Risk and Compliance 2026

Refining Oversight for a Volatile, AI-Driven World

April 2026

By Katharina Hefter, Julia Gebhardt, Malgosia Zegar, Florian Meier, Anne Kleppe, Biljana Bajic-Bizumic, Johannes Große, Sarah Lichtblau, Bernhard Gehra, Matteo Coppola, Pierre Roussel, and Abhinav Bansal

BCG

Table of Contents

Executive Summary

In 2026, risk and compliance leaders are navigating expanded export controls, tighter sanctions enforcement, widening regulatory divergence, and growing data-localization requirements. At the same time, generative and agentic AI systems are creating new opportunities to strengthen foresight, enhance coordination, and scale **risk and compliance** management capabilities.

This report provides insights into how leading organizations are adapting in this new landscape. It draws on proprietary data from more than 100 senior risk and compliance executives across six industries and seven regions. **(See "About the Study.")** With more than two-thirds of participating companies ranging from $0.5 to $5 billion in annual revenue and 50% employing over 10,000 people, the findings reflect the realities of global organizations operating at scale.

Exposure is concentrated in three interconnected domains:

- **Geopolitical and regulatory divergence**, which increasingly forces trade-offs between compliance certainty, cost, and market access. Nearly all respondents cite fast and unpredictable regulatory change as a top external burden, and an overwhelming majority report struggling with conflicting laws across jurisdictions.
- **Supply chain risks and compliance requirements**, where due-diligence needs, trade restrictions, and technology controls demand defensible evidence deep into sub-tier networks. Supply chain transparency remains among the lowest-maturity areas for companies, even as respondents identify it as a near-term priority.
- **Technology, data, and cyber risks**, which have evolved into enterprise-resilience challenges amplified by ecosystem complexity and third-party exposure. Cybersecurity and data protection consistently rank among the top enterprise risks, yet only a small minority of organizations describe their capabilities as fully mature.

The progression of forces is clear. **(See Exhibit 1.)** Rising geopolitical volatility and regulatory divergence drive operational complexity—most visibly in supply chains and digital ecosystems—where traditional, human-centric models struggle to keep pace. These shifts converge in an intensifying risk and compliance squeeze, where leaders must address the budget, talent, and capacity constraints. As complexity accelerates, advanced analytics, GenAI, and agentic systems become part of the solution—not only as levers for scale but as necessities to enhance both effectiveness and efficiency.

About the Study

BCG surveyed more than 100 organizations across six industries and five regions to capture current priorities, challenges, and emerging trends in risk and compliance. **(See the exhibit.)**

Most respondents operate at the group level, with almost 80% representing enterprise-wide functions. The sample is highly senior, with 90% of participants serving as heads of department or function. The companies surveyed are primarily large organizations, with over one third exceeding $5 billion in annual revenue and 50% with more than 10,000 employees globally.

Respondents represent a balanced mix of functions, including central risk or compliance (over 40%), combined compliance and legal (30%), and stand-alone compliance (nearly 30%). This provided a broad perspective on how leading companies manage risk and compliance today.

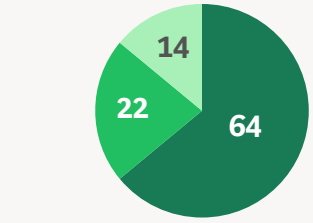
Our Findings Reflect the Insights of Leaders Across Industries and Regions

Industries

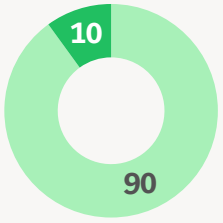
Equal participation across:

- Consumer products
- Energy
- Health care
- Industrial goods
- Infrastructure and transportation
- Technology, media, and telecommunications

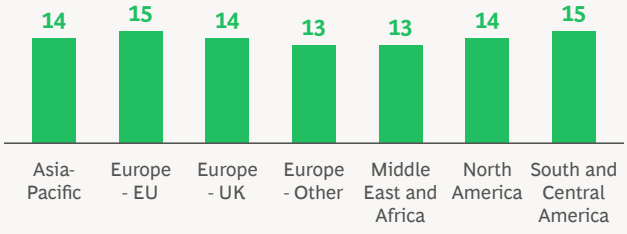
Revenue (%)



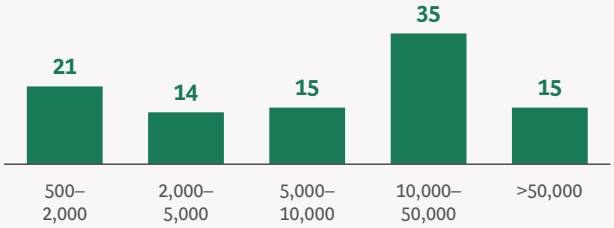
Seniority (%)



Headquarters regional distribution (%)



Company size based on the number of FTEs (%)



Source: Risk and Compliance 2026 Survey.
Note: FTEs = full-time employees.

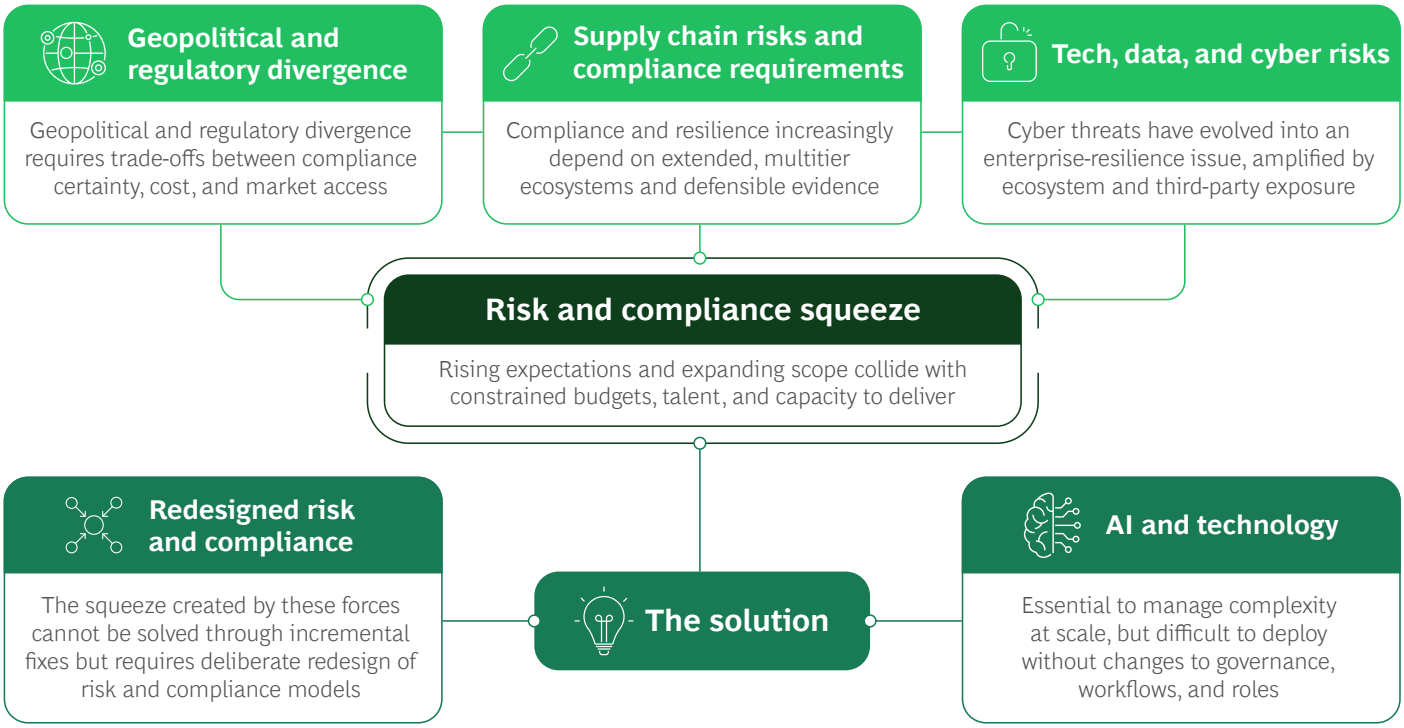
Global players cannot manage the sustained volatility resulting from these forces through incremental controls, additional headcount, or isolated technology deployments. Success requires companies to:

- **Institutionalize geopolitical foresight** to enable proactive decisions on market access, footprint, and capital allocation.
- **Redesign supply chains** for defensibility and resilience by enhancing traceability, dependency mapping, and trade compliance.
- **Elevate tech, data, and cyber resilience** into enterprise governance through board-level oversight of digital interdependence and third-party exposure.
- **Adopt AI-first operating models** with end-to-end redesigned workflows.
- **Ease the risk and compliance squeeze** by prioritizing investments and reallocating scarce talent toward the highest-impact activities.

Taken together, these shifts define a new risk and compliance mandate: proactive, integrated, AI-empowered, and deliberately designed for a world where volatility is persistent and trade-offs are unavoidable.

EXHIBIT 1

The Forces Reshaping Risk and Compliance



Source: BCG analysis.

Navigating Geopolitical Risks and Regulatory Complexity

Geopolitics has become a structural driver of regulatory divergence across major economies. Differing approaches by the US, Europe, and China—rooted in national security, data governance, and industrial policy objectives—are resulting in a more fragmented and less predictable global regulatory environment.

Among the companies we surveyed, nearly all see the current fast, unpredictable regulatory change as the top external burden. **(See Exhibit 2.)** Ninety percent struggle with conflicting laws across jurisdictions, while two-thirds are weak in integrating geopolitical risk insights with compliance strategy. Yet regulatory change management remains among the least mature areas in their risk and compliance setup, and 90% of respondents plan to prioritize improving it for the next 12 months.

Regulatory fragmentation creates material risk and compliance, operational, and commercial challenges for global companies. Different regulatory requirements are not always legally incompatible, but they are increasingly difficult to accommodate within unified global operating models. To manage regulatory trade-offs, costs, and market-access risks, companies must fundamentally adapt how they design and execute risk and compliance. Many are relying more heavily on ringfencing specific activities, shifting to locally managed data and operations, using licensing strategies, and adopting differentiated regional processes.

EXHIBIT 2

Regulatory Fragmentation Is Reshaping Risk and Compliance Decisions

Regulatory fragmentation is now a structural risk and compliance challenge for companies

Nearly all
Cite fast, unpredictable regulatory change as a top external burden

90%
Struggle with conflicting laws across jurisdictions

Two-thirds
Report weak integration between geopolitical risk insights and compliance

Risk and compliance risk is shifting from fines to business disruption for companies

Regulatory incompatibilities increasingly translate into operational and commercial consequences, including:

90%

- Expanding geopolitical risk analysis capabilities
- Experiencing denied market entry or licensing constraints
- Strengthening sanctions and export-control capabilities

70%

- Considering reducing or exiting operations in high-risk countries[1]

Where the gap remains

90% Plan to prioritize regulatory change management as a top focus area for the next 12 months, yet regulatory change management remains among the least mature risk and compliance capabilities

Source: Risk and Compliance 2026 Survey.
[1]High-risk countries are markets directly impacted by sanctions, trade restrictions, or armed conflict.

In practice, global companies are now confronting regulatory conflicts that cannot be resolved through technical risk and compliance alone. Prominent examples include conflicts centered on:

- **Sanctions-Related Regulation.** Tensions exist between regimes such as the US Office of Foreign Assets Control sanctions and the EU Blocking Statute. As a result, companies may face conflicting compliance incentives, reporting obligations, and enforcement or liability risks when managing the same transactions, counterparties, or market activities across jurisdictions.
- **Data-Governance and Localization.** Divergences between the EU's General Data Protection Regulation and China's data-protection, cybersecurity, and data-localization frameworks may be difficult to reconcile. Although cross-border data flows remain possible, they are subject to different conditions, approvals, and system design requirements. This forces companies to make significant investments in operational segmentation, localization, and risk and compliance.
- **Technology Sovereignty.** US export controls on semiconductors and AI-enabling technologies intersect with Chinese regulations, including expanded export-licensing requirements for critical minerals, such as rare earths, gallium, and germanium. Consequently, companies must navigate trade-offs between market access and the disclosure of sensitive industrial information.

In this environment, achieving fully aligned, upfront compliance across all regions is increasingly difficult—particularly for companies operating simultaneously in the US, Europe, and China. The focus is therefore shifting from avoiding isolated violations to managing trade-offs between compliance certainty, cost, and market-access risk. In many cases, the most material risks are no longer financial penalties, but commercial disruption: delayed shipments, denied market entry, suspended licenses, or forced operational redesigns.

These decisions now sit at the intersection of risk and compliance, customer commitments, and economic feasibility. Leaders are increasingly required to sequence and prioritize risk and compliance investments under uncertainty—balancing the risk of acting too late against the risk of committing capital and capabilities before requirements are fully defined or consistently enforced. This dynamic further intensifies reliance on scarce specialists who can interpret geopolitical signals, navigate conflicting sanctions regimes, and translate early policy developments into operational decisions.

In response, companies are beginning to rethink how they organize for risk and compliance, foresight, and strategic decision making. There are two key areas where leading companies are concentrating their moves:

Risk Sensing and Scenario Analysis for Early Warning Capabilities. Companies are moving beyond formal regulatory tracking to incorporate broader policy signals and market-access developments. They are increasingly using scenario analysis to test strategic and operational decisions under alternative geopolitical and regulatory futures.

To enable faster, more coordinated action when conditions shift, companies need to specify clear red lines for markets, suppliers, and data flows, and link them to predefined response options.

Strategic Footprint Adjustments for Risk Resilience. Companies are making deliberate efforts to rebalance exposure across markets, supply routes, and critical suppliers in response to persistent geopolitical risk. Most companies are considering reducing or exiting operations in high-risk countries—those directly impacted by sanctions, trade restrictions, or armed conflict. This includes plans to shift investments toward Southeast Asia and Latin America.

To succeed, companies need to conduct stress-test analyses of key markets, supply chains, and dependencies. They must also define indicators with threshold levels that trigger immediate actions—such as diversification, footprint shifts, or market exit—if a scenario materializes.

Supply Chain Risk and Compliance for a Fragmented World

Increased geopolitical and regulatory divergence is reshaping global supply chains. New generations of trade restrictions—such as forced-labor and deforestation regulations—require deeper sub-tier transparency and the use of digital tools and data analytics to generate defensible evidence of risk and compliance across extended supply networks.

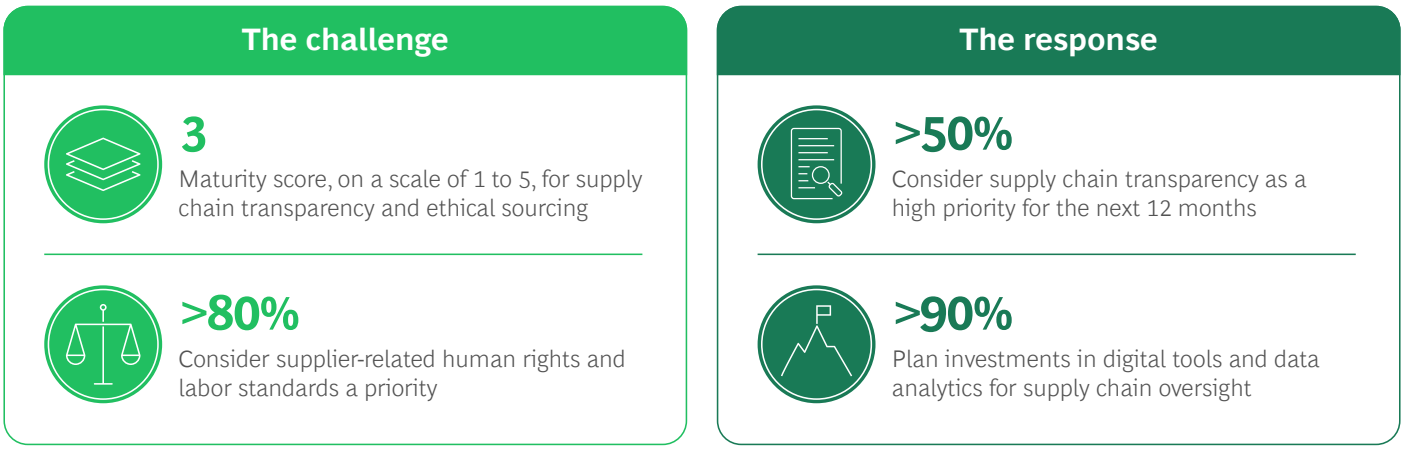
Yet supply chain transparency remains one of the lowest-maturity areas across organizations. **(See Exhibit 3.)** In our survey, over 80% of respondents cited supplier-related human rights and labor standards as a rising risk and compliance priority. More than 50% identified supply chain transparency as a high priority for the next 12 months, and more than 90% plan to increase investment in digital tools and analytics to strengthen oversight.

At the same time, tightening trade measures and policy interventions are adding friction to global sourcing models by increasing requirements for origin transparency, counterparty screening, and, in some cases, end-use controls. Combined with geopolitical instability, disrupted logistics, and fragmented regulatory regimes, these pressures are exposing structural vulnerabilities in cross-border supply chains.

As a result, supply-chain risk and compliance is no longer about reporting requirements at the edge of the organization—it is becoming a central driver of sourcing strategy. Country of origin is taking on greater strategic importance: enabling access to free-trade agreements, supporting compliance with national restrictions, and providing a buffer against heightened enforcement in key jurisdictions.

EXHIBIT 3

Supply Chain Risks Are Driving Transparency Investments



Source: Risk and Compliance 2026 Survey.

Leading organizations increasingly see supply chain risk and compliance as a design challenge, not a supplier-management task. Advanced players are emphasizing the following actions:

Diversifying and Mapping Sources for Resilience. Companies are diversifying suppliers and selectively insourcing critical capabilities. They are also mapping critical materials and components to identify high-risk jurisdictions, restricted origins, and single-source dependencies.

To fully succeed, companies need to determine where:

- Diversification is feasible (such as for aluminum components).
- Selective insourcing is required (for example, batteries and semiconductors).
- Dependencies (such as on rare earths) must be accepted and actively managed through buffering and contingency strategies.

Defining and Applying Tailored Resilience Thresholds. Leaders are unifying trade controls, import bans, sanctions, and sustainability requirements within a single operating model. They are conducting comprehensive supplier risk assessments and portfolio-level exposure management to enable earlier intervention and more resilient sourcing decisions. As part of this redesign, companies are defining resilience thresholds—acceptable levels of redundancy, dual sourcing, and inventory—tailored to product, region, and risk exposure.

To operationalize these thresholds, companies need to trigger immediate footprint, sourcing, or market-exit decisions as these conditions become present.

Building Enterprise Resilience Against IT Risks

Beyond reshaping supply chains, rising volatility and regulatory fragmentation are elevating tech, data, and cyber risks from IT concerns into a business-critical issues on board agendas.

Decisions across products, supply chains, partnerships, data, and AI all carry risk implications. When incidents occur, they can trigger immediate financial, operational, and reputational consequences.

At the same time, it is clear that readiness gaps remain significant. **(See Exhibit 4.)** While 90% of survey companies identify tech, data, and cyber risks as a top risk and compliance priority, only 60% have embedded them into their key risk and compliance processes—and nearly all companies consider that their capabilities are not highly advanced. Maturity is constrained by legacy systems, reliance on a small number of cloud and software-as-a-service providers, growing third-party and operational technology exposure, and aggressive regulatory timelines.

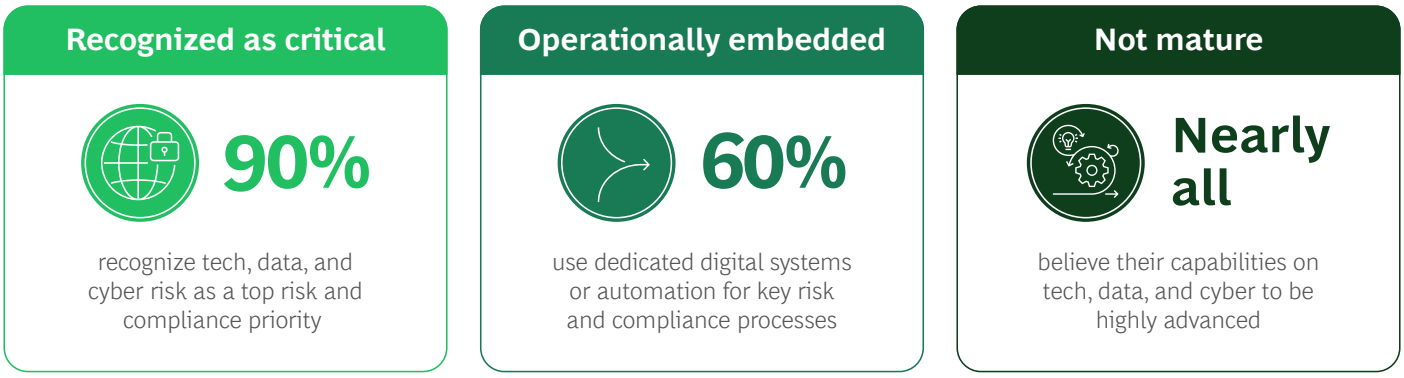
Companies now face three reinforcing pressures:

New Threats. State-sponsored campaigns, ransomware, supply-chain intrusions, and AI-enabled exploits are increasing in both frequency and impact. Geopolitical tensions raise the stakes further, heightening risks to critical infrastructure and industrial control systems.

More Regulation. Regulation is catching up. New frameworks include the EU's Digital Operational Resilience Act (DORA) and the Network and Information Security Directive 2 (NIS2). These regimes, together with new disclosure requirements, demand greater resilience, more granular reporting, and clearer executive accountability. Cybersecurity is now a regulatory and fiduciary expectation, not merely an optional best practice.

EXHIBIT 4

Companies Lack Mature Capabilities to Handle Tech, Data and Cyber Risks



A large tail of organizations remains reactive or fragmented, despite high perceived risk

Source: Risk and Compliance 2026 Survey.

Intertwined Risks. Tech, data, and cyber risks are increasingly embedded in supply-chain design. Supply-chain attacks are rising, particularly in lower-maturity industries and ecosystems where security baselines vary widely. As companies diversify suppliers, interfaces and data flows multiply, expanding the attack surface. Geopolitical decoupling compounds this challenge: diverging standards, localization requirements, and technology controls introduce additional boundaries that must be secured. Yet many organizations still lack visibility beyond tier-1 vendors, making cascading breaches difficult to anticipate and contain.

Against this backdrop, the strategic challenge is no longer simply to improve security across tech, data, and cyber, but to embed resilience into how the enterprise operates—shaping decision making, operating models, and ecosystem management across the business.

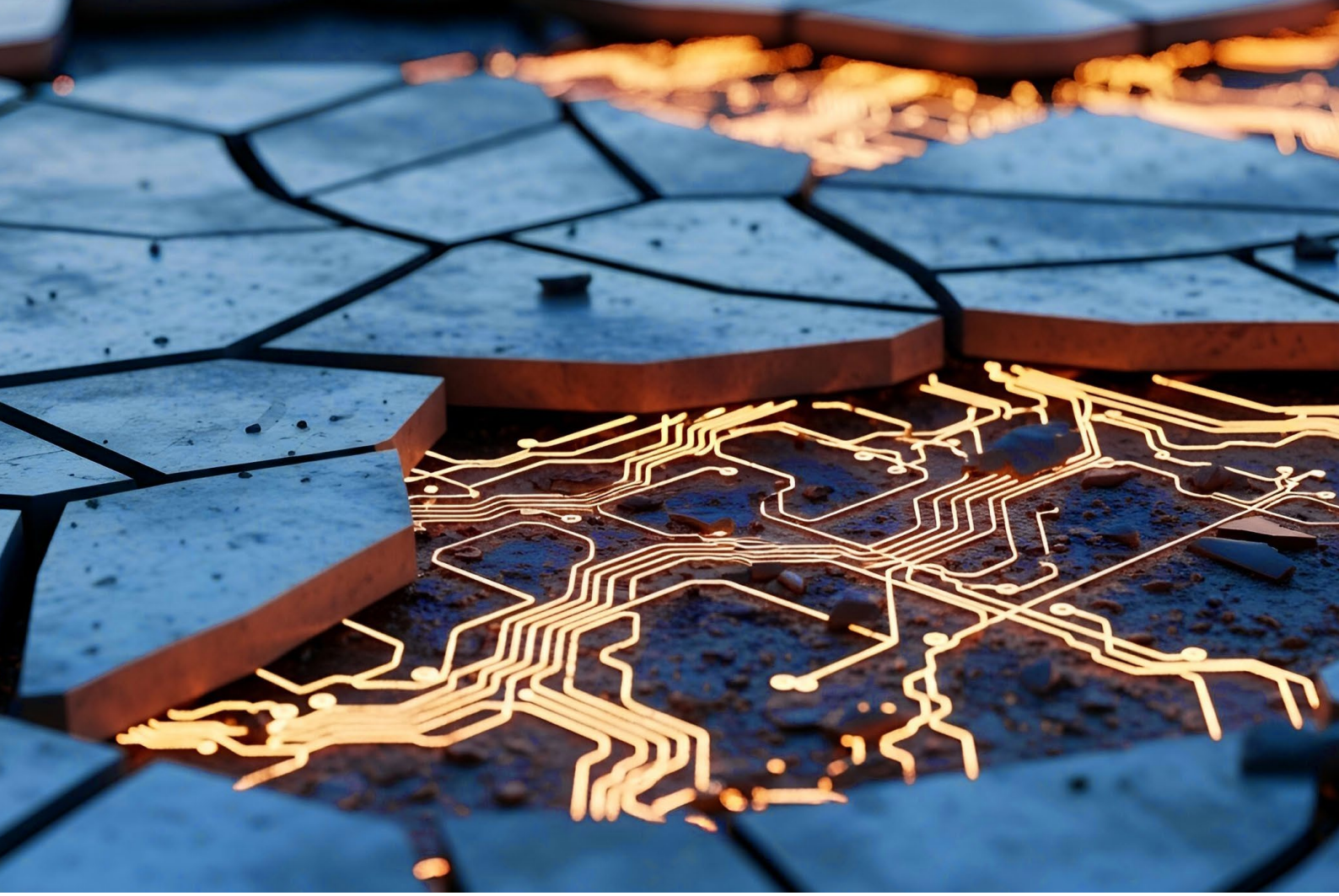
Leading organizations are responding to this shift by rethinking how they protect their systems and ensure business continuity:

Using AI to Enhance Cyber Security, Response, and Recovery Capabilities. Companies are embedding AI into core security activities to improve threat detection, analytics, and security operations center productivity, while also securing AI transformations themselves. This includes establishing durable controls over models, data, and platforms, as well as interim safeguards that allow the business to scale AI securely.

To succeed, companies need to integrate AI-specific and forward-looking threat scenarios into tech, data, and cyber control frameworks, including AI-enabled early threat detection, automated red teaming, and proactive validation of security posture. They need to shift their response and recovery capabilities to an automated and analytics-driven approach to contain attacks quickly, limit business impact, restore operations, and align with crisis management, legal, and communications processes.

Integrating Resilience to Strengthen Business Continuity. Companies are increasingly embedding tech, data, and cyber risk management into business continuity management and incident response. Although self-reported maturity is relatively high, many organizations overestimate resilience in the absence of fully integrated disruption scenarios.

To protect against ransomware and destructive attacks, leading companies need to establish robust backup strategies, tiered redundancy, and clearly defined recovery time and recovery point objectives. Then they need to align tech, data, and cyber resilience with broader operational resilience and business continuity planning, maintaining clear business ownership rather than technology-only accountability.



How to Leverage AI

The new dynamics across regulatory complexity, supply chains, and cybersecurity have created a widening scalability gap: workloads within risk and compliance are growing significantly faster than human-only operating models can absorb.

As mandates and expectations expand, AI is becoming a foundational capability for risk and compliance management—not as a productivity add-on, but as a prerequisite for scale.

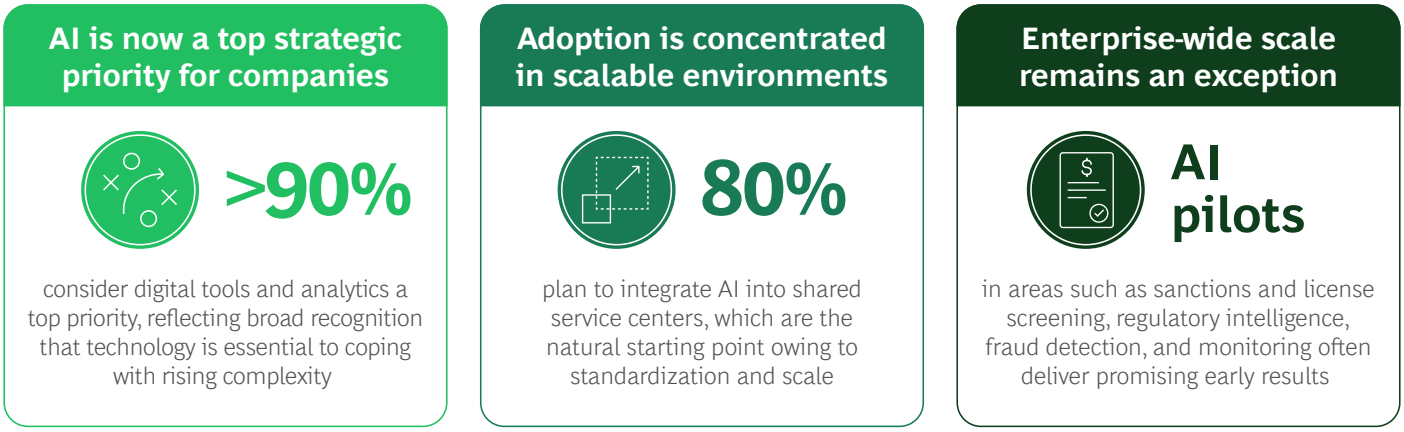
Our survey findings demonstrate this shift. **(See Exhibit 5.)** Digital tools and analytics are a top priority for more than 90% of respondents, reflecting broad recognition that technology is essential to managing rising complexity. Meanwhile, 80% plan to integrate AI into SSC environments, where standardized processes and scale make automation attractive. However, the findings also reveal a critical constraint: most AI projects remain pilots rather than enterprise-wide initiatives.

GenAI and agentic systems are now driving expectations for at-scale impact. These newer approaches offer the potential to automate high-volume, rules-based activities, improve detection quality, and free human capacity for judgment-intensive work. Early use cases span risk and compliance management domains, including:

- Regulatory scanning and cross-jurisdiction mapping for monitoring geopolitics and regulatory change.
- Entity screening and origin verification to promote supply chain compliance.
- Threat intelligence and anomaly detection for cybersecurity risk management.
- Automation of know-your-customer and know-your-supplier processes, ongoing monitoring to reduce risks, regulatory reporting, and case triage in compliance operations.

EXHIBIT 5

AI Ambition Is High, but Enterprise Impact Is Lagging



Source: Risk and Compliance 2026 Survey.

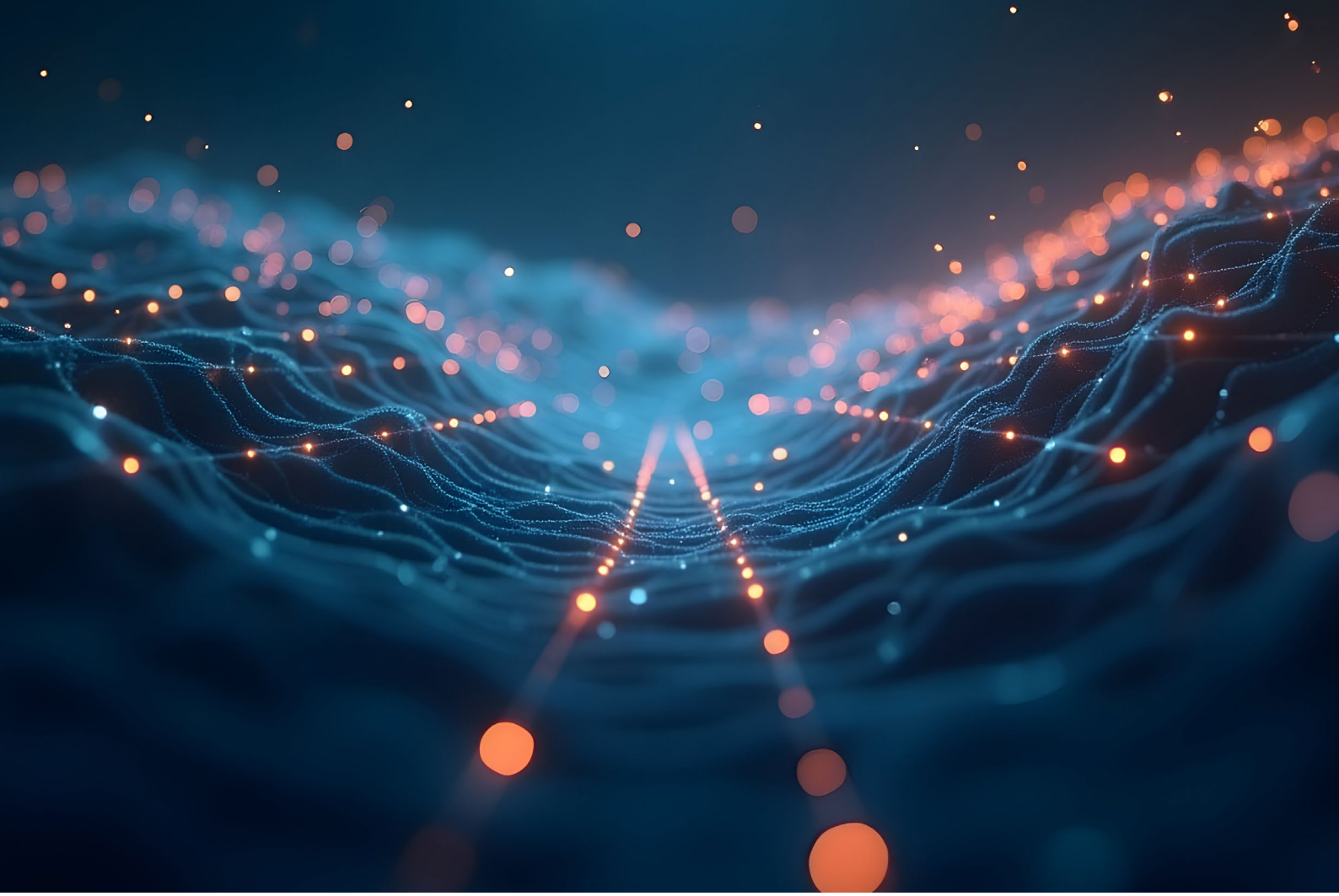
Scaling AI is as much a change-management challenge as a technical one. Embedding AI into day-to-day risk and compliance activities requires redesigning roles, workflows, decision rights, and incentives—and helping teams adapt to working alongside AI-enabled systems. At the same time, GenAI and agentic models introduce the need for new governance approaches. Organizations are still developing appropriate oversight structures for autonomous or semi-autonomous systems. Many existing risk and compliance processes were not designed to handle the volume, speed, and diversity of AI use cases now emerging. As a result, the gap between AI's potential and its realized impact continues to widen.

To ensure that AI delivers on its potential, companies need to set their AI ambitions by prioritizing two key aspects:

Investing in Data Foundations to Promote Scalability. Organizations must improve data quality, accessibility, and standardization, while upgrading legacy systems that limit scalability. Data foundations should incorporate unstructured inputs—such as text, audio, and images—to enable advanced analytics and AI use cases. Strengthening these capabilities ensures AI initiatives are built on scalable, enterprise-ready infrastructure rather than fragmented or outdated systems.

Embedding AI into Operating and Governance Models. Organizations should move to enterprise-wide AI deployment by embedding AI into operating-model redesign, transforming entire compliance verticals—such as regulatory change and supply chain management—rather than pursuing isolated tasks. Shared AI capabilities should be built centrally and extended through a hub-and-spoke model to avoid duplication. Clear, responsible AI governance, controls, and usage standards are essential to ensure proficiency, safety, fairness, security, and compliance, alongside engagement with regulators and industry bodies to shape evolving standards.

By taking these steps, risk and compliance functions can use AI to keep pace with rising regulatory complexity without increasing costs or headcount linearly. That requires treating AI and other technology tools as core enablers of scale and resilience, not incremental add-ons to existing processes.



Easing the Risk and Compliance Squeeze

Across industries, the forces discussed in this report are creating what we term a “risk and compliance squeeze”—expanding scope and accelerating expectations are colliding with constrained budgets, talent, and delivery capacity. **(See Exhibit 6.)**

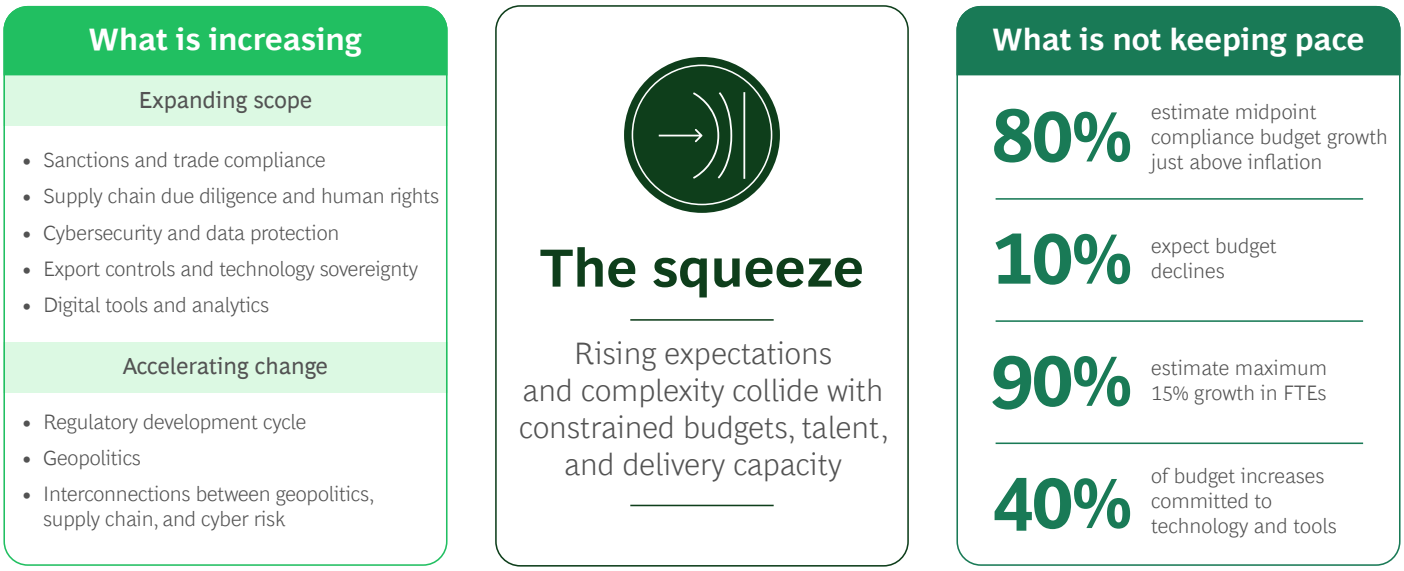
On one side of the squeeze, the perimeter of risk and compliance is widening. Sanctions and trade compliance, supply chain due diligence, human rights, cybersecurity and data protection, export controls and technology sovereignty, and digital tools and analytics are all expanding in scope. At the same time, regulatory development cycles are accelerating, and interconnections between geopolitical, supply chain, and cyber risks are deepening complexity.

On the other side, resources are not keeping pace. Eighty percent of survey respondents expected a midpoint compliance budget growth just above inflation, while 10% anticipate outright declines. Even where funding increases, much of it is pre-allocated: 40% of incremental budgets are already committed to technology and tools, including AI. This leaves companies with limited flexibility for additional staffing: 90% are expecting less than 15% growth in full-time equivalents, at a time when workloads and complexity are rising faster than capacity.

Teams operating within this squeeze are expected to cover a broader and more complex agenda, build new capabilities quickly, and remain agile amid accelerating regulatory and geopolitical change. Expectations have also shifted. Boards, regulators, and other stakeholders increasingly demand forward-looking compliance—anticipating risk, shaping resilience, and informing strategic decisions—not simply enforcing adherence or remediating issues after the fact.

EXHIBIT 6

Complexity and Constraints Are Driving the Risk and Compliance Squeeze



Source: Risk and Compliance 2026 Survey.
Note: FTEs = full-time employees.

Talent constraints intensify the pressure. As risk and compliance topics become more specialized and interconnected, organizations depend on scarce talent profiles that combine regulatory depth with digital fluency, geopolitical insight, or cyber expertise. Even where budgets are available, many companies struggle to attract and retain individuals with this blended capability set.

These dynamics point to a structural shift. The risk and compliance squeeze is not a temporary imbalance that can be resolved through incremental hiring. Organizations must instead make deliberate choices about the work risk and compliance teams perform, how it is delivered, and where to prioritize risk and compliance investments for the greatest economic impact.

As leading companies address rising complexity and constrained resources, two moves stand out:

Prioritizing Investments Based on Risk. Rather than treating all risk and compliance investments equally, organizations are increasingly adopting a risk-based approach that links investment intensity to materiality, regulatory clarity, and potential impact. Full and immediate compliance is prioritized in areas critical to market access, licensing, and board-level accountability. At the same time, a higher tolerance for managed exposure is emerging in areas characterized by regulatory ambiguity, evolving timelines, or uncertain enforcement. This allows companies to sequence risk-related and compliance investments and avoid premature or stranded costs. Importantly, this shift is not about lowering standards, but about aligning compliance efforts with risk appetite and economic reality.

To succeed, companies need to treat rising expectations alongside flat or modest budgets as a structural design constraint, not a temporary anomaly. Then they need to decide where to invest fully—and where to accept managed risk. Investment decisions should be made to consolidate scalable, repeatable activities while keeping high-judgment, context-rich work close to the business.

Redesigning Delivery Models. Given persistent resource constraints, simply expanding headcount is no longer viable. To address the challenge, companies are increasingly treating shared service centers (SSCs) and external providers as structural components of compliance operations rather than tactical supplements. However, poorly applied models risk eroding local insight and responsiveness. Leading organizations are therefore taking a more deliberate approach—carefully selecting which activities to centralize or outsource, and building safeguards to preserve local judgment, accountability, and control.

As regulations, capabilities, and technologies evolve, companies need to regularly revisit what should be centralized, outsourced, or brought back in-house.

Five Imperatives to Guide a New Agenda

The structural convergence of geopolitical fragmentation, supply chain exposure, tech, data, and cyber risks, driving the risk and compliance squeeze demands a coherent, AI-driven, enterprise-level response. Five imperatives should define the risk and compliance agenda for 2026 and beyond.

Institutionalize geopolitical foresight. Regulatory divergence and geopolitical fragmentation are reshaping market access and competitive positioning. Leaders are embedding scenario analysis into strategy, strengthening early-warning capabilities, and adjusting their global footprint proactively.

Redesign supply chains for defensibility and resilience. Risk and compliance within supply chains has moved from documentation to design. Organizations are mapping dependencies, diversifying exposure, integrating trade and risk frameworks, and defining resilience thresholds for critical materials.

Embed tech, data, and cyber resilience into enterprise governance. Leading companies have elevated digital-dependence risks to board-level business continuity concerns. They are strengthening third-party oversight and integrating risk scenarios into resilience planning.

Move decisively toward AI-first operating models. Advanced analytics, GenAI, and agentic systems can become part of the fix. This requires organizations to progress beyond pilots and redesign workflows around AI's strengths, invest in shared data foundations, and establish governance that enables safe scaling.

Treat the risk and compliance squeeze as a design constraint. Rather than stretching existing models further, leading organizations are prioritizing rigorously. They are centralizing scalable activities and continuously reassessing where risk and compliance activities create the greatest strategic value.

Together, these priorities define a more resilient and strategically integrated model for risk and compliance. Going forward, the competitive advantage will not lie in doing more, but in designing better: aligning governance, technology, and operating models to manage complexity without sacrificing speed, resilience, or commercial flexibility.

About the Authors

Katharina Hefter
Managing Director and Partner
Berlin

Malgosia Zegar
Partner
Munich

Anne Kleppe
Managing Director and Partner
Berlin

Johannes Große
Managing Director and Partner
Berlin

Bernhard Gehra
Managing Director and Senior Partner
New York

Pierre Roussel
Managing Director and Senior Partner
Paris

Julia Gebhardt
Managing Director and Partner
Munich

Florian Meier
Associate Director, Risk & Compliance
Berlin

Biljana Bajic-Bizumic
Managing Director and Partner
Zurich

Sarah Lichtblau
Partner
San Francisco - Bay Area

Matteo Coppola
Managing Director and Senior Partner
Milan

Abhinav Bansal
India Leader, Risk Practice
Mumbai

Acknowledgments

The authors thank Ramón Bravo and Eva Kalteier for their contributions to the writing of this report.

Boston Consulting Group partners with leaders in business and society to tackle their most important challenges and capture their greatest opportunities. BCG was the pioneer in business strategy when it was founded in 1963. Today, we work closely with clients to embrace a transformational approach aimed at benefiting all stakeholders—empowering organizations to grow, build sustainable competitive advantage, and drive positive societal impact.

Our diverse, global teams bring deep industry and functional expertise and a range of perspectives that question the status quo and spark change. BCG delivers solutions through leading-edge management consulting, technology and design, and corporate and digital ventures. We work in a uniquely collaborative model across the firm and throughout all levels of the client organization, fueled by the goal of helping our clients thrive and enabling them to make the world a better place.