
Baker McKenzie.
The Currency of Connection:
Mobilizing technology for compliance integration
Resilience
Recovery
Renewal

Baker McKenzie.

# Foreword

**Global organizations have been on a shared mission to become digitally-enabled enterprises. Maximizing the efficiency and commercial opportunity of technology has long been key to growth, but the COVID-19 pandemic has created a new and urgent imperative for companies across sectors to scale up and accelerate digital adoption. Leaders are acting quickly to pivot entire service lines, digitalize operations and automate processes — including within the compliance function.**

With accelerated change comes new risks and emerging challenges for compliance teams. In our Connected Compliance 2020 research findings, compliance leaders report that not only are their organizations implementing technology with little consideration for risk, but also that compliance is shut out of conversations relating to critical technology decision-making. Compliance leaders say this has already resulted in enforcement investigations and predict that regulatory scrutiny will rise as a result of hurried digitalization.

However, our research also reveals that technology is both a source of new risk to be managed and an essential connector for the compliance function. COVID-19 has catalyzed a re-examination of traditional approaches and many compliance teams are on the cusp of a radical reimagining of the function — embracing technology as an enabler of compliance integration and efficiency. From artificial intelligence (AI) and predictive analytics to eDiscovery and regtech (the management of regulatory matters through technology), the future of compliance is well and truly digital.

This report will highlight technology risk and break down compliance challenges arising from key shifts — forming an image of "next generation" connected compliance and reflecting on how compliance technology can address risk.

Through proprietary research and legal expertise, this report highlights:

- risks arising from the digital transformation of organizations and compliance functions;
- emerging opportunities for the application of technology in compliance;
- key considerations for compliance leaders in this regard and;
- the strategies of the most sophisticated compliance tech adopters.

These insights help answer the question facing compliance leaders of today: "What is the currency of connection?"

"Everything is tech. It is a means of doing things, not an end in itself. Nor is it separate from core business — technology these days is the core business."
**Ben Allgrove**
**IP, Data & Technology Partner and Global Head of Research & Development**

**Joanna Ludlam**
**Co-chair, Global Compliance & Investigations**

# About the research

The Currency of Connection is based on independent research among 1,550 compliance leaders across 18 global markets and six sectors. Interviews were conducted in the summer of 2020.


- Industrials
- Consumer Goods
- Energy & Infastructure
- Financial Institutions
- Healthcare & Life Sciences
- Technology, Media & Telecoms

Baker McKenzie.

# Digitalization of business drives new compliance risk

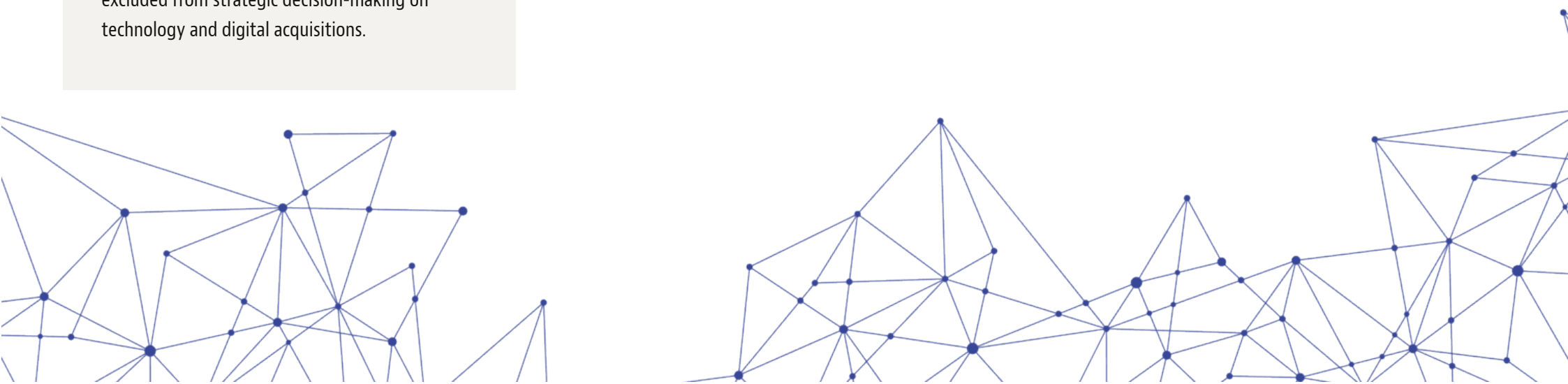
# Snapshot

- 47% of compliance leaders say that COVID-19 has accelerated a focus towards digital products, approaches and tools in their organizations.
- 41% state that ill-considered and poorly implemented technology has already resulted in enforcement investigations.
- Up to 64% of compliance leaders predict that scrutiny of tech-enabled business models as a result.
- Yet 47% suggest that the compliance team is excluded from strategic decision-making on technology and digital acquisitions.

**47% of compliance leaders say that COVID-19 has accelerated adoption of digital products, approaches and tools in their organizations. But the urgency of the shift to technology has generated significant new risk. Ill-considered and poorly implemented technology has already resulted in enforcement investigations, according to 41% of compliance leaders, with investigations likely to arise in relation to data privacy and cyber-security as well as tax, transfer pricing, fraud and antitrust — complex and sometimes interdependent matters that require careful attention.**

Yet compliance teams remain shut out of decision-making. 47% of global compliance leaders state that the compliance team is rarely consulted on compliance risk at the start of strategic decision-making on technology and digital acquisitions. A further 34% report that their organization is employing technology without regard for potential compliance risk.

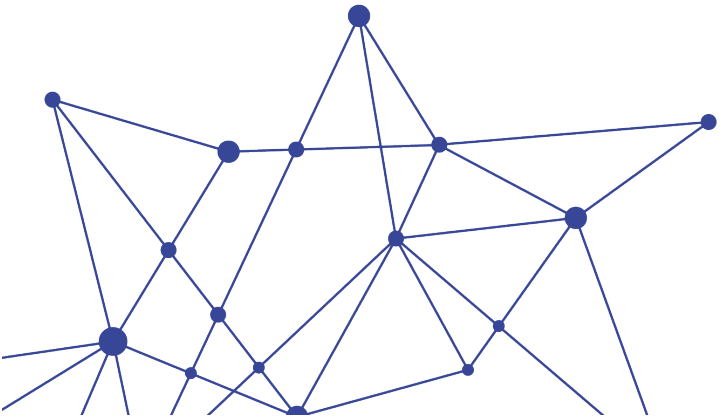
Considering the speed and scale of pivotal decisions, a rise in investigations and potential breaches appears inevitable to compliance leaders. Up to 64% predict that scrutiny of tech-enabled business models and data privacy issues will be top of regulators' to-do list as a result of COVID-19.

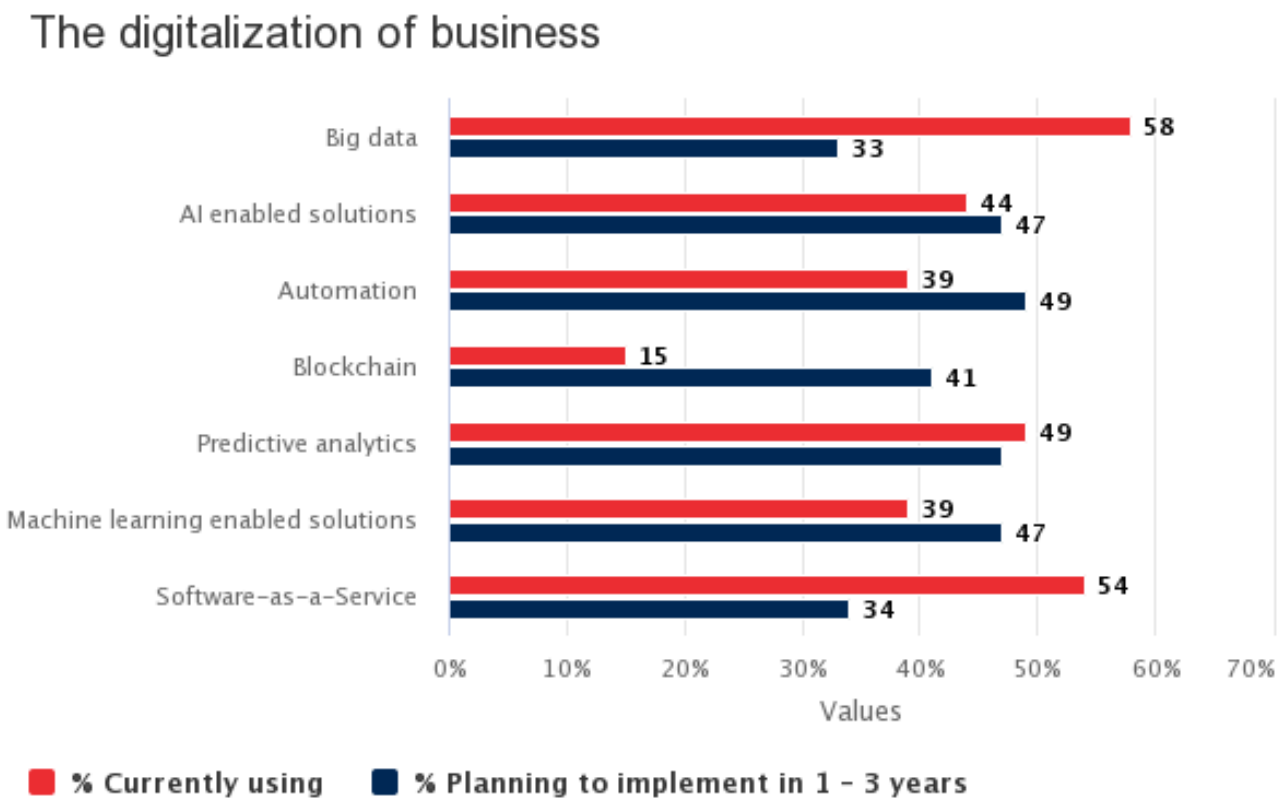


# The digitalization of business

**Insights by Ben Allgrove, IP, Data & Technology Partner and Global Head of Research & Development**

Digitalization is not new. Organizations have been integrating technology into business models and operations consistently over the last decade, but COVID-19 has been a catalyst for organizations to accelerate these efforts. The dramatic shift to remote-working and imperative to quickly shore up revenue streams and supply chains has sharpened focus on the advantages of being a tech-enabled enterprise. In particular, organizations that were falling behind the digital curve are now chasing rapid change.






Technology currently used by global organizations vs. intended adoption of these technologies over three years

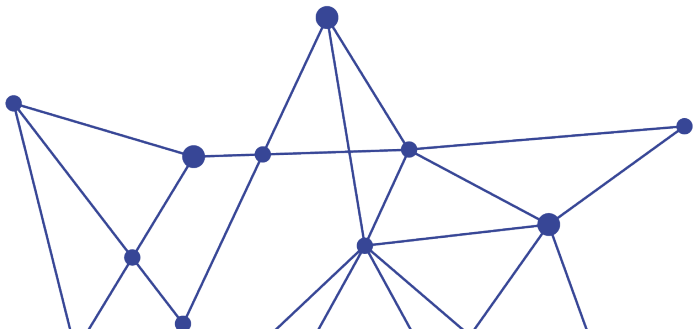
Organizations are already significantly engaged on tech adoption, using Software-as-a-Service and even machine learning to some extent — think of automated responses in Outlook or Gmail as simple examples. Our research suggests that global companies will continue to ramp up their use of digital tools, with a steep adoption curve in relation to predictive analytics and AI in particular.

The ambition to level up the application of business technology reflects the fast pace of change in the market and organizations' growing appetite to leverage data. Increasingly sophisticated digital tools are becoming available at comparatively low cost, offering huge computing power, data management capability, machine learning models, workplace systems and productivity improvements.

But significant risk can arise as a result of poor implementation of business technology — threatening to undermine potential gains. As with any large purchasing or outsourcing decision, it is critical to understand how technology can be a part of the solution and what further organizational changes are required to support successful rollout.

Organizations commonly underestimate the transition cost associated with new technology and transforming legacy systems, as well as the culture change required. As a result, they struggle to appropriately communicate how and why the technology is designed as it is, and the ways it supports rather than replaces existing people-managed processes. We also often see failure to effectively plan short, medium and long-term deployment review milestones and iterations as part of technology implementation.

"Compliance by design" is a useful mantra for business technology adoption — considering key issues such as cyber risk, data protection strategies, antitrust issues and real-time reporting before implementation and on an ongoing basis. It is key to identify what the problem is first.



"Organizations pivoting from traditional to digital business models must be aware that they are exposed to megatrends and risks which may not have been top of their agenda previously — particularly in terms of data privacy and taxation. Leaders must be aware of these trends and adjust their business strategies and risk management activities accordingly. This means making conscious choices with respect to use of products and standards, applying a new lens to tax planning and prioritizing data and cybersecurity in compliance programs and leadership communication. But these organizations must also accept that their trajectories are not yet carved in stone and that directions may change — making sure they remain nimble is critical."

**Christoph Kurth**
**Head, Zurich Compliance & Investigations Group**

# COVID-19 disruption puts post-pandemic enforcement on fast forward

**Insights by Jessica Nall, Compliance & Investigations Partner**

Top enforcement priorities are likely to be steadfast despite COVID-19 disruption — scrutinizing technology business models, data privacy breaches and fraud remain front of mind. However, the speed and scale of new investigations will ramp up as a result of economic uncertainty and radical change.

In certain companies and market sectors, calls to internal compliance hotlines have jumped in recent months and, assuming the economic distress triggered by the pandemic mirrors that of the global financial crisis, we can be confident that this uptick is also reflected in the number of tip offs to enforcement agencies. Lay-offs go hand-in-glove with whistleblowing activity — the leads that regulators rely on for expediting new investigations and criminal proceedings, particularly in terms of white collar crime.

The number of cyber-security investigations is also likely to rise as a result of mass remote-working and traditional companies attempting to pivot underinvested digital infrastructure quickly. Leaders are weighing difficult decisions — balancing cost with continuity as they seek to protect data and IP as well as revenue. But bolting on adequate digital security to legacy technology or transforming systems to be secure-by-design are not simple or quick tasks. The significant time and resources involved in making a traditional global organization digitally "water tight" belies the speed at which recent pivots have been made.

"Regulators are grappling with the implications of technology in relation to antitrust and market power. Many contend that, where previously the practice of "tipping markets" was relatively simpler to identify and address, today these forces are often undetectable until it is too late. Data is currency and organizations can, some allege, tip markets in their favor by virtue of access to uniquely valuable data. This presents a problematic and controversial new frontier in relation to competition and antitrust enforcement that is likely to play out over the next decade."

**Luis Gomez**
**Chair, EMEA Competition Group**

# The rise of surveillance culture

**Insights by Julia Wilson, Employment & Compensation Partner**

COVID-19 has been a trigger for the biggest change to working practices in decades. While many organizations had resisted the trend towards home-working in the past, the pandemic has given rise to a dramatic and near-universal shift to remote-working for office based workers. However, many businesses remain cautious and perhaps skeptical of home working and how it can impact productivity and quality, and the relationship of trust between employer and employee is coming under significant strain.

Absent in-person oversight, we are seeing an uptick in the number of organizations implementing remote-monitoring technology to understand whether their employees remain productive, meet their contractual obligations and refrain from high risk behavior. In the US, employees are already accustomed to relatively high surveillance and there is a greater cultural acceptance of monitoring at work.

But in Europe employee (and regulator) expectations are very different and there is strong European and local level law in place to protect overreach. A recent decision of the Hamburg data protection regulator ordered a major retailer to pay a EUR 35 million fine due to its monitoring of employees. Still, there is a new appetite in the region for increased employee surveillance as a result of the pandemic.

Tools that collect data on the keystrokes, application use, web traffic and system downtime of individual employees are increasingly common, but we are also seeing interest in products that empower employees to manage their own time and share data with their employer by choice. With any such system, there are three primary risks for organizations to consider:

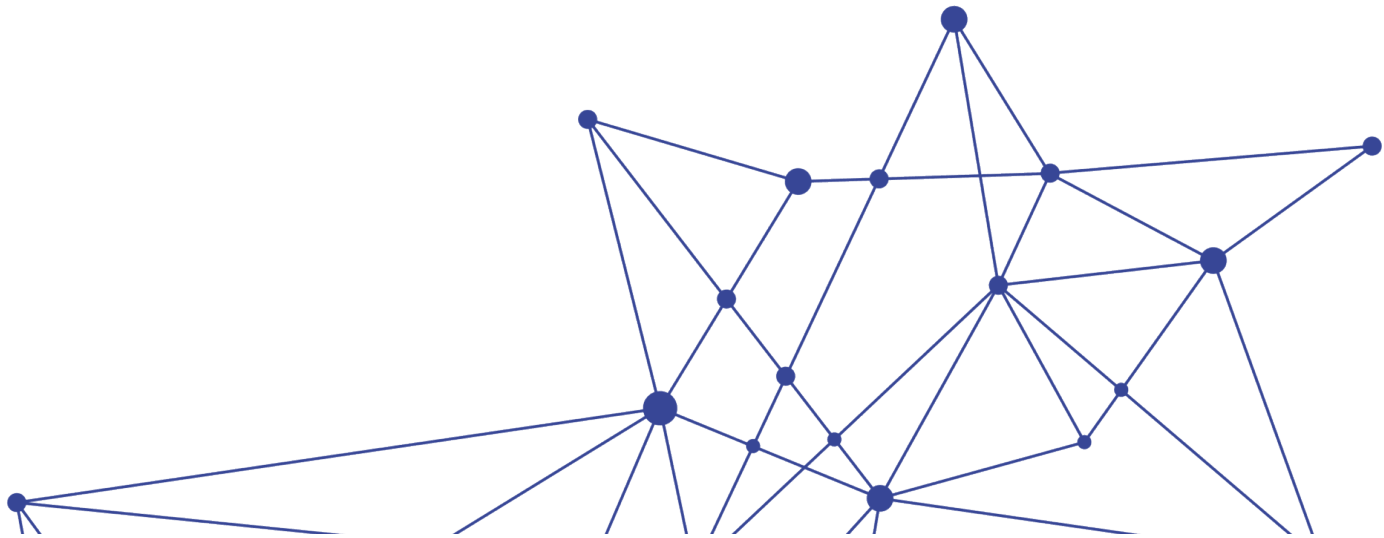
**1. Ethics and trust** — extensive monitoring of employees may jeopardize the written and unwritten contract between people and organizations, and in particular the relationship of trust and confidence — having a counterproductive effect on morale, engagement and output.

**2. Due process** — seemingly benign plug-ins to popular workforce management platforms can preempt or bypass due process required by law. For example, using such a system to flag potential candidates for redundancy in advance of any formal process is highly likely to breach the legal requirements for fair selection and could be challenged.

**3. Data risk** — many of the new technologies, if used fully in the way they are designed, will not be compliant with European data protection law. Routinely making information about individuals and their use of systems and productivity available to managers and HR opens organizations up to significant risk in relation to data privacy under GDPR. There may also be discrimination risk as a result of monitoring, where tracking activities and then making judgment calls on the basis of the data may have disparate impact. For example, in the case of employees with children, caring responsibilities or health issues.

Organizations should approach monitoring tools with caution — considering strategies for limiting access to individual data and aggregating personal information to make cross-workforce productivity and policy improvements, rather than taking punitive actions against individual employees.

Leaders would also be wise to engage trade unions and employees early, conducting consultation in advance of any tech purchase or announcement. We have seen recent examples of companies rolling back proposed monitoring following pressure from their employee communities.



Baker McKenzie.

# Compliance leaders leverage tech to address risk areas

# Snapshot

- 56% of compliance leaders report that budgets have been cut as a result of COVID-19.
- But they continue to make new technology investments to the tune of USD 4.4 million on average per organization.
- 71% agree that smart application of technology has already enabled the compliance team to reduce their administrative burden.

**The race to digitalize is also reflected within compliance teams. Facing budget cuts and a dramatic rise in digital and data risk, compliance leaders are themselves turning to technology to balance their dual role as protectors and creators of commercial value.**

56% compliance leaders report that budgets have been cut as a result of COVID-19 and another

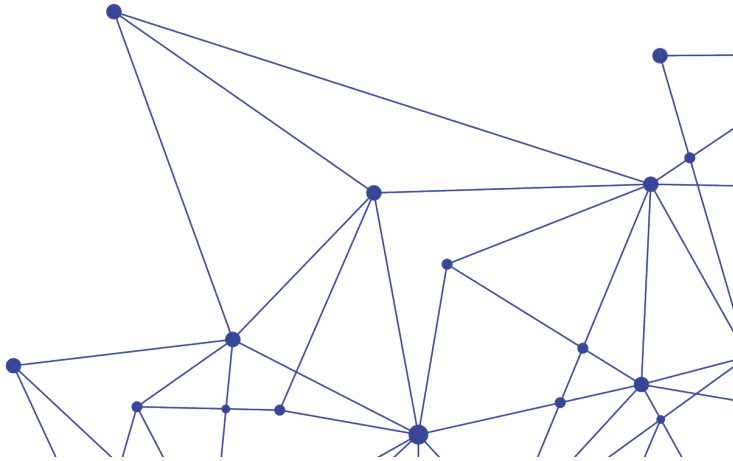
50% say that it is a constant struggle to balance their company's need for recovery and growth with compliance best practice.

Attempting to "square the circle" of stretched resources and growing risk, compliance leaders are making new technology investments of USD 4.4 million on average — aiming to focus compliance teams on strategic matters and more effectively manage compliance across jurisdictions and investments.

Efficiency matters. 71% of compliance leaders agree that smart application of technology has already enabled the function to reduce their administrative burden and a further 43% will implement new technologies to improve efficiency of the global compliance function.

"There is huge potential for compliance technology to deliver gains beyond efficiency. I expect to see greater use of artificial intelligence in future, to push the right information to the right people at the right time — supporting more comprehensive and connected compliance. The proliferation of new communications and collaboration technology is also an opportunity for organizations to provide next generation compliance programs — using augmented reality to improve the engagement of employees and partners with compliance policies and procedures."

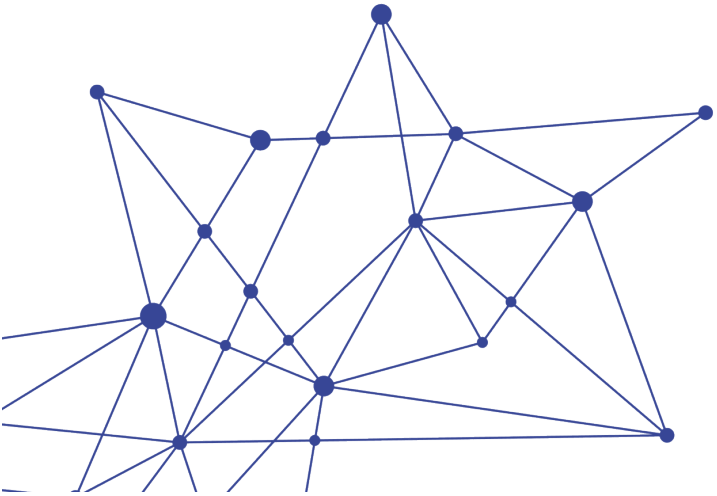
**Ben Allgrove**
**IP, Data & Technology Partner and Global Head of Research & Development**

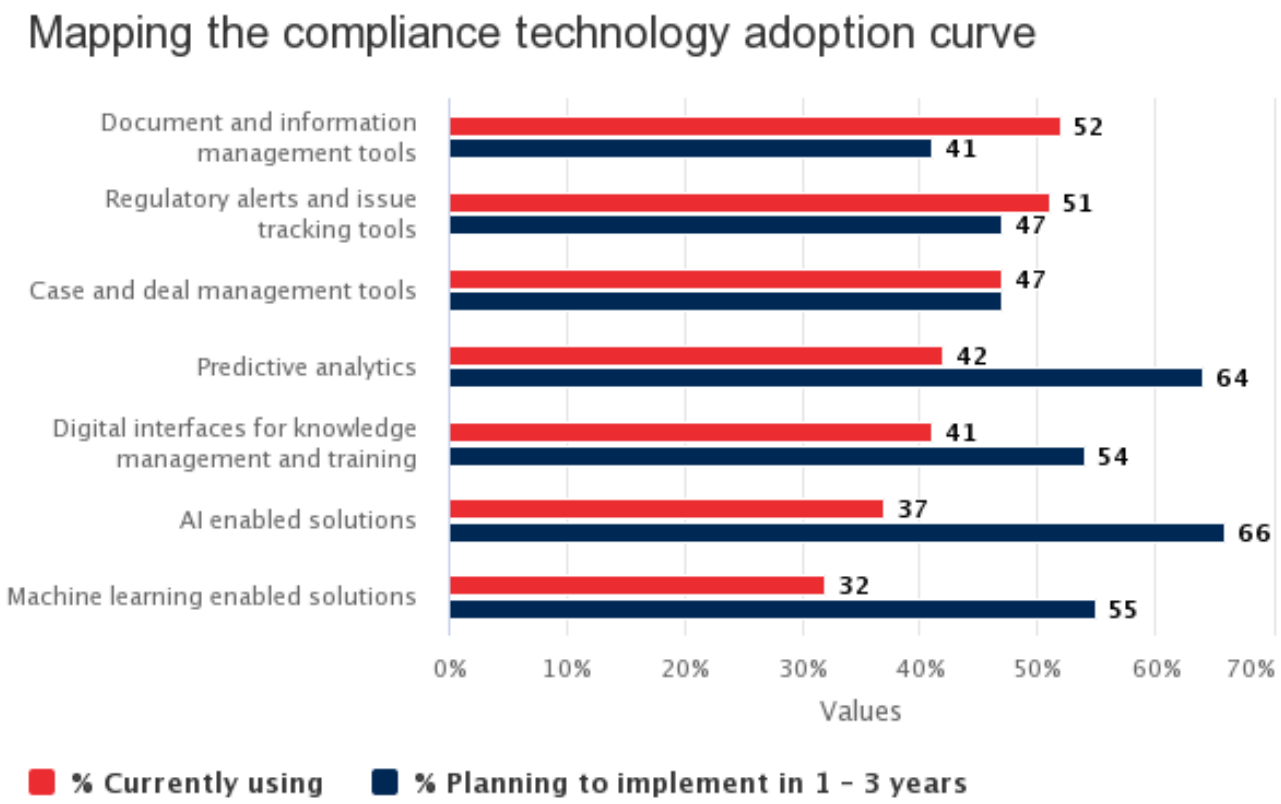


# Mapping the compliance technology adoption curve

**Insights by Joanna Ludlam, Co-chair, Global Compliance & Investigations**

Our data shows that compliance teams have prioritized practical compliance technologies to date — making smaller investments designed to relieve the administrative burden and automate what can be automated. For example, half of organizations are already using digital document management and regulatory tracking solutions, which monitor global legislation and enforcement action and highlight relevant change or key decisions, and assess emerging regulatory risk.

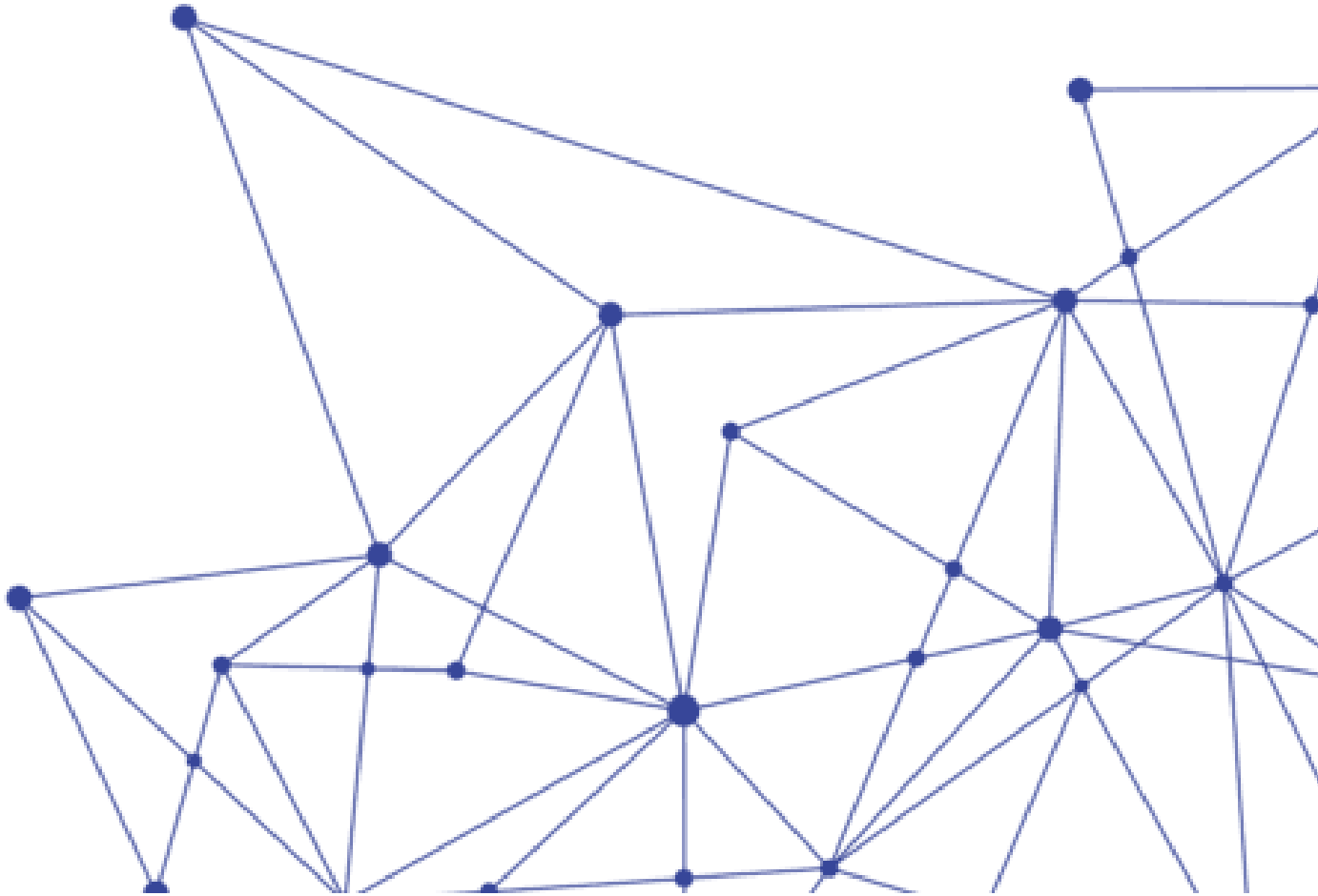





Technology currently used by compliance teams vs. intended adoption of these technologies in one-to-three years]

Compliance leaders also have ambitious long-term goals to leverage technology to make new connections — from buying single tools to manage specific compliance issues toward integrating multiple compliance technologies to manage several risks.

Within the next two years, the overwhelming majority of compliance leaders plan to further adopt machine learning, AI and predictive analytics within the function, and we are already seeing some advanced use of digital tools among tech-enabled compliance teams — including bots for finding and delivering information as part of compliance training and data-backed systems designed to identify concerning patterns of behavior.



# Regulators set a high bar for compliance technology

**Insights by Jennifer Klass, North America Co-chair, Financial Regulation & Enforcement**

According to our research, 53% of compliance leaders report that a lack of consistent guidance on compliance technology from regulators globally is a barrier to further tech adoption. While there is no singular standard on compliance technology among regulators, compliance leaders can be assured that there is only direction of travel when it comes to global enforcement — toward digitalization.

Regulators value the consistency of compliance technology for surveillance, supervision, and monitoring of internal controls — organizations that make use of digital solutions are often able to provide more consistent and comprehensive oversight, and more timely production of data in response to examinations and enforcement investigations. Regulators are also increasingly sophisticated users of technology and data. They are setting a high bar and have rising expectations in relation to how organizations should be deploying digital solutions to identify risk, conduct supervision and support compliance.

In the US, the Securities and Exchange Commission (SEC) is leading the way on the application of technology in global enforcement. They have developed a number of proprietary tools and analytic programs that leverage "big data" to review the activities of particular firms — such as aberrational performance and insider trading issues — as well as monitor broader market movements.

While 64% of compliance leaders may believe regulators should give more credit to organizations that apply data and technology to compliance challenges, they are unlikely to receive a pat on the back. From the point of view of the regulators, applying technology solutions to identify and manage risk is key to meeting modern compliance obligations.

"The digital world is at the forefront of regulators' minds, yet there remains considerable room for clarity, consistency and guidance in relation to accepted applications of compliance technology. Preferences vary globally and, while some basic compliance technology is widely welcomed by regulators, for example, document processing systems — many of the more sophisticated tools are untested. Enforcement agencies themselves are exploring increasingly advanced technology to address new digital challenges — expanding beyond forensic investigations and towards tools that can, for example, analyze market parameters and pricing to predict cartel activity."

**Luis Gomez**
**Chair, EMEA Competition Group**

# Managing third party investment risk with compliance technology

**Insights by Tristan Grimmer, Co-Chair, EMEA Compliance & Investigations Group**

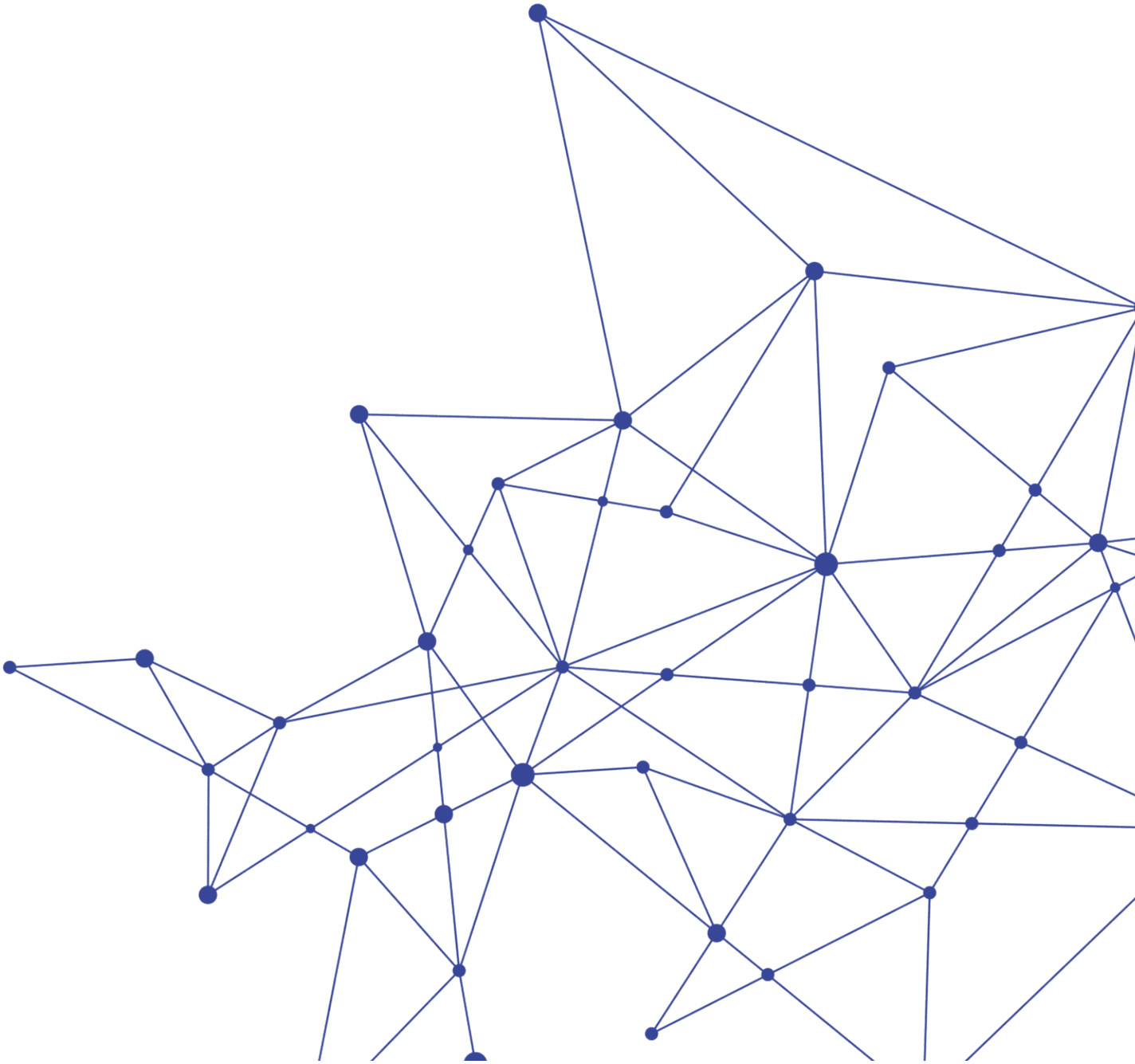
Compliance oversight presents cultural and commercial challenges for organizations and their investment partners. Determining the level of compliance control to apply to these relationships and how is a key concern for compliance leaders. 41% report a lack of cooperation from joint ventures and investment partners, which they say makes it impossible to ensure a consistent compliance response. A further 35% say they have no way of knowing whether these partners are compliant.

Complete ignorance to potential risk among investment partners is not a position any compliance leader is comfortable with, but nor does effective compliance oversight mean total control. While it makes sense to insist that majority investments and acquisitions adopt and report against the compliance framework of the corporate center, the calculus is less clear cut for minority investments and joint venture partnerships. Enforcing the full range of compliance program elements across an organization's entire investment portfolio is both practically burdensome and potentially counterproductive to encouraging compliant behavior — failing to account for cultural norms and the need to secure buy-in from investment partners. Further, it needs to be recognized that for some legal risks, the higher the degree of compliance control, the closer organizations and their investment parties are likely to be associated when it comes to legal liability and resulting reputational damage.

Defining a coherent corporate philosophy for dealing with compliance in a way that reflects the investment relationship and the associated legal risk, and applying this logic consistently is critical. What is the organization's appetite for control? Companies should consider at the outset of any investment the principle risks any relationship gives rise to and establish the prevailing legal framework — particularly in relation to highly complex joint venture partnerships. Understanding the legal framework creates the ability to select the appropriate solution to manage the key legal risks in the particular circumstances. This means engaging compliance teams earlier in investment decision-making, so that they can facilitate successful execution of the strategy by ensuring risk doesn't undermine value.

Technology is supporting compliance teams to implement best practice and manage risk among investment partners. According to our research, 45% of compliance leaders plan to deploy technology to monitor their actions and behaviors. We are seeing a rise in the use of risk assessment tools to conduct pre-partnership due diligence as well as oversight on an ongoing basis — streamlining the process of capturing and maintaining information that enables the identification and assessment of compliance risks. This trend is likely to accelerate as new technology comes to market.

Artificial intelligence (AI) is particularly useful in managing third party risk. This technology mines, collates and analyzes public source information relating to investment partners to make connections that otherwise may not be made and highlight risks that may otherwise remain hidden. Used in this way, AI can provide greater insight and transparency on investment and procurement decision making — making it easier to assess potential hotspots.



Baker McKenzie.

# Technology as a driver of compliance integration and business growth

# Snapshot

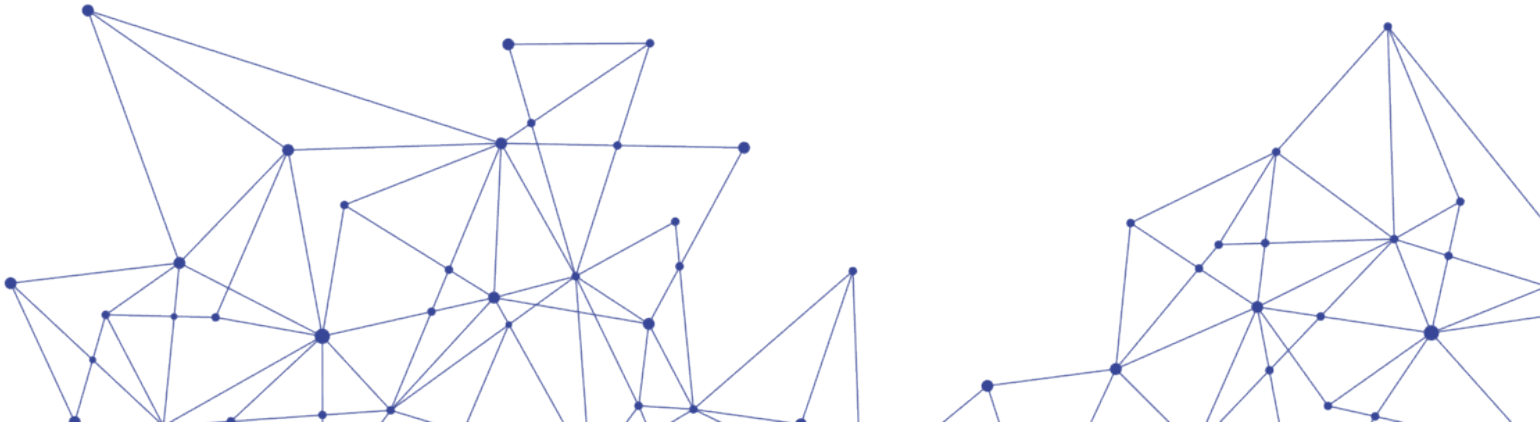
- Organizations with tech-enabled compliance teams are more likely to experience fast growth – with turnover rising by more than 10% in the past year.
- Leaders in these tech-enabled compliance functions expect to achieve 10% greater ROI on spend compared to others.

**Technology is not a panacea for managing risk. But our research shows that it is a key driver of compliance integration and business growth — reaffirming the findings of our original Connected Compliance** research.

Compliance teams that are deploying technology in more sophisticated ways — anticipating regulatory risk, focusing on value and championing innovation — report higher performance and greater return on spend.

Organizations with tech-enabled compliance teams are also more likely to experience fast growth – with turnover rising by more than 10% in the past year. And while there is little difference in the amount these organizations invest in compliance technology compared with the average (just USD 360 thousand), tech-enabled compliance teams expect to achieve 10% greater ROI on spend than others.

However, maximizing the value of compliance technology is still challenging for many. Only 56% of compliance leaders report that compliance technology is effectively achieving its primary purpose and 63% agree there is value yet to be realized from their digital tools.



# Rio Tinto:
# Customized and Collaborative Tech-enabled Compliance

**Insights shared by Stephen Storey, Chief Ethics and Compliance Officer, Rio Tinto (UK)**

In Ethics and Compliance, we look at investment in technology by asking ourselves what problems we are trying to solve and what do we want to achieve, then customize solutions to suit our specific needs. Our focus has been on how we use compliance technology specifically to better monitor and analyze data, inform our business integrity risks and to connect our internal teams and make efficiency gains in the compliance team.

The importance of using data strategically cannot be overstated. We operate a tailored information hub, to which behavioral science technology can be applied to map behavior based on disclosures and other key data held within it. The core benefit of having this in one place is an integrated, bespoke picture of emerging behaviors and profiles as they are linked to technology use. This enables us to connect data points that translates into learnings for onward compliance program action — we identify the key focus areas and decide where we need to target better training, resources and launch campaigns to raise awareness for monitoring activities. We are also able to create messages that are leader-led to raise flags that teams should be looking at. This allows us to build better, stronger bridges and facilitates embedding integrity across the business.

We have also evolved our monitoring program quite extensively, including bringing the right talent on board to harness data in strategic ways. Our data scientists build analytics based on scripts and automation, allowing us to boost efficiency through the production of automated compliance reports. The output is designed solutions that are demonstrable, valuable and actionable enabling our compliance teams to focus resources to risk. Reports can be used to communicate our suggested actions to the business, which then inform our tailored regional and global compliance plans. This is not only great for cost saving, but also allows us to create many more efficiencies for the compliance team.

Regulators can and should do more to further help incentivize compliance teams to learn from other effective practice through better sharing insights gained in enforcements matters into compliance program evaluations in relation to the use and application of technology. Rather than more guidance, practical examples and case studies to promote tech-enabled risk-based compliance programs would encourage organizations to proceed with more certainty.

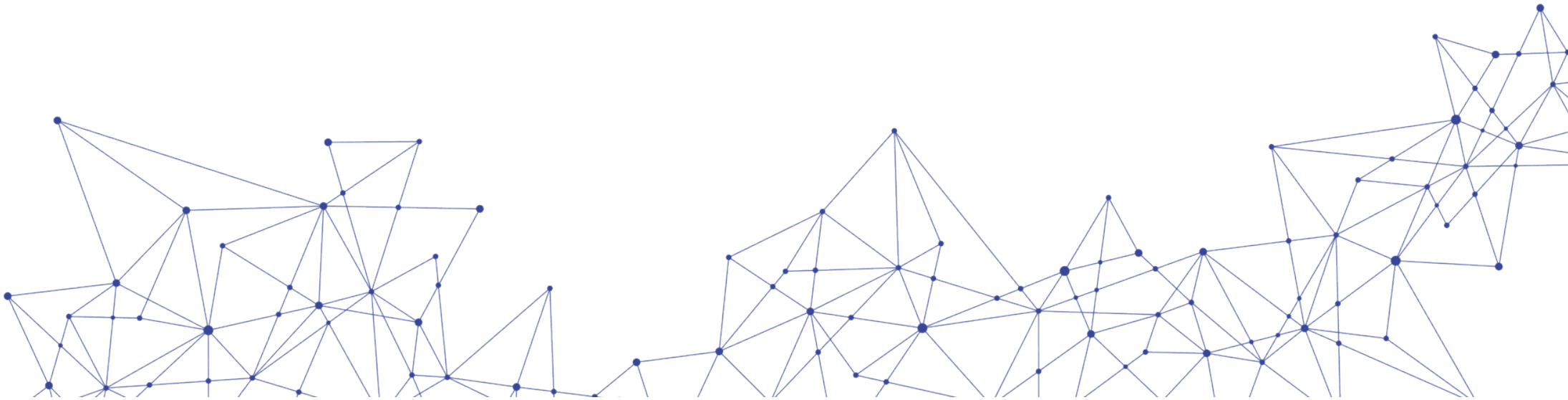
# Five key steps to tech-enabled compliance success

**Insights shared by Stephen Storey, Head of Group Ethics and Integrity, Rio Tinto (UK)**

**1. Feed back into the corporate process.** One of the best things about what we've managed to achieve at Rio Tinto is that, by integrating some key technology outputs, these systems and processes are feeding back into a corporate process. If tools are held in isolation in the four corners of your program, they can't "speak" to the processes that ultimately go to executives or the board. And if your programs and data are not helping to identify principal risks, then those programs or data in and of itself creates a principal risk.

**2. Return on investment is key.** For anyone that considers or wants to sell connected compliance tools to their management, they need to make the proposition attractive in a number of different ways. Firstly, it is essential to highlight some of the material benefits in terms of cost and efficiencies. Secondly, there has to be a consideration on how these tools shift the dial on risk. Thirdly, the focus should be on trying to integrate compliance-related processes with other technology outputs — using these learnings to build and improve a global enterprise risk management platform.

**3. Be prudent with technology decision making.** There are technologies that profess do one thing, but when you really get into the detail, are unable to deliver against objectives. Sometimes, it is only when you get "under the hood" of the contract or program, or when you are in the implementation phase, that you start to uncover some of the material flaws in the design. At this point, there is rarely a silver bullet solution.

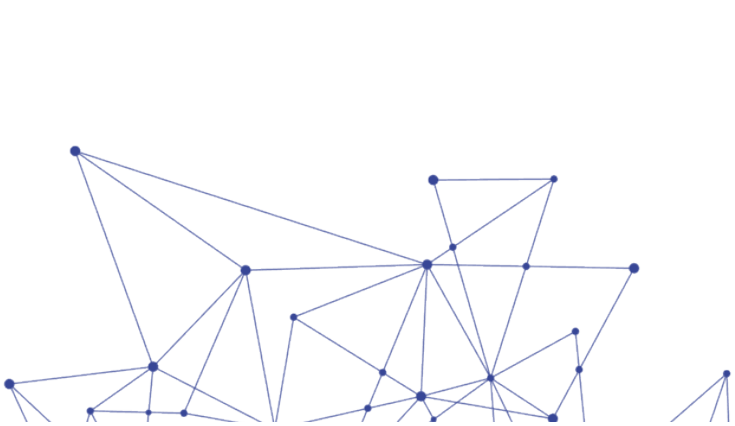


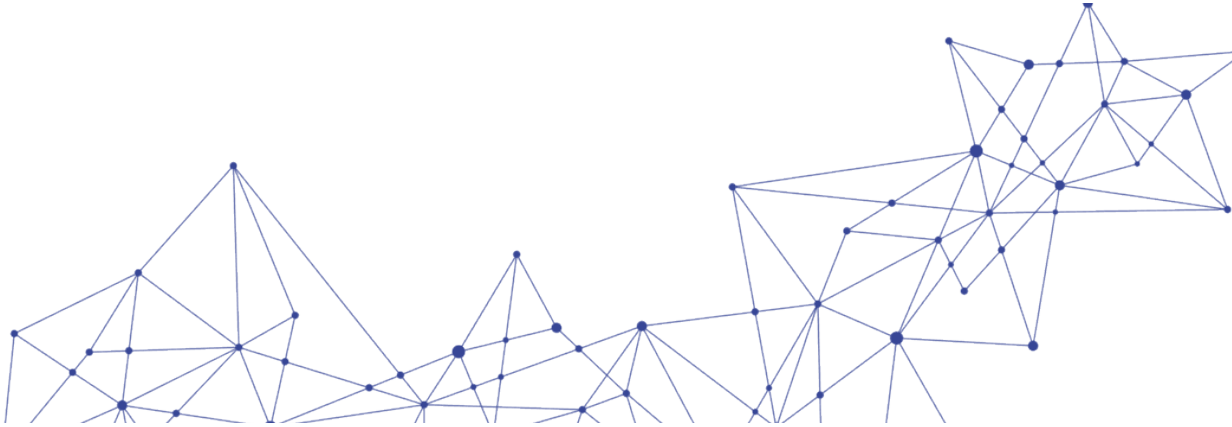
**4. Avoid the risks of overreliance or over customization.** A huge risk in this age of tech-enabled compliance is an over reliance on technology. There is no replacement for qualitative assessment, where the human mind interprets risk areas in a way that considers core business issues and communicates this information in a way the business understands. Another risk is over customization — where companies add too much to the script of their digital compliance tools and the back—end IP becomes unstable.

**5. Don't find false comfort in tech-enabled compliance.** Every technology has its limitations and is subject to failure. But in this case, the business is at stake. There is a need for the internal compliance team to map, inform and help conduct risk assessments of technology. For example, knowing the risks if a particular process doesn't work, or the technology fails or there is a material bug that will undermine insights.

"The value of compliance data is only as good as the viability of the technology and the ability to interpret it accurately and action it appropriately. In compliance investigations, there is a very specific and valuable skill set associated with analyzing and attributing appropriate weight to key evidence. The same applies to technology. Compliance leaders must be in a position to know and understand whether risks exist. For example, determining if data gaps are apparent because there are true gaps in the information available, or because of a failure in the technology itself. Without this knowledge, regulators could lack confidence in the robustness of internal compliance processes and investigations."
**Joanna Ludlam,**
**Co-chair, Global Compliance & Investigations**

*1. The views and opinions expressed in this article are those of the contributor and do not necessarily reflect the official policy or opinion of the Rio Tinto Group.*





# Data break out — comparing technology adoption and risk around the world and by sector

## How technology-enabled are global compliance teams?

### Pivot to digital

In response to COVID-19 disruption, organizations in China & Hong Kong have accelerated the pivot to digital products, approaches and tools faster than peers. 72% of leaders say the pandemic has increased their organization's focus on technology.

Companies in Brazil (53%) and the US (52%) have seen digital transformation efforts similarly galvanized by COVID-19.

### Investment in compliance technology

Organizations in the US are making the most significant investment in compliance technology at over USD 5 million per company — this is double the smallest average investment.

Compliance leaders in China & Hong Kong are most likely to state that investment in compliance technology will increase as a result of COVID-19.

### Technology adoption

Compliance leaders in Europe are at the cutting edge of technology. Organizations in France plan to adopt key digital tools including machine learning (56%), artificial intelligence (52%) and big data (38%) in greater numbers than global peers.

Similarly, leaders in Germany have their sights set on blockchain (55%) and automation (54%), and UK leaders plan to implement Software-as-a-Service (36%) more often than others. Compliance leaders in Africa and the Middle East are particularly interested in implementing predictive analytics (52% and 50% respectively).

## Rising risk

The hurried pace of digital change is creating heightened organizational risk. This is particularly apparent in China & Hong Kong, where 74% of leaders report that pressure to pivot to digital products, approaches and tools as a result of COVID-19 is dramatically increasing the risk exposure of their organizations.

Leaders in China & Hong Kong are also most likely to report that their organization is employing technology without considering compliance risk (54%). As a result, 59% say their company has already experienced a compliance investigation.

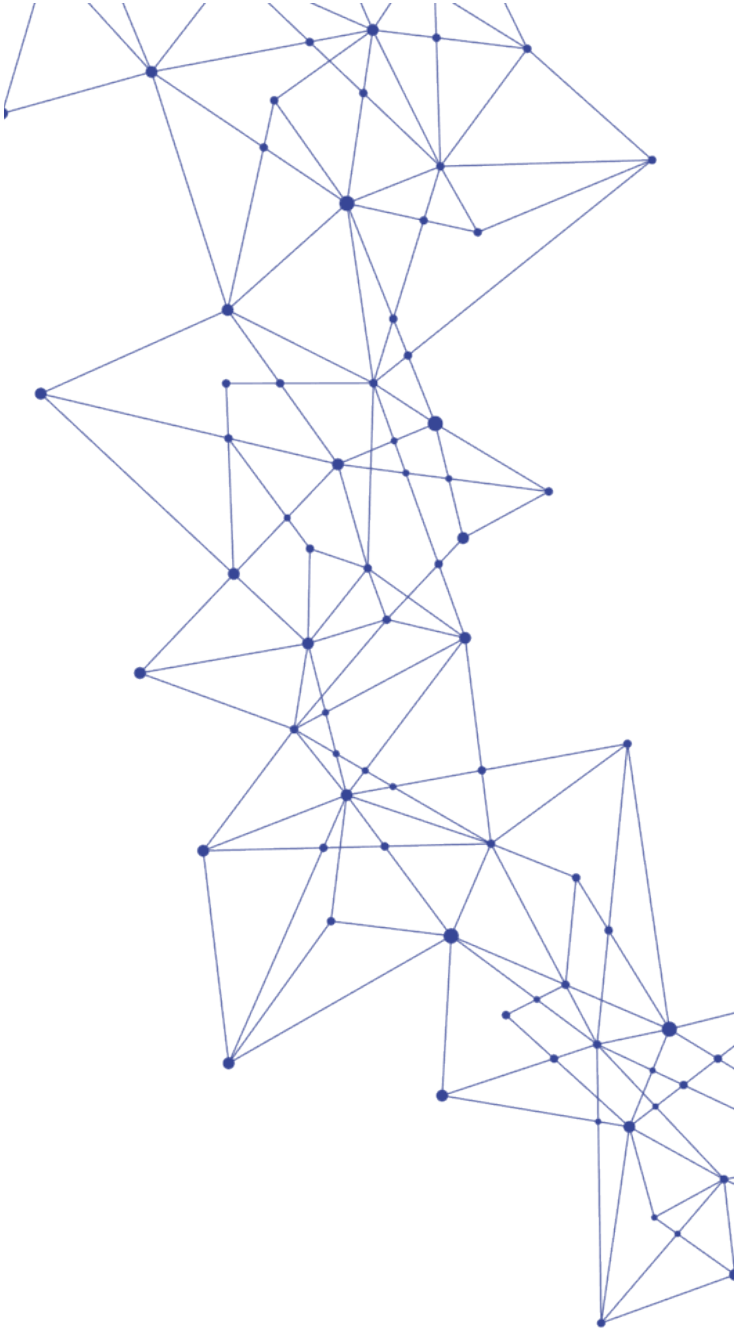
Organizations in Africa are least likely to employ technology without due attention to compliance risk (20%) and relatively few have been subject to a compliance investigation as a result of poorly implemented business technology (26%).

## Effectiveness of compliance technology

Organizations in Singapore are most successfully extracting value from their compliance technology. A comparatively low 47% of leaders in this jurisdiction report that there is value yet to be realized from existing investments, compared to 84% in China & Hong Kong.

64% of compliance leaders in Singapore also state that smart application of technology has enabled the compliance team to reduce its administrative burden and focus on adding value to the business. However, this is still a way behind Brazil, where 89 per cent of leaders report being able to devote more time to strategic matters as a result of smart compliance technology.

Leaders in Brazil were also the most likely to state that compliance technology is achieving its primary purpose.



## How technology-enabled are compliance teams in key sectors?

### Pivot to digital

In response to COVID-19 disruption, organizations in TMT have accelerated the pivot to digital products, approaches and tools faster than peers. 57% of leaders say the pandemic has increased their organization's focus on technology.

By contrast, organizations in Energy & Infrastructure (41%) and Industrials (42%) report that COVID-19 has had a relatively low impact on digitalization plans.

### Investment in compliance technology

Organizations in the Energy & Infrastructure sector are making the largest investments in compliance technology — USD 4.7 million on average per organization — which is closely followed by the TMT sector at USD 4.6 million.

Compliance leaders in Healthcare & Life Sciences are most likely to state that investment in compliance technology will increase as a result of COVID-19 (41%), alongside those in TMT (40%).

### Compliance technology adoption

Compliance leaders in Consumer Goods organizations are at the cutting edge of compliance technology. Organizations in the sector plan to adopt key digital tools including artificial intelligence (53%), automation (53%) and machine learning (52%) in greater numbers than global peers.

Similarly, leaders in Financial Institutions have their sights set on blockchain (66%) and Software-as-as-Service (37%).

## Rising risk

The hurried pace of digital change is creating heightened organizational risk. This is particularly apparent in Financial Institutions — where 52% of leaders report that pressure to pivot to digital products, approaches and tools as a result of COVID-19 is dramatically increasing the risk exposure of their organizations, compared to 40% in Healthcare & Life Sciences.

Leaders in Financial Institutions are also most likely to report that their organization is employing technology without considering compliance risk (40%). As a result, 46% say their company has already experienced a compliance investigation.

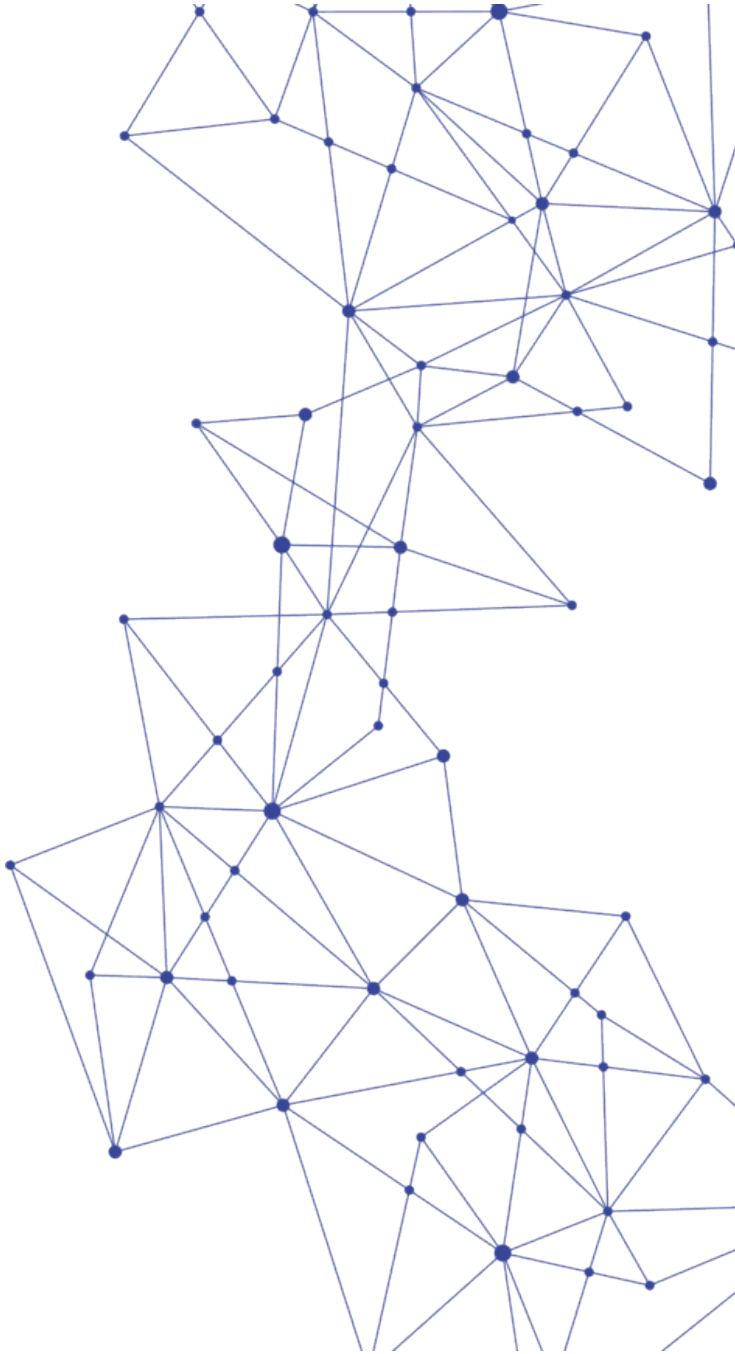
Industrials are least likely to employ technology without due attention to compliance risk (29%), yet 38% have still been subject to a compliance investigation as a result of poorly implemented business technology.

## Effectiveness of compliance technology

Organizations in Consumer Goods are most successfully extracting value from their compliance technology. 59% of leaders in the sector report that there is value yet to be realized from existing investments, compared to 68% in Financial Institutions.

Compliance leaders in TMT are also performing well. 76% state that smart application of technology has enabled the compliance team to reduce its administrative burden and focus on adding value to the business, compared to 67% in Energy & Infrastructure.

Similarly, leaders in TMT were also the most likely to state that compliance technology is achieving its primary purpose (66%) compared to Energy & Infrastructure (48%).



Baker McKenzie.

# Conclusion

Leveraging the CASE framework for continued success

What can we learn from how tech-enabled compliance teams leverage digital tools for integration, that can ensure compliance leaders maintain and build on progress made?

## Collaboration

Break down internal silos and create shared responsibility for compliance across the organization — using technology to provide a shared platform for knowledge and cross-functional collaboration.

## Agility

Anticipate regulation and emerging organizational issues with technology — identifying and preparing for new areas of risk.

## Strategy

Leverage technology to reduce the administrative burden — focusing your team on protecting commercial value — and pioneer new tech-enabled solutions to key business challenges.

## Effectiveness

Avoid wasted effort and duplication — analyzing risk data to match compliance resources to greatest organizational risks.

"Digital risk is building a growing case to involve the compliance function in technology decision making — lending expertise to robust due diligence and contracting processes. However, this may not go far enough. As the digitalization of business models expands, increasingly new risk is inherent within products sold. For example, we have seen enforcement action against software companies that sell solutions designed to manage and transfer data, that could be said to facilitate collusion and anti-competitive practices. As digital risk is baked into revenue streams, there is space for compliance to take on a new strategic role in specifying and advising on the development of new products."

**Luis Gomez**
**Chair, EMEA Competition Group**

**How connected is your compliance function?**

Benchmark the performance of your setup against our extensive global compliance database, to highlight areas of strength and key actions to improve integration.

https://connectedcompliance.bakermckenzie.com/

Baker McKenzie.

# Key Contacts

# Contacts

**Joanna Ludlam**
Co-Chair, Global Compliance & Investigations Group
Email
Bio

**William Devaney**
Co-Chair of the Global Compliance and Investigations Group
Email
Bio

**Luis Gomez**
Chair, EMEA Competition Group
Email
Bio

**Ben Allgrove**
IP, Data & Technology Partner & Global Head of Research & Development
Email
Bio

**Tristan Grimmer**
Co-Chair, EMEA Compliance & Investigations Group
Email
Bio

**Christoph Kurth**
Head, Zurich Compliance & Investigations Group
Email
Bio

**Jennifer Klass**
Co-Chair, North America Financial Regulation & Enforcement
Email

**Jessica Nall**
Compliance & Investigations Partner
Email
Bio

**Julia Wilson**
Employment & Compensation Partner
Email
Bio

Baker McKenzie.

# Our Resilience, Recovery & Renewal Model

## The Resilience, Recovery & Renewal Model

Our Resilience, Recovery & Renewal model is helping organizations navigate the business and legal impact of the COVID-19 pandemic. While most businesses will pass through all three phases of the model, the phases themselves are non-linear and may recur or overlap, particularly for those with global operations. Wherever you are in your response to the pandemic, we will help you with the services and resources you need. Visit our Resilience, Recovery & Renewal Roadmap to Stability hub for more information. Also, visit our Beyond COVID-19 Resource Center for the latest legal and regulatory updates from around the world.

Baker McKenzie.

Thank you for reading

# Connected Compliance 2020