KPMG

# Transforming Compliance in financial services

November 2023

home.kpmg

# Contents



# Introduction: Drivers for Change

Compliance functions have gone through a major period of growth and investment. Many firms have seen a massive expansion in their Compliance functions. Despite this, they have been put under significant strain driven by the external market conditions, increased adoption of digitalisation, developments in operational and financial resilience increased focus on consumer outcomes and the implementation of ESG obligations.

As a result of these challenges, firms are realising that they need to improve: the (i) effectiveness and (ii) efficiency of the Compliance function. In this paper, we focus on how Compliance can meet these twin objectives.

Since 2008, Compliance functions have increased their resources and have widened their range of tasks, with a dramatic increase in their monitoring, supervising and surveillance activity, whether manual or substantially automated.

This growth has reflected, in part, the post 2008 regulatory reform agenda (including not only resilience and resolution requirements, but also a host of retail conduct, wholesale conduct, anti-money laundering, governance, culture and individual accountability requirements), more intensive and intrusive supervision, and the impact of Brexit and COVID-19. Whilst some of these initiatives have, undoubtedly, enabled firms to be more resilient, with others nonetheless placed firms under considerable new stresses and firms have been keen to learn the lessons.

Compliance functions now have an increased profile and higher expectations placed upon them. These expectations have never been higher than in the aftermath of the pandemic, when the financial sector played a critical role in supporting the economy and grappled to understand and manage the resulting risks of doing so.

Combining this with immense cost pressures on financial institutions has led to increasing pressure on Compliance functions to transform into a more value-add service line that can deliver more effectively and efficiently.

Moreover, despite having strengthened the control requirements, the focus and mindset of Compliance in many firms remains overly risk-averse and still struggling with the remediation of past problems, resulting in limited bandwidth to proactively support – as well as continuing to challenge – the business. This focus may be partly the result of perceptions of regulators' expectations.

In addition, in some firms there is a lack of clarity over the mandate and role of Compliance, how it fits within the three lines of defence, and the relationship between Compliance and the business.

# Compliance needs to:

- Support and challenge the business effectively, by adapting to changes in the business itself. (See chapter 02)
- Operate in a much more strategic and predictive capacity.
- Spend less time fire-fighting, with a greater focus on making strategic investments to ensure a more proactive approach to risk identification.
- Revisit the mandate of the Compliance function. (See chapter 03)
- Take a consolidated view of the skills, capabilities and experience across the Compliance function, together with periodic assessment of where there are gaps between the current skills and capabilities and those necessary to effectively deliver the mandate. (See chapter 04)
- Reconsider the skillsets they hire, with more diverse and experienced professionals to complement existing Compliance expertise.
- Increase their efficiency through greater use of technology, and more focus on data and process optimisation. (See chapter 05)

# Supporting the business as a strategic business partner

Compliance can only support and challenge the business effectively if it evolves in response to changes in the business itself and is fit for future financial services.

In recent years, business activities have developed in five main ways - all of which have implications for Compliance

First, as regulation has become more important in shaping business strategy, front-office management (the first line of defence) has become increasingly involved in analysing and implementing regulatory reforms.

Second, front-line business functions have taken on greater responsibility for customer due diligence and other financial crime regulatory requirements, some credit and insurance underwriting sanctioning, some surveillance activity and, in some cases, complaint handling.

Third, accelerated by the pandemic, many firms are looking to leverage technology so they can respond in an agile way to future changes in external conditions with this new reality. Compliance needs to keep up with the pace of change here, in particular to deliver compliance with information technology security, the control, security and privacy of data, artificial intelligence, cyber security, outsourcing, anti-money laundering, regulatory reporting and associated obligations. Further, as automation underpins and accelerates the journey of firms towards digital transformation, new technology applications may interact establishing complex digital eco-systems - Compliance will need to inform its mandate, redefine its strategic capabilities and adapt its operational methodologies in alignment with new internal and external requirements. The application of new technologies by firms requires a commensurate set of targeted policies and controls. For example, regulators increasingly emphasise the importance of operational resilience and collaborate broadly in mitigating artificial intelligence risks.

Fourth, business models and organisational structures are changing as a result of the pandemic, the UK's departure from the EU, competitive pressures and wider market developments.

Fifth, in some firms, the focus is shifting from silo-based and risk-based Compliance functions to functions that support individual business service lines (for example private banking, wealth and asset management, general and life insurance, and retail, corporate and investment banking).

Compliance functions need to adapt to changes in the business itself in order to support and challenge the business effectively, not least the increasing use of data and technology by the business. They need to transform from functions focused on preservation, conservativism and remediation to ones that, in addition to maintaining regulatory compliance and capital conservation, operate in a more strategic and predictive capacity.

This in turn requires Compliance functions to spend less time fire-fighting, with a greater focus on making strategic investments to ensure a more proactive approach to risk identification and customer outcomes. By utilising, and engaging with, evolving technology and data analytics, the Compliance functions will be better able to address hotspots and prevent issues before they occur.

## Case study

In October 2022, the Bank of England and the FCA published a **survey** to better understand the applications of AI and gain deeper insight on its adoption in the industry. The survey's findings pointed to an accelerating use of AI in financial services - with enhanced data and analytical capabilities, operational efficiency and better detection of fraud and money laundering highlighted as key positives.

The FCA seeks to promote the benefits of AI technologies for consumers and firms and innovates for better AI outcomes: it has made available the Digital Sandbox, develops a regulatory framework for AI and it is building its synthetic data expertise.

# Mandate of the Compliance function and its position within the three lines model

It is important that the Compliance function's mandate and desired outcomes are absolutely clear, understood by internal and external stakeholders, and maintained to support business strategy, growth and innovation.

There should be a clear assignment of responsibilities and accountabilities for the Compliance function, to prevent any confusion over roles and responsibilities and to prevent any overlap and duplication of activities and conflation over risk ownership. Once set, this demarcation should be policed and enforced.

## Redefining the Compliance function mandate

The core activities of Compliance generally include:

- Regulatory compliance – monitoring whether the firm meets its regulatory obligations.
- Independent oversight of business activity – ensuring that compliance risk is identified, managed and mitigated effectively.
- Whistleblowing, management of conflicts of interest and personal account dealing.
- To ensure the impacts of such changes on the conduct and regulatory risk profile are understood and managed. Advising, supporting and challenging the first line of defence on regulatory changes and internally-driven developments (the degree and type of challenge may vary considerably across firms).
- The design, documentation and maintenance of compliance frameworks.
- Providing training on regulatory risk.

A number of firms have amalgamated Compliance and Risk (operational or conduct risk) teams or functions that work closely together due to the interplay of these activities and types of risk.

Beyond this, the key drivers of change outlined in chapter 02 and the importance of Compliance adapting continuously to the changing environment and evolving responsibilities suggest that there can be considerable value to firms from Compliance taking on additional activities. Equally, however, this is often where challenges can arise as there is a general tendency to push items that the business does not want to address into Compliance.

Compliance needs to focus its role on a combination of providing independent oversight whilst being sufficiently engaged to advise and challenge business decision-making. This focus can be challenging to maintain, particularly in a stress situation like the immediate response to the pandemic, where some compliance staff were temporarily moved into the first line to help support it with capability or capacity gaps.

Compliance also needs to be empowered to operate at a business model and propositions level, so as to contribute to addressing the material risks and conflicts that may arise. At a more operational level, the right involvement and challenge from Compliance can add value to defining target markets, robust and objective product governance, and solution design.

**The Compliance function may therefore take on additional roles, focusing on where it can add the most value, such as:**

- Providing the value of a 'centre of excellence' on regulatory requirements, not just exercising an advisory role.
- Taking a more strategic and proactive approach to risk identification and risk monitoring.
- Taking a more principles-based approach (considering how a firm defines what a regulatory principle or high-level regulatory requirement means for the firm and what the firm should do to meet it by focusing on the outcomes rather than focusing only on more detailed rules and prescriptive controls.
- Focusing more widely on conduct risk and the delivery of good customer outcomes.
- Inputting actively and constructively to remuneration decisions and to new product development.
- Helping the Board and senior management to communicate and to reinforce a strong compliance culture across the firm, including focusing on the underlying conduct and cultural drivers of behaviour and supporting and embedding wider cultural and behavioural change.
- Contributing more actively to challenging and delivering the firm's strategy, business plans and propositions.

## Reviewing and re-organising the operating model perimeters and interfaces

Within a three lines model, as discussed in chapter 02, there has been movement of functions that were previously in the second line of defence to the first line, as some firms have moved towards a more empowered first line with a clear understanding of its role in delivering compliance and risk management.

But this has not been entirely one-way traffic – there have also been examples of some surveillance activity moving from the first line of defence to Compliance. Such organisational change is likely to continue in the coming years, especially as firms adapt to the new post-pandemic reality.

Meanwhile, in some firms there have been examples of business areas not properly engaging with Compliance and viewing the function as a business inhibitor, perhaps reflecting in part a tendency for opaque and protracted decision-making of middle management in Compliance, which itself may be due to a lack of clear empowerment and delegation, or a tendency towards risk aversion/avoidance. The right balance needs to be found between the independence of the Compliance function and its close collaboration with the business.

Together with the shifts in the ways that Compliance needs to support the business, there is therefore a need for clarity on – and a clear shared understanding of – the role and purpose of the Compliance function.

**This should also be useful in identifying and resolving any areas of inefficiency, duplication or confusion. This requires:**

- A more effective proactive apportionment of certain activities between the first and second lines and clarity over the shifting boundaries between them.
- Clarity over the key risk management and oversight outcomes consistent with the mandate of the Compliance function, including a clear specification of the associated priorities, activities, tasks and resource, infrastructure and control implications.
- Clarity over how Compliance balances its role as an advisor to the front line with its role of providing challenge. The role and responsibilities of Compliance should enable it to provide independent and objective oversight.
- Clarity over the apportionment of responsibility across second line functions, and the interactions between these functions, including Compliance, Risk, Financial Control and Legal.
- Clarity over the interaction between Compliance and the third line (Internal Audit). A key question here is whether Compliance should undertake any 'assurance' activities, or whether risk assurance activities should be performed solely by an independent assurance function. Internal Audit may not have sufficient experience and expertise to perform oversight on some key functions, leading to an increasing trend toward a co-sourced model, where required.

This clarity should be useful for developing core outcomes, management information and key performance indicators for Compliance. There may also be implications for the internal organisation of the Compliance function, in terms of its various roles in advising, monitoring, surveillance and testing. This may include centralising some activities within Compliance, such as regulatory training, to achieve economies of scale and avoid any duplication or unnecessary use of resources.

On the positioning of Compliance, there has been a trend in recent years for Compliance to move to reporting to the CRO (or CEO), away from the CFO, Head of Legal, or COO. There are good reasons for this, not least to provide the over-arching view of risks and risk management that is required of a CRO. Compliance should be regarded as being very much part of the risk universe.

> **Should compliance undertake any risk assurance activities - or should these activities be performed solely by an independent assurance function.**

# Resourcing implications for Compliance

Once the mandate, roles and responsibilities of Compliance are clarified it should be possible to translate this into key priorities, key activities, and the skills, competencies and resources required for the function to be capable of discharging its mandate effectively. The Compliance function also needs to be organised in a way that maximises efficiencies. Helpfully, changes in working patterns as a result of COVID-19 are providing firms with access to a wider talent pool and greater flexibility around how, and where, they source their talent.

The precise mandate and approach agreed for the Compliance function will have implications for staff resourcing. One objective here may be to move towards an integrated Compliance team with fewer staff and greater knowledge sharing. The way forward will vary across firms, but consideration should be given to four main areas of development:

## Expertise about the business

Business and product knowledge are required to understand and effectively challenge business (first line) activities. For example, as firms adopt fintech applications – digitalisation, artificial intelligence, data intensive operations, cyber security and new products or business models – Compliance may require an increasing reliance on data scientists and technology specialists, and on more advanced and specialist training. Consideration should be given to the use of rotating secondments to the business and technology functions of the firm.

## Ability to face off with the business

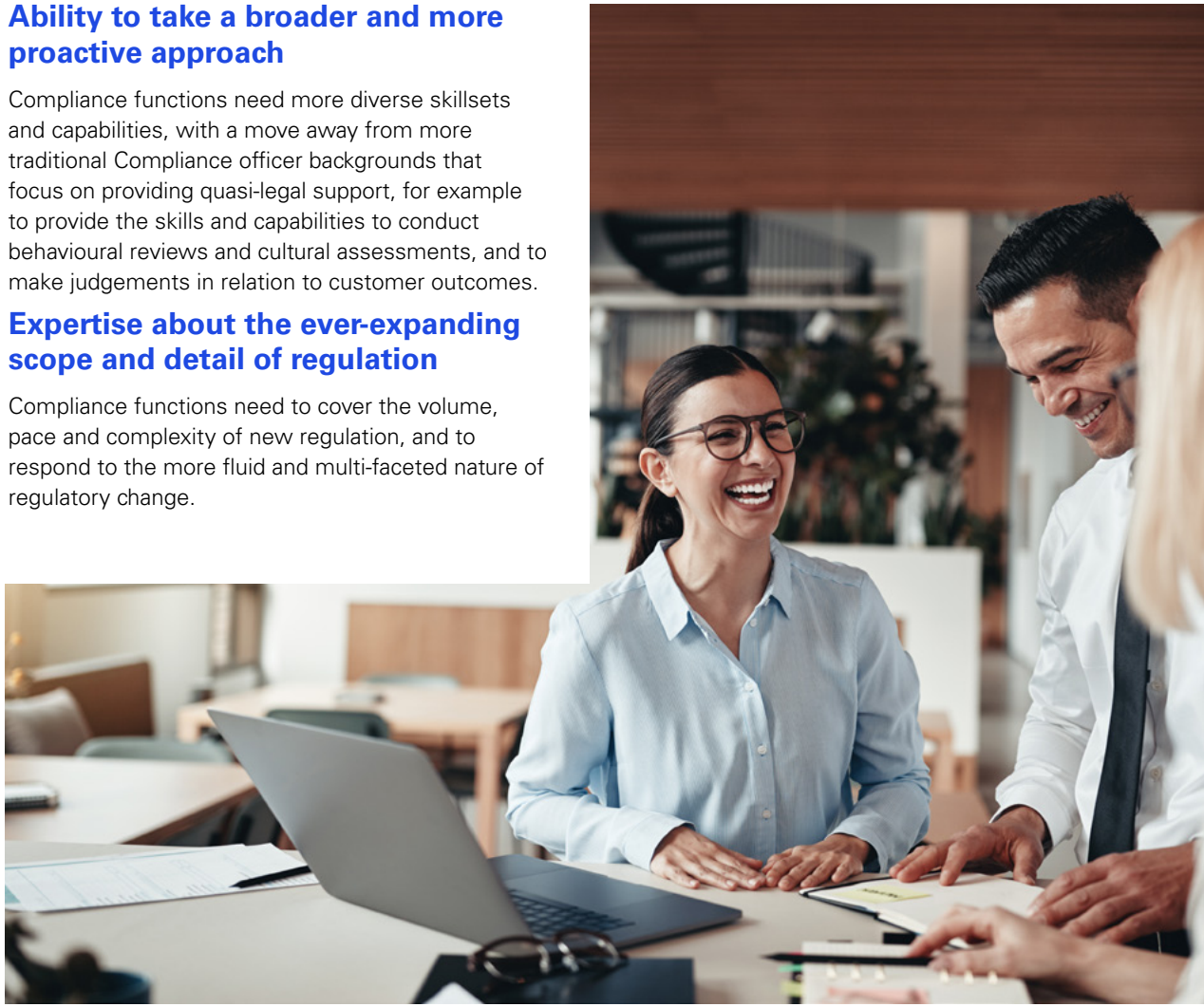
Compliance staff need the interpersonal and influencing skills and credibility to enhance the effectiveness of their challenge of the business. Personal and functional delegation should provide sufficient empowerment, while personal responsibilities and accountability should be clearly defined and documented to enable effective decision-making. Compliance staff need sufficient gravitas and understanding of the business, in addition to technical regulatory expertise. Ultimately, they need to be regarded as trusted advisers to the business.

## Ability to take a broader and more proactive approach

Compliance functions need more diverse skillsets and capabilities, with a move away from more traditional Compliance officer backgrounds that focus on providing quasi-legal support, for example to provide the skills and capabilities to conduct behavioural reviews and cultural assessments, and to make judgements in relation to customer outcomes.

## Expertise about the ever-expanding scope and detail of regulation

Compliance functions need to cover the volume, pace and complexity of new regulation, and to respond to the more fluid and multi-faceted nature of regulatory change.



# Effectiveness and efficiency gains driven by data and technology

Data and technology are key to improving the effectiveness and efficiency of Compliance functions and to driving a more innovation-driven mindset and transformation. Smart deployment of data and technology supports sound decision-making and the identification of events and risks through value-add analytics and insights, which should have an impact on the firm meeting its business plan and strategic objectives while also meeting regulatory expectations.

There is considerable scope to use more technology to improve the effectiveness and efficiency of Compliance. This is likely to require significant investment, not just in technology to automate and improve operational and reporting processes, but also in the simplification and standardisation of processes, and in data enhancement and cleansing to support the development and migration towards artificial intelligence models (see the KPMG International report on 'Generative AI models — the risks and potential rewards in business' and the KPMG International article on 'Artificial Intelligence and Machine Learning: Regulatory approaches are being developed'. These disciplines extend beyond the technical competence of a traditional Compliance function.

**The potential rewards here are considerable. They include:**

- The more effective and efficient delivery of regulatory requirements.
- Using data quality and data analytics to identify and address issues before they occur.
- Establishing Compliance priorities on high risk areas identified from more sophisticated surveillance technology.
- The consolidation of multiple historical systems and platforms.
- Agile resourcing models including use of offshoring, near-shoring and outsourcing to complement a smaller, more specialised team.
- Greater automation and standardisation of manual processes.

A further potential reward is the ability to generate real-time management information and dashboards, moving away from management information reporting practices that are manual, resource-heavy and time-consuming to reporting that is clear, concise, effective and forward-looking. This allows the business and senior management to make real-time, sound and strategic decisions, and limits time wasted by interrogating and interpreting poor quality data.

As with other applications of technology, Compliance functions taking this path should recognise and take account of the potential risks involved. Technology changes and data cleansing can be very costly and may involve complex transformations from multiple legacy systems. Technology-based solutions need to be resilient and robust, while data need to be not only of high quality but also both comprehensive and secure. Artificial intelligence systems carry the risk of bias, which needs to be minimised through transparency, explainability, process verification and algorithmic model testing.

Whilst technology is a mechanism by which effectiveness and efficiency can be delivered, it is not necessarily free from risk. KPMG professionals have seen many firms introduce digital or technological solutions in response to the new conditions of the pandemic, but Compliance functions will need to keep pace as regulators start to determine how best to regulate AI, for example. Equally, considering data ethics alongside meeting data protection obligations will add to the complexity, as firms expand their use of technology and data.

## Building capacity

Using technology to increase, enhance or streamline surveillance and/or monitoring capabilities; building robust, targeted surveillance reports that allow Compliance to focus quickly on specific risks or business activities; and using advanced data analytics and visualisation to help Compliance discharge its mandate.

This is of increased importance where the Compliance function is likely to have reduced physical oversight as working is split between office and remote working for a sustained period.

## Robotic automation of existing manual processes

Using chat bots to answer basic queries, for example on gifts and entertainment policy, and conflict of interest policy.

Investing in artificial intelligence software can allow staff to interact with a chat bot to answer their non-complex and non-advisory compliance-related queries, thus cutting down on time and resources to answer straight forward queries on standardised compliance advisory processes. These chat bots can leverage Natural Language Processing, Machine Learning and Semantic Analysis in order to ensure they remain relevant.

An appropriate use case, the successful design and implementation of the relevant technology are critical. However, of equal importance are ensuring that there are appropriate controls in place in relation to data ethics, model risk management, culture and corporate governance.

## Regulatory change

Interpreting new regulations and implementing them into day-to-day operations can be very labour intensive and complex.

Creating an automated inventory of regulations, laws and obligations from global regulatory sources using artificial intelligence allows for real-time notification of new rules and proposed rule changes, tracks regulation life cycles and enables a quicker impact analysis when obligations change (through the mapping of regulations to applicable controls).

### Case study

A US financial institution has created a centralised library of regulatory obligations relevant to its material legal entities across the world and utilised technology to map those obligations to the firm's policies and procedures. This taxonomy has given visibility, through a technology interface, of the obligations that impact the businesses' activities and the key policies and procedures by which those requirements are addressed, ensuring effective line of sight for executive sponsors and empowering Compliance activity in the first line.

## Financial crime prevention

Using data mining, advanced analytics and the monitoring of different communication channels to improve the monitoring and surveillance of financial crime and trading activity.

Advanced eDiscovery tools can monitor communications and identify word patterns, sentiment and understanding, which is of significant value in both wholesale and retail firms (for example, call monitoring, controls monitoring and complaints processing). Innovative solutions driven by data and technology can enable greater coverage, faster feedback and improved effectiveness for less cost. COVID-19 has increased the general level of fraud risk in firms, and given the scale of COVID-19 related lending and forbearance, technology will be a key mechanism to manage this risk.

The pandemic has seen increased volumes and volatility in the wholesale markets leading to increased volumes of alerts. Systems use algorithms and artificial intelligence based on expected customer behaviours and activity patterns. Abnormal spending patterns during lockdown have led to an increase in the number of false positives, which could increase the risk of a real fraud going undetected. Therefore, Compliance functions may need to recalibrate their surveillance systems to take account of changes in customer behaviour and possible further market volatility measures.

## Client due diligence, anti-money laundering and related alert systems

Employing a full end-to-end managed service solution that leverages information already submitted by the customer and produces a robust audit trail to perform financial crime risk checks.

This can be created using a bespoke cloud-based solution which includes an integrated customer portal, a work flow system that creates an auditable electronic customer file, and a document absorption and policy rules engine that absorbs, assesses and classifies unstructured data.

Intelligent software can also conduct research of millions of web sources across multiple languages, including open web, deep web and structured web, as well as premium subscription sources and a proprietary database of archived web sources, in order to provide thorough screening coverage. Machine learning can reduce false positives and irrelevant content, thus reducing time and costs, while improving overall quality.

## Innovative training approaches

Employing new agile training approaches to design and deliver digital based micro-learning module (able to be delivered or accessed remotely) that incorporate leading practice learning methods to enhance engagement and drive better understanding in the business of regulatory requirements.

# Roadmap to automating Compliance processes and activities

- Establish a plan ensuring that the level of automation is integrated with Compliance strategy and with the firm's culture and risk tolerance.
- Identify compliance processes, data and analytics that can be integrated and automated (including evaluating data availability and integrity) in order to allow an overall risk assessment.
- Set priorities by measuring benefits and limitations to help determine budgets, resourcing for pilots and timelines.
- Define a governance structure and change management approach, including communication strategy and training plans.
- Select a solution through partnering with the right solution provider or IT function.
- Evaluate existing technology, develop and integrate data and technology as needed and ensure it remains future-proof.
- Design a detailed implementation plan.
- Execute the plan and upskill the Compliance team in analytics to facilitate full use of data analysis, an ability to identify and address risks and to communicate insights to senior management as appropriate.

# Next steps in transforming Compliance

KPMG firms' specialists can help you understand what the issues raised in this paper could, in practical terms, mean for your Compliance function and how you could approach transforming compliance.

If you would like to discuss any of the topics above in more detail, please do not hesitate to get in touch with a member of the team overleaf.

## Adapt to the business

- Recognise how the business model is changing.
- Identify ways for Compliance to become more strategic and predictive in supporting and challenging the business.
- Pursue opportunities to add value.

## Role

- Establish a vision of future state roles and responsibilities of Compliance, with clarity on how this fits within a three lines of defence (or other operating) model.
- Determine a path for moving to this redefined operating model.

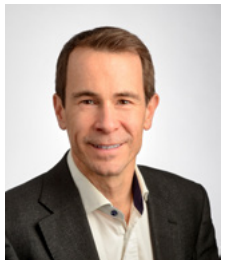
## People

- Perform competency assessment of current skillsets against future operating model resource requirements.
- Expand recruitment pool and review recruitment strategy to move away from traditional networks, recruit individuals froma wider talent pool as a result of increased remote working.

## Data and technology

- Identify opportunities for using data and technology to deliver a more effective and efficient Compliance function.
- Engage with technology functions to understand the existing technology platforms and infrastructure that could be leveraged.
- Allocate budget to exploring regulatory technology and consider partnering with external providers and new entrants to the market.

# Contacts

## Chris Steele

Partner, Regulatory and Risk Advisory

KPMG in the UK

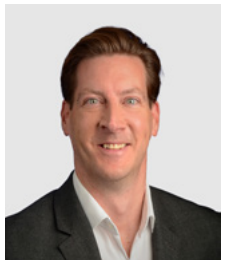
**E:** chris.steele@kpmg.co.uk

## Kate Dawson

Director, EMA FS Regulatory Insight Centre

KPMG in the UK

**E:** kate.dawson@kpmg.co.uk



## Philip Deeks

Director, EMA FS Regulatory Insight Centre

KPMG in the UK

**E:** philip.deeks@kpmg.co.uk

## Bernadette Moore

Director, Regulatory and Risk Advisory

KPMG in the UK

**E:** bernadette.moore@kpmg.co.uk

## Dave Lennon

Director, Regulatory and Risk Advisory

KPMG in the UK

**E:** dave.lennon@kpmg.co.uk

## Chris Coltella

Director, Regulatory and Risk Advisory

KPMG in the UK

**E:** chris.coltella@kpmg.co.uk

kpmg.com/uk



CREATE: CRT147809