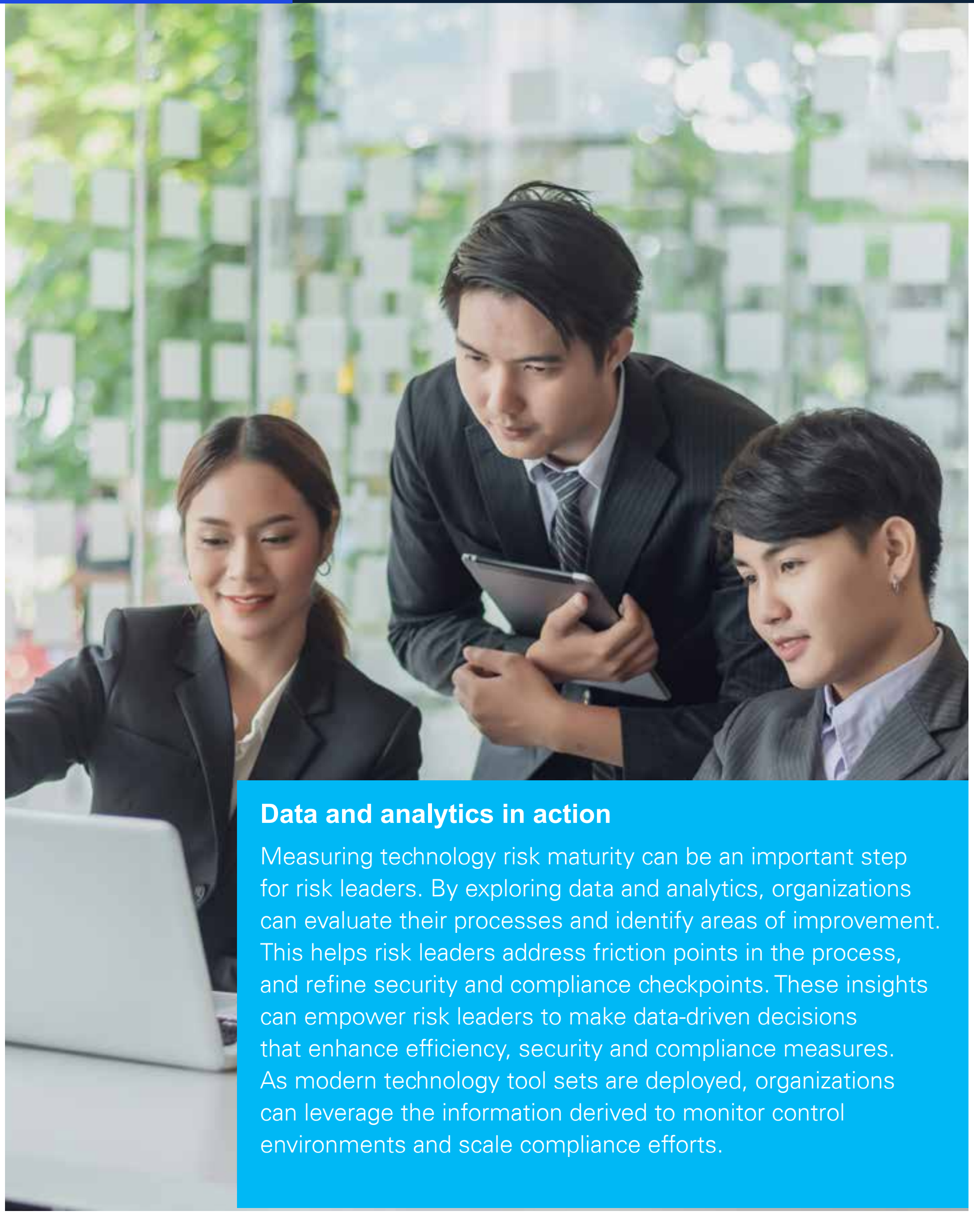
According to the KPMG Global tech report 2023, 68 percent of organizations report that their work with data and analytics has gone beyond the experimental phase, while only 17 percent describe their approach to data and analytics as 'embedded' — fully integrated into daily operations and is generating returns.[5] This suggests that many technology risk leaders should embrace a mindset of continuous improvement to enhance how they use the data they are gathering.

Often, people assume using analytics requires highly advanced programs with sophisticated dashboards. But there's a spectrum and several accessible ways to use data to better diagnose the health of an organization's 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 generate vast amounts of data, and even small applications can produce a significant quantity of data. In the past, the challenge for analytics was not getting enough data to work with tools; there's almost an overload of data now. Organizations face two challenges — first, data quality. If the data collected is not sufficiently structured or consistent, it becomes useless or requires advanced tools to cleanse, structure or perform quick checks. The second challenge is to understand the data and to use it to make informed and smart business decisions.

From a risk perspective, the expected 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.

[5] KPMG Global tech report 2023, KPMG International, 2023.

04. Reducing technology risk in ESG transformation

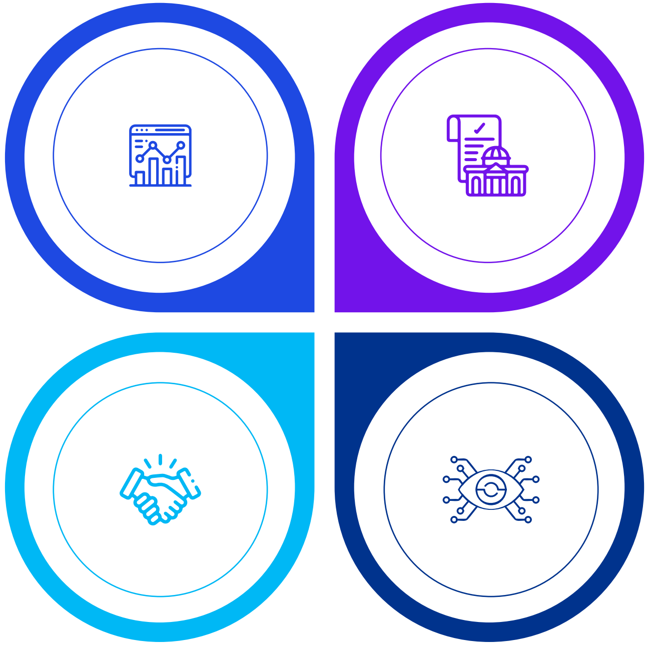
The potential for technology to help businesses tackle environmental challenges within ESG is significant. Companies are implementing innovative measures to reduce carbon emissions, such as adopting more efficient working practices or improving their carbon emissions reporting accuracy. Twenty-five percent of business leaders also recognize the great impact ESG will have on their customer relationships over the next three years, while 17 percent believe that it will enhance their brand reputation.[6]

As ESG requirements shift from being merely reporting responsibilities to driving change and creating value within an organization, technology will become increasingly vital for achieving business success. The KPMG Global tech report 2023 found nearly half of the respondents (48 percent) said that advancing their ESG priorities will be a primary innovation goal for their technology functions over the next two years.[7]

However, this transformation is not without risks, as it requires a paradigm shift involving regulatory obligations, new business models, consideration of new environmental and social performance metrics in decision-making and increased systemic risks to resources.

To effectively manage risks on your sustainability journey, consider these four key elements.

Key elements for sustainable transformation



Tools and data

Data is the foundation of ESG reporting. It should be the first element to secure before starting any transformation program. ESG tools support data collection, internal control monitoring and ESG reporting.

Process and governance

Governance body and operational processes required for your ESG reporting are to be defined at the early stages of your ESG project.

Third parties

Many IT third parties are involved in the production process and monitoring of non-financial reporting elements (data collection, analysis, production of KPIs). Obtain and provide assurance on the internal controls of these third parties.

Internal controls

Beyond the statutory obligations, robust internal controls is a way to enhance your ESG transformation. The assurance you can provide is critical for your activity and business partners.

[6] KPMG 2023 CEO Outlook, KPMG International, 2023.

[7] KPMG Global tech report 2023, KPMG International, 2023.

The management of ESG data is still in its early stages for most companies. The data is often unavailable, unconsolidated, unclean, and unsuitable for automation, among other issues. Furthermore, ESG data will not only be necessary for compliance purposes, but stakeholders will likely also require it for their reporting. Providing complete, accurate and easily manageable ESG data could be a competitive advantage as regulatory obligations and societal demand for transparency increase. The KPMG 2023 CEO Outlook found that more than two-thirds (69 percent) of global business leaders have fully embedded ESG into their business as a means to create value, yet 68 percent indicate that their current ESG progress is not strong enough to withstand potential scrutiny from stakeholders or shareholders.[8]

Digitizing your processes is essential in automating your ESG reporting. A critical step towards achieving this is implementing an ESG tool in your IS cartography/environment. Sustainability performance management should be treated as a transversal aspect, similar to financial information, to help ensure a truly positive impact rather than just an acceptable level of efficiency that keeps costs under control.

When implementing a new reporting system, processes should be adapted. This is especially true for ESG data, as much of the data collection (including CO^2 emissions, biodiversity impacts, social impacts, water and energy usage, etc.) is specific to local conditions and can only be accurately captured at the operational level. This requires effective governance to coordinate efforts across the organization.

Alongside the development of reporting, improving the internal controls of ESG reporting is crucial to provide reasonable assurance to stakeholders and regulators. In addition to addressing increasing regulatory obligations (where ESG reporting is expected to be as closely monitored as financial reporting in the future), a strong assurance mechanism enhances the value of your data for stakeholders. Furthermore, a robust internal controls system is necessary for making informed decisions and achieving impactful performance management.

[8] KPMG 2023 CEO Outlook, KPMG International, 2023.

05. 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 specialists in change management, who can help with risk transformation. Building the skills to meet evolving technology risk challenges is a top priority.

According to the KPMG Global tech report 2023, more than a third (36 percent) of organizations are concerned about the lack of skills within the organization.[9]

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 emerging technology such as: artificial intelligence, machine learning and DevOps.

Co-sourcing partnerships play a crucial role in minimizing employee burnout. By gaining short-term access to niche expertise and skill sets, technology risk functions can give full-time employees the space and time to balance upskilling with their daily workloads.

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.

[9] KPMG Global tech report 2023, KPMG International, 2023.

06. Enabling digital acceleration

Digital acceleration provides the opportunity to bridge the gap between operation and risk, by providing fully embedded controls and security mechanisms. 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. The KPMG Global tech report 2023 found more than half (57 percent) of respondents believe that AI and machine learning, including genAI, will be important in helping them achieve their business objectives over the next three years. In addition, 68 percent say these technologies will be vital in helping them to achieve their short-term business goals.[10]

Adoption of new technologies can be an opportunity for the business to take a step back and reassess controls and environments to help 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 should better manage risk technologies to also manage controls. One reason: stakeholders want more data. As they become more sophisticated, stakeholders want better reporting on key indicators and various metrics that can now be captured through risk-management technical solutions.

[10] KPMG Global tech report 2023, KPMG International, 2023.

07. Accelerating technology risk transformation

Technology risk management must not fall behind the ongoing evolution of operating models, market conditions and regulatory developments. According to the KPMG Global tech report 2023, almost half of organizations (46 percent) say their technology function lacks the governance and coordination it needs to effectively support transformation initiatives.[11]

The process of transforming and modernizing the technology risk function is tailored to each company's unique roadmap, challenges, priorities and resources. To help with this journey, here are some recommendations and suggestions to consider.

1 Clearly understand the business strategy, purpose and values before making changes

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.

2 Start small

Launch a pilot with limited scope to get a quick win and gain internal support.

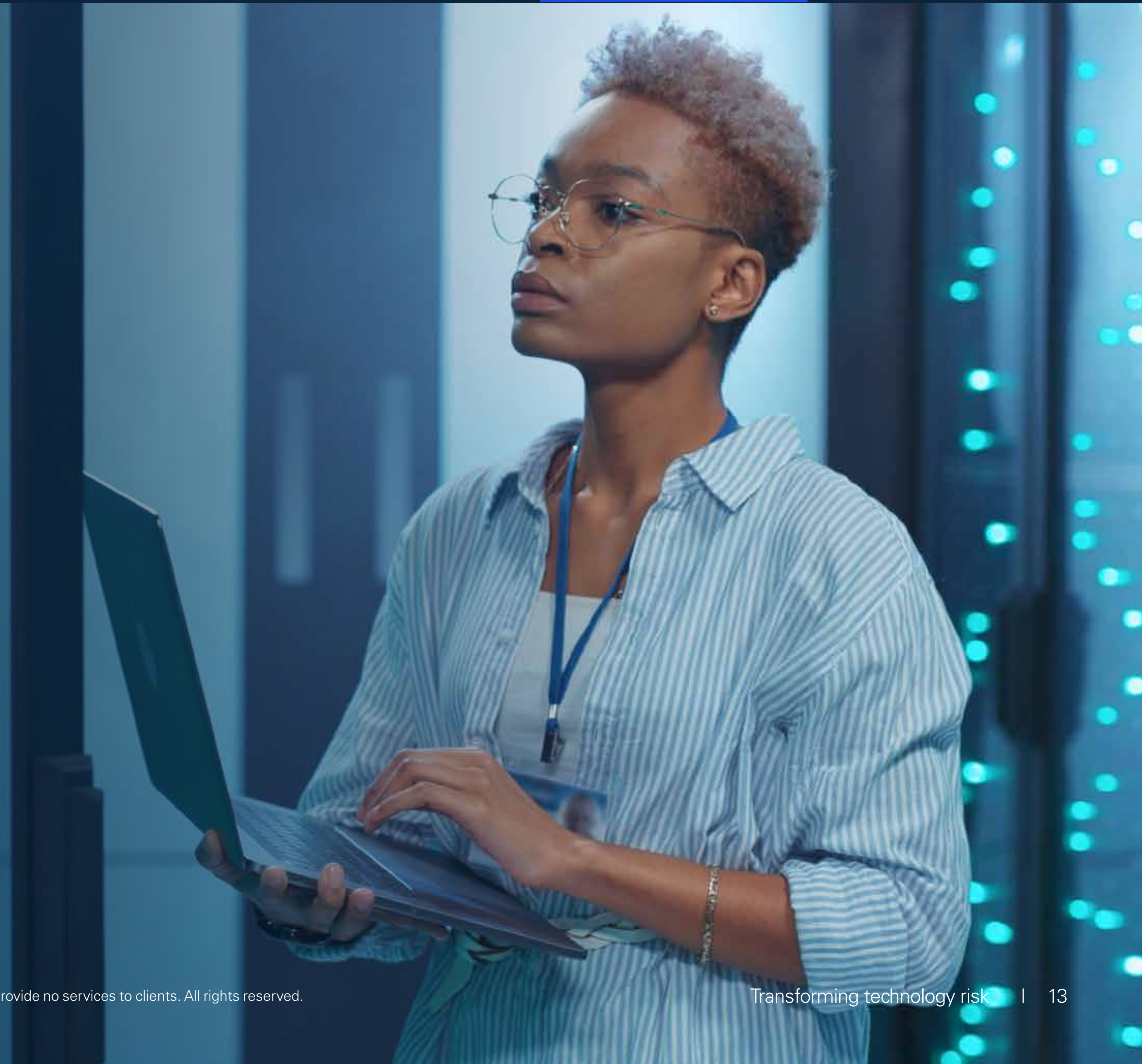
3 Leverage agile approaches

Complete work in sprints to provide flexibility in scope coverage and allow for more real-time reporting and response.

4 Understand which customers and partners are prioritizing digital trust and transparency

The traditional technology risk stakeholder group is evolving and expanding. Understand the ecoysystem of stakeholders: sales engineering and product teams, as well as customers and suppliers.

[11] KPMG Global tech report 2023, KPMG International, 2023.



Client success stories

Technology risk transformation in action

Case study

Taking security and risk controls to a new level in financial services

A Belgium-based global financial services company, the world's largest central securities depository, was facing the challenge of increasing efficiency and reducing IT risk for clients across various business units. With client assets worth around US$39 trillion, the company specializes in managing domestic and cross-border securities transactions, as well as global securities trade settlements. To transform its IT governance and controls, the organization turned to KPMG in Belgium for assistance.

As a leading provider of Financial Market Infrastructure (FMI) services, and amid the need for reliable access to broad IT capabilities, it was deemed critical to modernize the IT governance and controls framework. The company's IT organization provides mission-critical production and project delivery services to diverse business entities. Operating in a strongly regulated environment and facing increasing control requirements, IT capabilities serve as the first line of defense and the client needed a robust risk and control environment providing evidence.

In addition, the client's IT organization had embarked on an IT transformation initiative amid evolving business needs, including faster time to market, enhanced service quality and ongoing innovation. The transformation involved changing several practices, processes and tools, including the introduction of an agile way of working and deployment of ServiceNow to support IT operations in a first step, before evolving to cover most IT-management processes. To improve enterprise risk and control processes enterprise-wide, implementing ServiceNow's Integrated Risk Management (IRM) module was essential.

The mission to implement a new IT governance and control framework needed to cover IT strategy and investments, IT operations, risks and controls, performance and resourcing. The existing IT control environment was based on the COBIT framework. Descriptions of control objectives and activities, and evidence of their execution, lacked consistency and robustness and the ServiceNow IRM module (formerly known as Governance, Risk and Compliance or GRC) would serve as a single repository to manage control objectives, activities, evidence, KPIs, status and risk management.

The business also needed to implement ISAE3402 and SWIFT CSP regulations and controls while remaining compliant with CSDR and CPMI-IOSCO. This led to the need for regulatory mapping, in parallel with risk assessment for defined IT processes. The company also required professional assistance to innovate other critical areas of operation, including alignment with all regulations, plus the control design for each security domain and implementation of ServiceNow IRM with dashboards and reporting capabilities.

The organization turned to KPMG in Belgium's multidisciplinary team offering crucial experience in IT governance, risk and compliance, cybersecurity and the ServiceNow IRM module. Our professionals were also responsible for ensuring that key resources from the client's IT governance and controls (ITGC) project were available on this latest initiative.

Bringing KPMG Powered Risk and ServiceNow experience together for success

KPMG professionals led by our Belgium team collaborated closely with the client, combining essential ServiceNow IRM tools and capabilities with timely insights gained from the KPMG and ServiceNow global alliance. Crucial to success on this project was the guidance of our certified ServiceNow IRM specialists in delivering smart insights for effective enterprise-wide project management.

Case study

Our application of KPMG Powered Enterprise Risk was also critical. As the client clearly understood, risk in today's dynamic and hypercompetitive business environment must be continuously reframed to enhance organizational strategy, decision-making and risk management.

KPMG Powered Enterprise Risk is an outcome-driven, functional transformation solution featuring in-depth industry expertise. Our approach is built on years of KPMG firms' leading-practice knowledge of business processes, collection of assets and accelerators, delivery methodologies, operating models and extensive industry experience, together with a deep understanding of today's leading technology platforms.

KPMG Powered Enterprise Risk proved instrumental in setting up the ServiceNow IRM solution, including the Powered Risk Target Operating Model (TOM) to embed ServiceNow IRM capabilities. It links the technology layer (ServiceNow configuration) to the process layer for risk management optimization, as well as the people layer defining roles and responsibilities, while also offering timely insights on performance and innovative reporting possibilities.

Our specialists also applied other KPMG Powered assets to define IT risks and controls. All IT and cybersecurity innovations started with the TOM to accelerate the process. Key to our success was the KPMG multidisciplinary approach, combining our cross-border expertise on the financial sector, the regulatory environment, risk and controls, IT general controls, cybersecurity and ServiceNow solutions.

This project has been referred to by the client's CISO as one of the company's most-successful risk projects to date. Our success prompted the client to engage KPMG in Belgium specialists to also build and embed a new security-control framework, focusing on cyber domains. Enhanced security controls were created based on the CIS Critical Security Controls Version 8 framework — a prioritized set of safeguards to combat today's increasingly sophisticated and dangerous cyberattacks.

The following key benefits were delivered to the financial services company:

- One security-control framework or control library that incorporates all control requirements across the company's security domains and in-scope regulations.
- The potential to rationalize controls that address multiple requirements and regulations, enabling the ability to 'execute once, report many.'
- A centralized platform to manage the security controls, integrated with IT and operational risk-control libraries.
- Harmonized processes across teams and the broader organization.
- Instant automated notifications to risk and control owners for rapid manual control execution as needed.
- Real-time insights into current compliance levels for specific regulations related to individual processes and departments.
- Lower effort and put-through time to demonstrate compliance to authorities, using the linkage between authority documents and control performance.
- Reduced control costs using a systematic and consistent approach to manage the lifecycle of all controls and policies.
- Seamless and enhanced insights on compliance across the organization.
- Improved compliance and risk remediation and minimal disruption of business operations by facilitating and tracking corrective actions in a timely manner.
- Lowering the bar for first-line adoption of GRC regulatory practices by focusing on user-friendliness, approachability and automation.

Case study

Harnessing quantification insights to mitigate US$13m of tech risk

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 the technology risk professionals in KPMG in the US, 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 can enable it to consistently prioritize and optimize its risk reduction investments and improve future enterprise-wide risk decision-making.

Returns achieved from following KPMG in the US professionals' advice:

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

Case study

Transforming risk and compliance for a bold new era of challenges

A global insurance company based in Hong Kong (SAR), China, with over US$63 billion in assets, required expert support on an unprecedented initiative to transform its enterprise risk and compliance capabilities. The organization needed specialists to collaborate on a transformation program featuring the adoption of ServiceNow IRM technology. The challenge included assistance with overall program management, data migration and ServiceNow technology implementation for key business functions such as: risk management (including incidents), controls, policy management, regulatory change, business continuity management (BCM), metrics, dashboards and reports.

KPMG in China impressed the company's risk and compliance leaders with our market-leading understanding of the future of risk – combined with deep industry knowledge and our timely insights on how best to meet the client's needs through the KPMG and ServiceNow global alliance. KPMG China professionals collaborated closely with the insurance giant to develop a comprehensive strategy, utilizing KPMG Powered Enterprise Risk methodology and Powered assets specifically tailored for the ServiceNow implementation.

The KPMG China team took advantage of its technical expertise on ServiceNow products to create a simple and highly effective new ecosystem that provides modern, future-ready risk and compliance capabilities — including functional role-based processes and enhancement of the client's existing risk and compliance frameworks.

KPMG in China also leveraged previous experience working on multiple projects with the client and its Risk and Compliance department, which provided KPMG professionals with critical knowledge of the firm's regional strategy and operations within the hypercompetitive global insurance and financial-services sector. The KPMG Delivery Network (KDN) provided crucial support through our ASPAC team to strengthen delivery capabilities when onshore capabilities proved challenging to meet the transformation project's needs.

The following key benefits were delivered to the insurance company:

- Strategic and operational risk integration across risk and compliance and throughout the client's global business, leading to increased risk awareness and improved transparency in today's fast-evolving digital economy.
- Streamlined processes featuring fewer workflow steps and enhanced efficiency through increased reliance on modern automation tools. Time-saving new workflow configurations now provide automated closure of issues and the setting of key dates using system-driven prioritization — all serving to enhance user experiences.
- Fast and reliable user access to self-service features through the ServiceNow IRM portal.
- Migration of key processes to ServiceNow.

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.

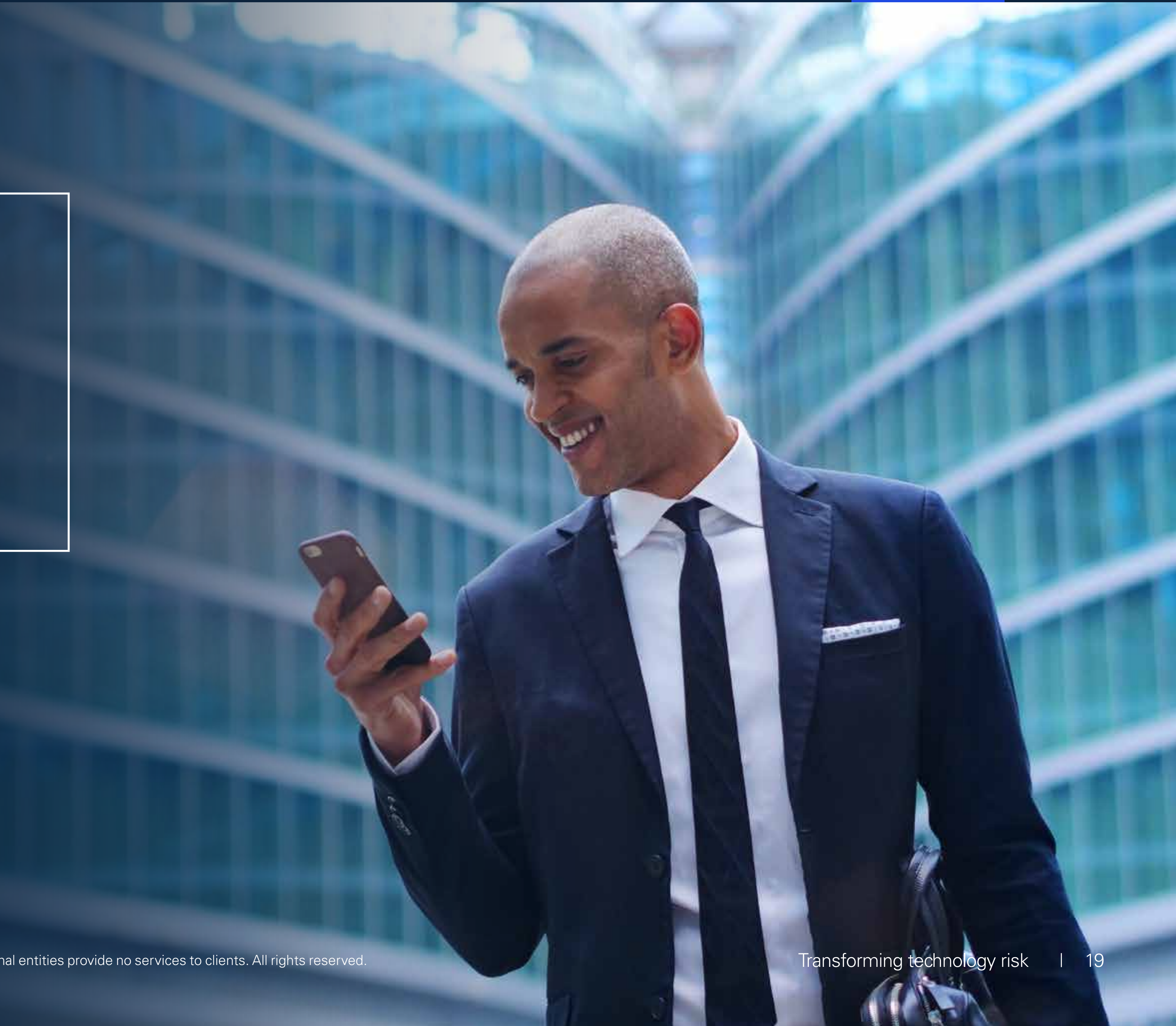
KPMG in the US helped the company create controls for data migration and systems development lifecycle tailored to each application's unique migration strategy. This included moving SOX applications from on-premises to the cloud, which required translating control coverage from on-premises to the cloud's infrastructure and considering the timing of the migration's impact on 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 in the US 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 in the US 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

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 leading technologies in line with cloud platforms, artificial intelligence, and digital architecture to scale and meet regulatory mandates while maintaining stakeholder trust.

1

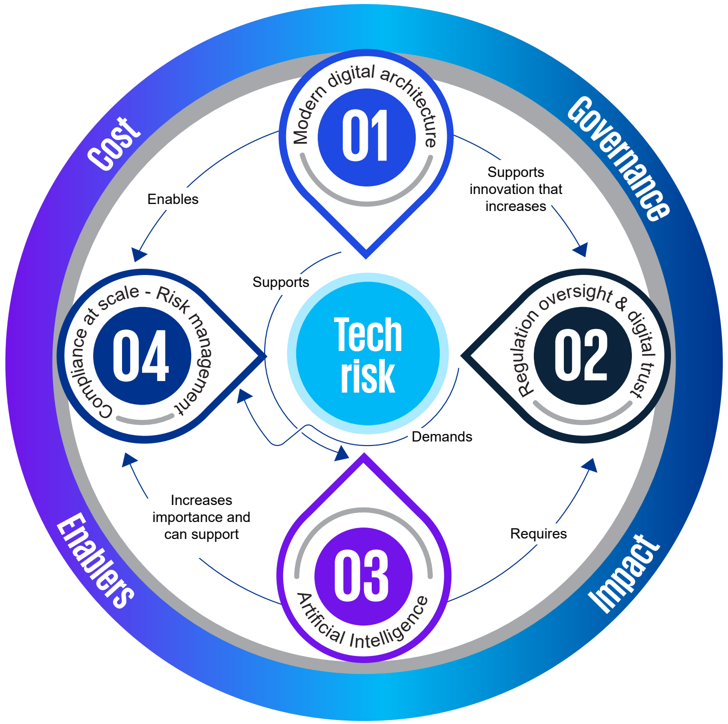
Digital tools, solutions and processes that introduce new revenue streams, optimize operations, and demand cutting edge risk treatment. Cloud platforms combine with loosely coupled services to scale on demand. These advances demand leading risk treatment and create the opportunity to treat compliance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

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

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


Cost
Governance
Enablers
Impact
Tech risk
01
Modern digital architecture
02
Regulation oversight & digital trust
03
Artificial Intelligence
04
Compliance at scale - Risk management
Enables
Supports innovation that increases
Supports
Demands
Increases importance and can support
Requires

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

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

Getting going

Technology 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 likely 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, are expected to 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 expected 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 can result in a risk organization that is proactive, strategic, and an increasingly essential partner with the business.

How KPMG can help

How this connects to what we do

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.

Tech risk transformation and modernization can help build stakeholder trust in existing processes and technologies. This will provide reasonable assurance over the As-Is and allow decision-makers to focus on developing and expanding their business.

The KPMG technology risk services professionals have deep experience supporting organizations in managing technology risk in the most complex, fast-changing and global business environments. Our multidisciplinary teams have deep risk management and technology skills, with specialization in key industry and functional areas.

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

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

Learn more at: kpmg.com/technologyrisk

The KPMG digital transformation suite

KPMG firms are helping global businesses in various sectors embrace a new era of opportunity in the digital economy. From strategy to implementation, KPMG professionals can help make the difference on your transformation journey. Together, we can help transform your current business model to drive future competitiveness, growth and value. **KPMG. Make the Difference.**

KPMG transformation journey

KPMG Connected Enterprise
Rebuild your business around your customers.

KPMG Powered Enterprise
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

Laurent Gobbi
Global and EMA Technology Risk Leader
KPMG International and Partner
KPMG in France
lgobbi@kpmg.fr

Jill Farrington
Americas Technology Risk
Leader and Partner
KPMG in the US
jfarrington@kpmg.com

Henry Shek
Asia Pacific Technology
Risk Leader and Partner
KPMG China
henry.shek@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

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.

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.

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 detail about our structure please visit kpmg.com/governance.

Publication name: Transforming technology risk | Publication number: 139092-G | Publication date: November 2023