Finance for Europe

Artificial Intelligence: Challenges and Opportunities for Compliance

September 2023

Association for Financial Markets in Europe
www.afme.eu

Disclaimer

AFME's *Artificial Intelligence: Challenges and Opportunities for Compliance* (the "Report") is intended for general information only and is not intended to be and should not be relied upon as being legal, financial, investment, tax, regulatory business or other professional advice. AFME doesn't represent or warrant that the Report is accurate, suitable or complete and none of AFME, or its respective employees shall have any liability arising from, or relating to, the use of this Report or its contents.

Your receipt of this document is subject to paragraphs 3, 4, 5, 9, 10, 11 and 13 of the Terms of Use which are applicable to AFME's website (available at https://www.afme.eu/About-Us/Terms-of-use) and, for the purposes of such Terms of Use, this document shall be considered a "Material" (regardless of whether you have received or accessed it via AFME's website or otherwise).

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers LLP, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

September 2023

Contents

Foreword

AFME in collaboration with PwC is pleased to publish 'Artificial Intelligence: Challenges and Opportunities for Compliance', a paper which comes at a critical time for our members.

Whilst Artificial Intelligence (AI) and Machine Learning (ML) models have been used within the financial services industry for nearly seventy years, the range and sophistication of use cases for AI and ML, and their subsequent adoption, have sharply accelerated over recent years. In their 2021 paper on AI in Business and Finance, the OECD estimated that global spend on AI within the financial services industry will reach USD 110bn by 2024[1] .

For financial markets, AI offers opportunities in multiple areas from Front to Back Office. Areas such as trading, decision making, process re-engineering and data analysis have all received investment in the quest for better outcomes and greater efficiencies.

This expanding adoption of AI and its deployment in wholesale markets presents compliance officers with new challenges and opportunities, neatly summarised in two main areas: firstly, they need to understand how AI is being deployed – particularly in the Front Office - in order to provide effective advice and challenge to the business on implementation and secondly, how to adopt AI to generate efficiencies within the Compliance function itself.

To support firms in meeting these challenges, this paper sets out how firms' adoption of AI, within both the first and second lines, is impacting the Compliance function and how Compliance itself can adopt AI. It considers the benefits, risks and regulatory challenges, then concludes with a series of recommendations which Compliance teams can consider as they develop and evolve their respective approaches to realising the potential of AI.

AFME would like to thank PwC for their efforts in compiling this report, as well as members from AFME's Compliance Committee and all of those who made contributions that were integral to the development of this publication. We are also grateful for the input of several key regulators and supervisors who agreed to be interviewed for this report.

James Kemp
Managing Director
GFMA & AFME

> **"The expanding adoption of AI and its deployment in wholesale markets presents compliance officers with new challenges and opportunities"**

[1] https://www.oecd-ilibrary.org/sites/39b6299a-en/index.html?itemId=/content/component/39b6299a-en

Executive Summary

This paper considers the impact of AI on the Compliance function and aims to provide a view of industry sentiments on the rapidly evolving technological and regulatory environments in relation to AI. Ultimately, it seeks to address two key areas:

1. How a firm's use of AI affects the Compliance function and how the Compliance function provides the associated oversight and challenge; and

2. What opportunities exist for the Compliance function to adopt AI to improve its own functions and keep pace with deployment in the business.

The majority of firms are exploring possibilities for the deployment of AI, with mature firms now actively deploying new technologies with consideration of the impact on their risk frameworks and governance. The interviews and survey results provided a view of the current state of the industry and identified future areas of focus. In summary:

- **Progress in the deployment of AI is more advanced in the 1st Line of Defence (1LoD)**, with a range of use cases including monitoring, trading decisions and strategy recommendations, surveillance, chatbots and fraud.

- **While AI might not create completely new risks for organisations, there was recognition that it may amplify existing risks.** These risks were related to ethical and performance concerns, such as explainability and data privacy. Transparency around the outcomes of AI systems is critical, and some firms reported simplifying their AI in order to meet internal and regulatory requirements. Considerations of data privacy and data leakage, particularly when using third party vendors, has limited some firms' level of comfort in deploying AI.

- **Management of AI risks is through existing governance and risk frameworks,** with only few firms reporting having specific frameworks, processes and governance in place for AI. Similarly, the split of responsibilities for oversight between 2nd Line of Defence (2LoD) functions, and the interaction model between these functions, follows existing mandates and allocation of risk stripes.

- **There is appetite within Compliance functions to realise the potential of AI**, and firms do not want to fall behind the curve in terms of evolving industry practice. Use cases for the deployment of AI in compliance to date have been seen mainly in activities related to horizon scanning, Anti-Money Laundering (AML)/Know Your Customer (KYC) and monitoring, with benefits focused on improved operational efficiency and additional capacity to focus on value-add activities.

- **The mandate of the Compliance function will not fundamentally change with advances in AI, as compliance will still require "human-led" subjective assessment.** However, the composition of the compliance officer's role and the associated skill set is expected to change over time. There is an expectation that Compliance employees will need greater digital literacy in order to effectively execute their mandate, with advanced firms already upskilling staff in their understanding of technology.

- **AI presents an opportunity to deliver a holistic and "dynamic" approach to compliance,** with "real time" monitoring, advanced data analytics and the use of preventative, rather than detective, controls driving the embedding of an enhanced compliance culture. Firms see the overcoming of silos and strong collaboration across the organisation, with the Compliance function as a central player, as key to achieving this.

- **Regulation is at an early stage and, in the main, firms are using existing expectations to guide their use of AI.** Public policy for AI can signal the direction of travel for future regulation (such as the risk-based approach of the EU AI Act) and so firms can start preparing by understanding key characteristics and putting in place proportionate governance. There is a preference for a principles-based framework that provides guidance but also encourages innovation.

- **There are clear steps that Compliance functions can take to enhance their AI capabilities.** Focusing on robust governance, analysis of risk exposure and an end-to-end approach to compliance will support the increased adoption of AI across the business in a secure and sustainable way. It will also give firms a better sense of any gaps in compliance skillsets, metrics and monitoring.

Approach

The content of this paper is based on a survey completed by 17 AFME member firms, supplemented by qualitative interviews with eight AFME members in order to explore their survey responses in more detail. Four European and UK regulatory and supervisory bodies also provided input on their expectations and the future regulatory landscape.

Survey and interview respondents comprised a range of firm types in size and scale. The majority of respondents (15) had a global geographical reach, while the remaining two respondents had European & UK businesses.

Input on survey responses was sought from relevant functions including Compliance, Technology, Financial Crime, Operational Risk, Data & AI, Legal and the Front Office.

Definition of AI

There is no universal definition of AI, and firms will have articulated their own internal definitions to aid in the assessment of regulatory obligations and the implementation of AI. For the purposes of this paper, we consider AI to be defined as the ability of machines to imitate human intelligence processes, which comprises a number of different capabilities. This includes, but is not limited to:

- Machine learning (a subset of AI that enables machines to learn from existing data and improve upon that data to make decisions or predictions);

- Deep learning (a machine learning technique in which layers of neural networks are used to process data and make decisions); and,

- Generative AI ("GenAI") (the ability to create new written, visual and auditory content given prompts or existing data).

> **"We consider AI to be defined as the ability of machines to imitate human intelligence processes, which comprises a number of different capabilities"**

AI in the Business

The majority of the Compliance function's focus on AI is driven by its increased adoption within the wider business and the requirement to provide 2LoD oversight of the associated risks. A significant majority of survey respondents (77%) indicated that they had seen AI adoption in the 1LoD, with all of those respondents noting adoption in the Front Office in particular. AI has been implemented on a widespread basis across a range of mature use cases, including:

- product trading algorithms;
- trade strategy recommendations, thematic analysis and intelligence;
- business decisioning;
- client engagement and service (such as chatbots);
- transcription and translation;
- trade surveillance and suspicious activity monitoring;
- behavioural analytics (such as recording trades and sales to identify trends and raise alerts);
- cybersecurity (such as identifying suspicious indicators of compromise)
- payments (such as cash flow intelligence and payment repairs); and,
- fraud (such as face recognition for clients).

Business use of AI seeks to improve efficiency through the automation of key business processes, and to support employees in making more intelligent decisions through advanced data analysis capabilities. Survey and interview findings identify a range of adoption levels across the industry. While the vast majority have implemented AI for standard use cases such as algorithmic trading and transaction monitoring, others are deploying more sophisticated use cases such as behavioural analytics. There is not a guaranteed correlation between size of organisation and level of adoption: while larger-scale, global firms tend to be more advanced in their deployment of AI, so to are a number of middle market firms with some bulge bracket firms in very early stages of adoption in the 1LoD.

Respondents agreed that AI should be used where it is the best and most appropriate solution to meet a business need, rather than looking to use AI across all processes. One firm articulated this as "starting with the issue, rather than the technology".

> **"Business use of AI seeks to improve efficiency through the automation of key business processes, and to support employees in making more intelligent decisions"**

Considerations for the Compliance Function

Implementing AI within the business brings benefits, but also has the potential to amplify existing risks that the Compliance function needs to support the business in managing. The table below outlines some of the benefits and risks for the applications mentioned by members in our survey, which are then discussed in further detail.

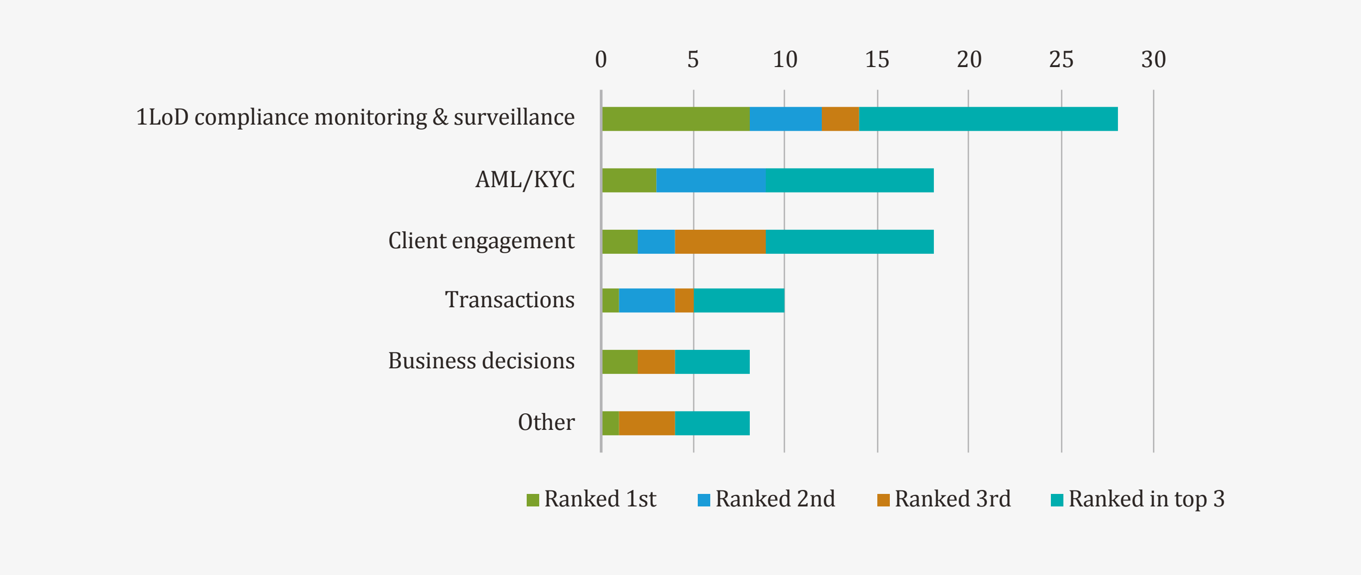
Areas	Types of AI Applications	Potential Compliance Benefits	Examples of Incremental Compliance Risks
Transactions	• Product trading algorithms • Trade strategy recommendations, thematic analysis and intelligence	• Faster and more accurate generation and analysis of trading data • Better outcomes for clients	• More complex accountability for trading decisions • Limits on explainability of model outputs • Potential for 'herding' behaviours with widespread adoption of similar products
Business decisions	• Business decisioning	• Faster and more accurate generation and analysis of business data • In depth data insights to support improved decision making	• Limits on explainability of model outputs • More complex accountability for business decisions
Client engagement	• Client engagement and service (such as chatbots)	• More efficient client communication • Faster and more accurate analysis of client communications to identify trends and issues	• Dilution of accountability for client engagement • Limits on explainability for client responses • Impact on client experience
1LoD compliance monitoring & surveillance	• Transcription and translation • Trade surveillance and suspicious activity monitoring • Behavioural analytics (such as recording trades and sales to identify trends and raise alerts) • Cybersecurity (such as identifying suspicious indicators of compromise)	• Faster analysis and alert generation, even real-time • Increased capacity for communications surveillance • Combination of different/new and more disparate data sets • Increased accuracy / reduction of false positives	• Use of larger and more complex data sets may increase risks such as data quality, data privacy, bias etc. • Limits on explainability of model outputs
AML/KYC	• Fraud (such as face recognition for clients)	• Improved security • More efficient screening processes for clients • Improved client experience • Greater security from and faster resolution of cyber attacks	• Limits on explainability of model outputs • Breach of data privacy / client confidentiality
Operations	• Payments (such as cash flow intelligence and payment repairs)	• Reduced potential for manual errors • More in depth analysis using greater range of data • More intelligent forward looking operations management	• Limits on explainability of model outputs • Dilution of accountability for operations

AI within the Business as a Driver of Efficient and Effective Compliance

While efficiency and cost benefits are often the focus of AI implementation opportunities, AI also provides an opportunity to enhance compliance outcomes in the business. This can drive an improved compliance culture through "real-time" monitoring, the ability to access and analyse greater sets of data, and the use of preventative, rather than detective, controls. The ability to analyse a wider dataset through AI and machine learning means that firms can gather deeper and more useful insights that support informed and timely decision making and improved compliance risk management. AI also allows for quality assurance (QA) checks to be embedded at all stages of business processes ("QA at source"), with advanced use of predictive analytics to enable early detection of potential breaches.

Compliance monitoring and surveillance in the 1LoD (such as trade surveillance, communications surveillance and behavioural analytics) was seen by survey respondents as the greatest opportunity for the implementation of AI (47% ranked it as their top opportunity, while 87% ranked it in their top 3). One advanced firm referenced the use of digital reasoning tools to record trades and sales, enabling quicker and more accurate identification of trends and raising of alerts. The outputs are used by the business risk and control teams, who escalate any issues as appropriate to surveillance governance committees.

Figure 1: **What are the top 3 1LoD compliance processes/areas in your firm that would present the greatest opportunity for AI implementation?**



Key Risks for the Compliance Function to Consider

When identifying risks associated with business use of AI, respondents identified two key areas concerning the Compliance Function: explainability and model transparency; and data privacy and confidentiality. Other emerging conduct-related risks related to the use of AI identified included the dilution of human accountability and responsibility, creating an over-dependence on the results generated by these technologies, as well as biases in models that may incorporate and exacerbate existing prejudices. The Compliance function has a key role to play in supporting the business to understand these risks and provide advice on appropriate outcomes.

Explainability and transparency

41% of survey respondents identified "explainability", or lack of transparency, as their top risk in relation to the implementation of AI. Explainability and transparency can be blurred, though they have separate definitions: explainability focuses on why an AI system has reached a specific output and is therefore related to the operation of the model and the data that is used to train it, while transparency involves being open about data handling, model limitations, potential biases and the context of its uses to ensure that all stakeholders clearly understand the workings of the AI system. Having transparency in your processes and systems will tend to accompany explainability. From a risk perspective, explainability risk relates to the lack of understanding in how a model or system generates results: a lack of explainability can result in issues such as model bias, low accuracy, or inappropriate model use. There is an increased focus from governments and regulators around transparency, particularly in algorithmic models, and an awareness of the need to build robust internal frameworks, governance and controls.

Interviewees identified instances where model outputs had been wrong and they did not have the ability to understand why, particularly when it came to testing new technologies such as GenAI. Limitations had therefore been put in place around the use of such technologies. Other firms reported needing to "dial back" the complexity and sophistication of some algorithms to meet internal explainability requirements.

Data privacy and confidentiality

Challenges around data privacy were also identified in the survey and interviews as a key risk for Compliance functions. Interviewees noted that the most sophisticated AI solutions often require the use of sensitive client information and there was not yet a clear understanding of what data could be shared, where it could be stored and whether it needed to be masked. A number of firms reported only using publicly available data in their AI use cases or only using internal servers until issues related to data privacy are better understood and could be managed appropriately. This has also been a challenge for AI vendors in working with firms that are nervous about storing data on the cloud or external servers. Industry leaders are exploring the use of synthetic data to mitigate data privacy issues, especially at the proof of concept stage. In the UK for example, the Financial Conduct Authority (FCA) is working with the industry to drive and manage the adoption of synthetic data ("artificial" data that is generated by a model or algorithm to (among other uses) train AI models, protect sensitive data, and mitigate bias).[2]

Bias and discrimination

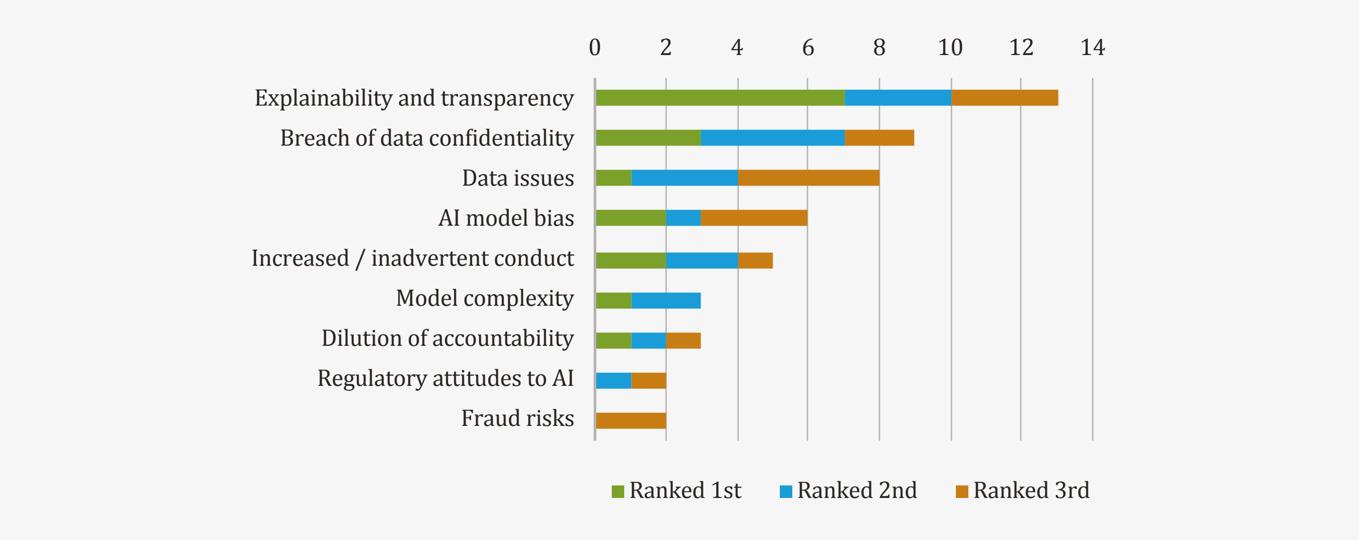
Bias is often cited together with explainability as a concern, as an inability to understand how a system or model comes to a decision or output can hinder responsible AI adoption and use. A lack of transparency and clear communication can create risks by providing misleading outputs and can compromise a firm's reputational risk. AI poses significant conduct risks, particularly where it is used in high-risk decisions that impact clients and customers and where unjust bias could lead to discrimination or unintended outcomes. The risks are not limited to the retail market, where using AI for decisioning use cases that impact customers (such as credit decisions) may breach requirements under legislation such as the EU Equal Treatment Directives or the UK 2010 Equality Act of 2010. In wholesale markets, trading activity could result in poor conduct outcomes if an algorithm owned by the business is inadvertently manipulating the market.

[2] https://www.fca.org.uk/publications/research-articles/exploring-synthetic-data-validation-privacy-utility-fidelity

Accountability considerations

Managing the deployment of AI in line with changing regulatory environments and internal requirements, as well as effectively mitigating the associated risks, requires robust governance and accountability. Interviewees noted the need to implement clear accountability mechanisms and define accountable parties for AI use, development and oversight. It is key to embed a "human-led" element into processes where individuals are still responsible for the actions taken based on AI algorithms and models, particularly given the challenges in transparency of AI models outlined above.

Figure 2: **What are the top 3 risks concerning the Compliance function in relation to your business adopting AI?**



Market Integrity Risks

Regulators and other bodies are starting to consider more systemic risks associated with the greater use of AI. Market integrity is increasingly an area of focus; for example, a potential convergence or "herding" of AI algorithmic trading strategies (where firms across the industry are using the same embedded models) has led to concerns about increasing intraday volatility and a potential lack of liquidity in the market. Data issues may also lead to systemic risks at the market level, with the potential for market instability risk if data disruptions occur.

There are also fundamental societal issues related to AI that may affect the financial services industry. GenAI could have a considerable impact as a result of the creation and dissemination of misinformation; for example, a deep fake image of an explosion at the Pentagon in May 2023 disrupted global financial markets[3]. Even if these risks cannot be mitigated by firms on an individual level, they will play an important role in working with industry bodies to define and manage them to protect the integrity and operation of the markets.

[3] https://www.bloomberg.com/news/articles/2023-05-22/fake-ai-photo-of-pentagon-blast-goes-viral-trips-stocks-briefly?leadSource=uverify%20wall

AI Governance and Oversight

The majority of firms surveyed (65%) do not currently have discrete frameworks and policies in place for AI, although 82% of those firms had plans to change this in the future. It was noted however that any plans for the creation of AI frameworks and policies are dependent on the clarification of regulatory expectations and would be adapted as required. Currently, risks related to AI are mainly managed through existing governance, frameworks and processes, depending on the type of technology being implemented and the purpose for which it is being used. For example, models are managed under model risk management frameworks, while technology that concerns the hosting of information on cloud systems is required to go through existing cyber security processes and approvals. It was noted that much of the risk is now concentrated in the development phase, rather than in the use, and therefore the configuration of the AI is critical to mitigating associated risks.

One firm, where AI adoption in the Compliance function was relatively mature, reported that they have developed a separate Compliance AI framework owned by the Compliance function. The framework consolidates regulatory requirements related to AI (including governance, explainability, model management and third party considerations) and allocates these requirements to other functions as appropriate, such as Risk, Information Technology (IT) and Human Resources (HR).

From our survey and interviews, model risk was the most common framework under which AI risk is currently managed, including requirements related to model development, testing and classification. Industry leaders are increasingly stressing the importance of adapting their technical model validation and monitoring functions to the new challenges posed by AI (such as the scope and scale of models), including refining their processes and technology to ensure that modelling approaches are sufficiently standardised across the organisation and shifting model testing and controls as much as possible to the 1LoD. One regulator noted firms' concerns that the requirements for model risk management were too onerous, particularly for internal models, and agreed that a lighter-touch approach could be used for model governance, provided it was performed in an appropriate, risk-based manner and satisfied current regulations. Whether or not AI model risk is managed as part of existing structures, leading firms are incorporating explicit provisions for these risks in their processes. In relation to model bias for example, organisations have adopted enterprise-wide definitions of bias, created taxonomies to identify the most suitable metrics to measure bias depending on the use case domain, and/or incorporated explicit tests to identify data and model bias throughout the model lifecycle.

Firms indicated in interviews that they are awaiting further clarity from internal stakeholders and/or other external regulatory and market developments before deciding on whether to develop discrete AI frameworks and policies. Regulatory sentiment is broadly in favour of this approach outlined above and are of the view that, where existing frameworks, processes and controls are mature in their embedding, these should be largely sufficient to incorporate additional requirements around AI. It is critical to understand and define how the AI will be used, and therefore how it can be appropriately managed within the existing risk taxonomy.

While 24% of survey respondents reported having a Committee with a specific responsibility for the management of compliance risk in relation to AI, 59% did not have a Committee with this responsibility. The remaining 17% reported having a Committee who oversaw AI as part of a wider mandate around technology. Broad industry consensus suggests that AI governance is managed through existing Committee and Board structures, depending on the technology and the corresponding review and approval processes and requirements. One mature firm reported having a specific AI Committee with responsibility for setting the guardrails and control requirements for the firm's identification and deployment of AI, while another has a Committee with responsibility for recommendations on the ethics of the use of AI, with representatives from the Board, Legal and Compliance.

The Role of the Compliance Function

Responsibility for the oversight and governance of AI risk is dependent on the firm's operating model in relation to the allocation of risk stripe oversight between 2LoD teams. Survey respondents showed a mix of responsibility for oversight of AI across Compliance, Operational Risk, Enterprise Risk, Technology/IT Risk and other functions. The role of the Compliance function and the split of responsibilities between the Compliance and Risk functions therefore tend to follow existing mandates and responsibilities.

Figure 3: **Does the Compliance function have responsibility for the oversight of AI compliance risks?**

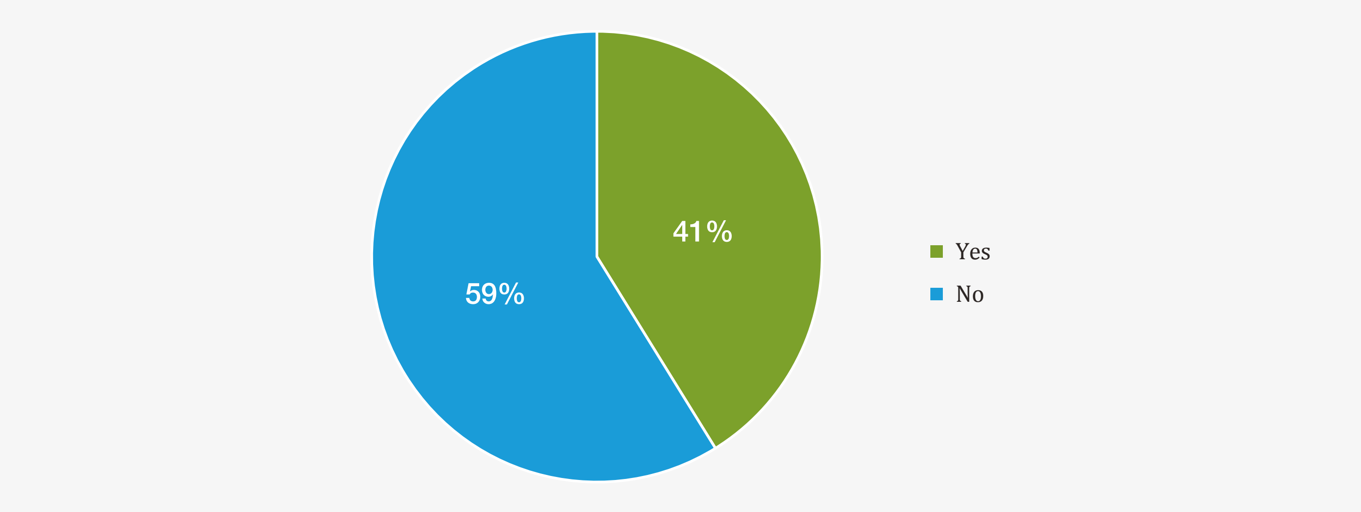
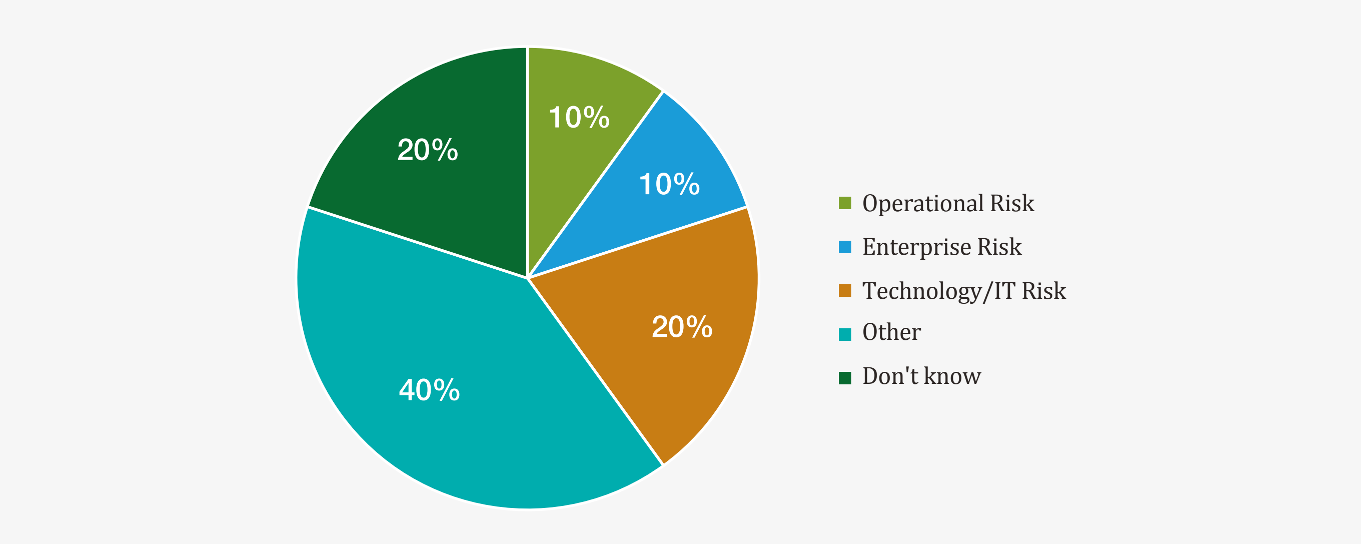


Figure 4: **Where the Compliance function does not have responsibility for the oversight of AI compliance risks, which team does?**



The Compliance function needs to consider how it executes its 2LoD role in relation to AI. Recognising that AI is being used enterprise-wide across many risk areas and business units, the Compliance function should have line of sight of where AI is being used (particularly where the use relates to regulated activity such as client advice, production of client materials, client data and surveillance) in order to challenge the outcome of the activity and make sure that regulatory requirements are being built into AI tools. Where the function is responsible for the oversight of particular risk stripes (such as conduct or compliance risk), it needs to understand how AI impacts the risk profile and incorporate updated requirements into relevant frameworks, policies and standards.

AI risk also needs to be incorporated into compliance risk assessment programmes and other standard monitoring activities, with the Compliance function providing informed oversight and challenge to the business. The firm's use of AI in relation to the particular risk theme should be considered as part of the risk assessment and control effectiveness scoring. The nature of AI and machine learning, whereby models are driven by data which may be continuously subject to change, requires ongoing monitoring of AI model compliance to regulation as well as to internal policies and business objectives. This could put existing compliance processes under stress and may need to be reviewed against increased internal and regulatory requirements.

Given that existing regulations are not generally designed with AI in mind and the regulatory approach in most cases is principles-based, regulators expect firms (and Compliance functions in particular) to anticipate and interpret regulatory requirements on outcomes. This requires a significant degree of informed judgement from Compliance functions in providing guidance and challenge to their organisations on how they have defined and met outcomes in relation to AI. Where Compliance functions have a more legal based mandate as opposed to advisory, this may create further challenges with more outcomes-based regulations and require consideration of where the responsibility, and associated skill set, for regulatory interpretation sits. Where a principles-based approach does not translate neatly into internal compliance rules, having a holistic approach to AI governance, with a clear internal accountability structure, will allow for guidance and principles to be actioned effectively.

> **"AI risk needs to be incorporated into compliance risk assessment programmes and other standard monitoring activities"**

AI in the Compliance Function

Current State

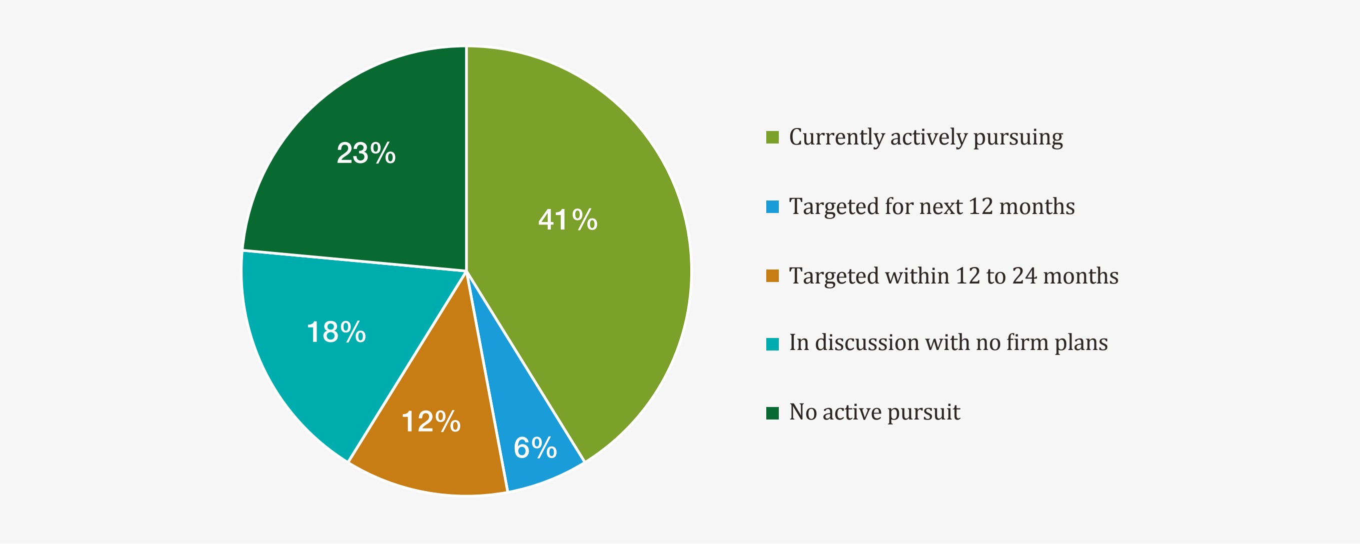
The advancement of AI capabilities also presents an opportunity for Compliance functions to use technology to execute their 2LoD role more efficiently and effectively, through automating key processes and gathering deeper and more useful insights that support informed and timely decision making in compliance risk management.

Compared to the 1LoD, the Compliance function is less mature in the identification and implementation of AI related opportunities, with 59% of firms reporting AI adoption efforts in the 2LoD compared to 77% in the 1LoD. As with the 1LoD, there is a spectrum of maturity within the industry, with more advanced firms starting to pilot use cases while others are still either at early stages of implementation or are not currently looking to implement AI. There are a minority of notable exceptions, however, where Compliance functions are playing a pioneering role within their firms in deploying AI. These functions have set up their own teams with a mandate to identify and implement innovative use cases in areas such as horizon scanning, monitoring and cross-border requirements.

Future Plans

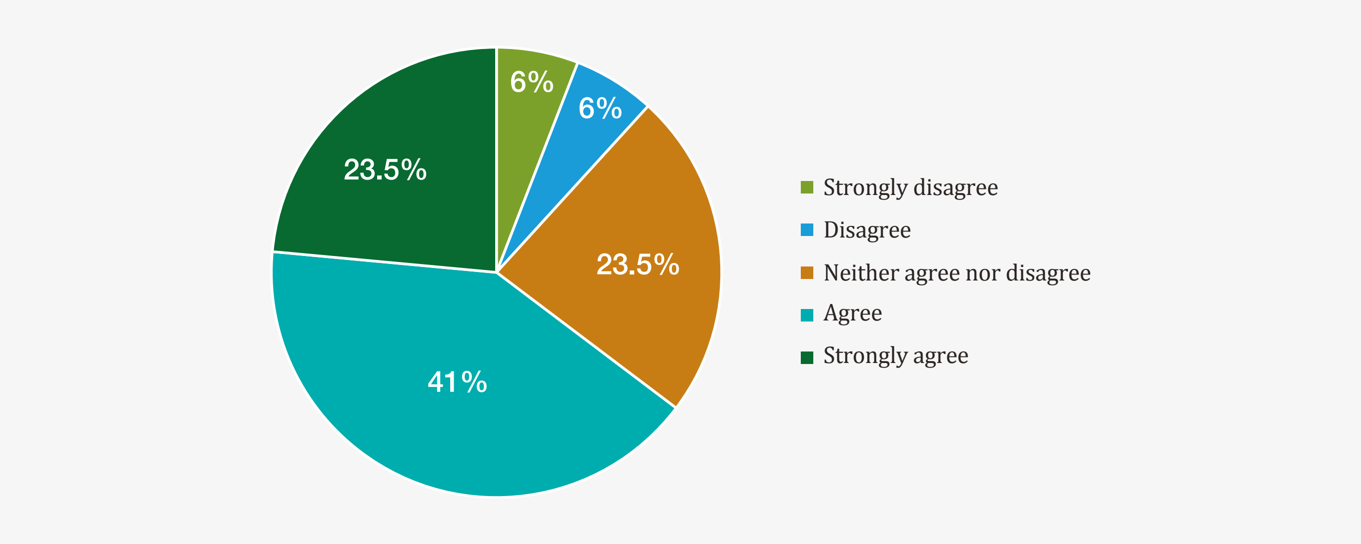
41% of survey respondents indicated that they are actively pursuing the use of AI for compliance processes, with a further 18% targeting pursuit within the next 24 months; this demonstrates the increasing focus on AI with firms actively trialling the use of these technologies. The purpose of the majority of these use cases is to improve the efficiency of manual activities within the function (such as horizon scanning and AML/KYC). However, a significant number of respondents (24%) indicated that they had no active pursuit underway at this present time.

Figure 5: **Is your firm actively pursuing the use of AI for compliance processes?**



Survey results showed a mixed appetite from the Compliance function in implementing AI into compliance processes in the future. While a majority agreed that there was interest (with 24% strongly agreeing with the statement), 24% of respondents appeared to be unsure about the potential for implementation of AI into compliance processes (neither agreed nor disagreed).

Figure 6: **To what extent do you agree or disagree with the following statement: There is interest from the Compliance function in implementing AI into compliance processes?**



Use cases currently tend to be point solutions that address a specific activity or need within the function, but AI represents exciting possibilities for Compliance functions to be transformative in their approach to compliance management. There is an opportunity to be significantly more ambitious in the deployment of AI, creating end-to-end, enterprise-wide solutions that utilise sophisticated AI capabilities to monitor in real time and identify advanced correlations to provide greater insight and efficiencies.

Key Compliance Use Cases

Within the range of implementation maturity, there was a spread of active use cases across activities including compliance monitoring, horizon scanning and AML/KYC, where AI implementation was reported to be either planned or in flight. There were also some more advanced use cases reported to be of interest, such as the use of GenAI in policy management.

Horizon scanning

Horizon scanning (using AI to scan for new or amended regulations and to create a comprehensive obligations registry) is one of the most common use cases for AI implementation, particularly as for many firms this has traditionally been a time-intensive and manual task. Multiple vendors offer the ability to scan for new or updated regulations using Natural Language Processing (NLP), scraping regulatory text to create a detailed inventory and provide an initial view of applicability, all based on the firm's footprint and product offering. This has particular benefits for firms that are part of a global group, subject to local regulatory requirements across multiple jurisdictions, and for whom horizon scanning is therefore a more complex task; however, this does also create greater challenges and more room for error in the technology. There is also the potential for more advanced use of AI in supporting regulatory obligations management; for example, using GenAI to draft obligations based on the firm's regulatory inventory, with a review by Legal and/or Compliance teams to validate the output. This is easier with prescriptive regulation that AI can identify and turn into specific obligations, and more potentially more difficult where regulation is outcomes-based.

Chatbots for engagement with the business

Business areas have implemented chatbots, particularly in the retail space, to engage externally with customers, but there is also the opportunity within wholesale businesses to implement internal chatbots for employee compliance queries, with answers based on the ingestion of obligations, policies and procedures. These chatbots could save the Compliance function time and effort on frequently asked questions (for example, on gifts and entertainment or personal trading requirements). Leading firms are looking at more advanced chatbots that are able to provide compliance advice to the business through machine learning; this requires more sophisticated technology and validation by the Compliance function.

Sanctions, AML and fraud

Where financial crime oversight (including AML, KYC and fraud) sits within the remit of the Compliance function, AI can automate repetitive tasks that rely on the gathering of significant volumes of data. For example, AI can provide rapid client ID verification through multiple sources of data. It can also speed up client sanctions screening and immediately identify breaches. Fraud is another common use case, with technology providing real time fraud alerts and enabling the Compliance function to perform real time monitoring.

Surveillance

To the extent that surveillance sits within the remit of the Compliance function, AI is used to effectively monitor both voice and e-communications to quickly detect any issues. AI can also provide automatic transcriptions of conversations, which enables quick screening and scanning of employee discussions to identify compliance and conduct breaches.

Policy management

Dynamic policy management utilising AI includes the use of technologies such as GenAI to write policies, based on inputs such as regulatory obligations, with proofreading and validation by experts in the Compliance function. One example of an advanced use case discussed was the use of AI to review existing policies for gaps on an ongoing basis, based on the dynamic ingestion of other risk, regulatory and business information.

Report and MI generation

Advanced data analytics tools can generate and analyse MI (management information) quickly, more accurately and with greater depth to support business leaders understand their compliance risk profiles and take informed decisions. AI can also auto-generate reports, freeing up time for the Compliance function to validate outputs and focus on value-add insight and commentary.

Benefits of AI Adoption within Compliance

Improved data capabilities were ranked by survey respondents as the greatest anticipated benefit for the Compliance function of implementing AI (59% ranked it in their top 3). Having faster and more accurate data will allow compliance monitoring and assessments to become more "real time", and will drive enhanced insights and transparency, improving compliance outcomes. Other benefits of AI cited by survey respondents focused on operational efficiency, productivity and cost efficiency benefits: critical given the industry wide pressure on organisational costs. There was consensus from our interviews that AI will make the execution of its responsibilities more effective and efficient through the automation of data-heavy, repetitive, manual tasks. Horizon scanning, automatic alerts and transcription of voice and e-communications were given as examples of use cases where this is already occurring. AI is also expected to improve the coverage of the Compliance function; instead of testing a sample of business activities, the function will be able to test a risk-based sample of AI outputs that have 100% coverage.

Mature firms are already seeing the impact of implementing technology, particularly in areas such as surveillance: multiple firms reported that AI had reduced the number of false positives, while one reported that improved accuracy in the system had reduced the overall number alerts by 60% and freed up capacity. However, the realisation of benefits was not universal. For example, issues such as high volumes of false positives in automated surveillance or significant errors in transcriptions had in fact increased the manual effort required in some firms, given the need for intervention.

One firm where AI adoption in the Compliance function is relatively mature reported that the use of AI had improved their relationship with the business. Where previously the Compliance function had been a limiting factor in business expansion, due to a lack of monitoring capacity, automating compliance activities had provided that additional capacity. The use of chatbots that could answer business queries on governance documents (compared to previously where the business would need to read and understand detailed and often voluminous documents) was also seen as responding proactively to the business' needs and the Compliance function was increasingly seen as a strategic partner.

While AI adoption in the Compliance function can enhance compliance risk management outcomes, currently the majority of firms have not yet formally measured the impact of AI from a compliance perspective. 60% of firms who have adopted AI reported that they have not yet seen any impact on compliance outcomes from their deployment of AI (although 33% indicated that it had had positive outcomes). From interviews, the assessment of the impact of AI remains focused on business outcomes (such as improvements in client management and client experience) and it appears that any impact from a compliance perspective is limited largely to surveillance technologies. This represents an area for future focus, as AI is deployed more widely into compliance processes.

Barriers to AI Adoption within Compliance

Implementation of AI is complex, and survey respondents indicated a number of barriers to adopting AI within the Compliance function. The majority of respondents cited concerns about data governance and complying with data privacy regulations, as well as the quality of the data being ingested. Across the firm, the effectiveness of AI deployment within the Compliance function is reliant on the ability to access accurate and timely data and on the existence of robust data governance and assurance. Other barriers cited by survey respondents were explainability and issues related to outdated legacy systems.

Interviews provided further examples of challenges faced by Compliance functions in adopting AI. One was the accuracy of the outputs from AI, including those from vendor solutions. Firms were concerned, for example, in the accuracy of horizon scanning results, with scenarios provided where outputs of searches using machine learning or NLP had either led to gaps or yielded significant volumes of irrelevant results. The lack of confidence in the outputs led to more intervention and therefore more effort from compliance officers.

Interviewees also cited the lack of appetite or enthusiasm for change within the Compliance function (and in some cases the organisation more broadly), where the lack of support for deployment impacted the pace of change. Firms did expect that this would change over time as the technology became better understood and there was greater industry consensus on use cases and vendors.

Impact on the Role of the Compliance Function

Our research shows that, despite advances in automation, firms still expect that compliance will be "human-led", requiring subjective assessment and critical thinking. Indeed, the vast majority of survey respondents (88%) believe that AI will have a limited or moderate impact on the role of the Compliance function, although no respondents said that AI would have no impact. Responses indicated a gradual evolution in the changes to the Compliance function brought on by AI, with a belief that the overall role of the function would remain broadly unchanged even while processes were enhanced. Interviews with regulators indicated that they agree the core discipline of compliance will follow existing frameworks and responsibilities, and they expect compliance officers to exercise expert judgement when it comes to the interpretation of regulations.

However, while AI will not change the fundamental responsibilities of the function, the automation and enhanced accuracy and coverage of compliance activities with the deployment of AI may change the composition of the compliance officer's role. With time freed up from currently manual tasks, compliance officers will spend more of their time on expert assessment, decision making and advanced analysis. We also expect that there will be a greater emphasis on quality assurance activities, reviewing and challenging the output of AI used by the business. This is where greater digital literacy within the function will be critical.

Changing Skills in the Compliance Function

The skill set within most Compliance functions is still heavily weighted towards traditional compliance and regulatory capabilities and AI has not yet led to a significant shift in the resource or skill mix. Most firms (65%) indicated that they are not recruiting for AI skills within the Compliance function at this point in time. However, firms have recognised that there will be a need for a gradual change in skills where employees in the Compliance function become more AI literate, even if they are not experts, in order to provide informed and robust challenge of models and other types of AI.

Given the improvements in data analytic capabilities that come with the implementation of AI across the firm, the Compliance function will need to invest in data analysis skills to use the increased available data and convert insights into actions. Mature firms reported recruiting for data scientists within the Compliance function: unlike data scientists sitting in technology functions, these individuals are expected to have business and compliance knowledge alongside their data capabilities so that they can engage constructively and robustly with the business and technology (including model owners).

Firms should also consider what skills they need when it comes to deploying AI within the Compliance function itself, such as technology or data analysts to identify and implement new AI opportunities. Survey respondents were not sure whether their Compliance function currently has the right skills to harness the opportunities for AI (41% neither agreed nor disagreed with this question). Most firms locate responsibility for developing AI in a central technology or innovation team, but there is an option for the Compliance function to set up their own innovation teams to capitalise on the specific possibilities of compliance technology for the function itself. One organisation reported having a dedicated AI team within the Compliance function that own the requirements related to AI and have responsibility for identifying and implementing use cases.

Of course, AI opportunities are most effective when developed in collaboration across the firm under an effective AI governance umbrella that enables different teams to work together; this is where central innovation teams can play a role in identifying end-to-end systems that create a coherent compliance risk management approach across the firm. In more mature firms, there are dedicated innovation teams and ideas on opportunities are sought from all employees, with chosen proofs of concepts going into production in sandbox environments.

Leading firms are increasingly focusing on uplifting digital literacy across the firm and expect their people to remain up-to-date with technological innovations and developments. In a number of cases, this has involved transferring individuals from the 1LoD into the Compliance function to enable the sharing of skills and ensure that individuals in the function have business as well as technical knowledge. This is driven by a tone from the top, where management encourages innovation, embeds necessary changes into the firm's operating model and organisational structure, and creates time and space for employees to prioritise their ongoing learning and development.

Talent Management

The long-term impact of AI on talent management and succession planning has not been fully understood, a challenge that is not limited to financial services. The skills and expertise for compliance oversight, particularly for junior members of staff, have traditionally been developed through the execution of critical compliance activities, and greater automation of these activities may mean that employees have limited opportunity to develop these skills early in their career. However, it is true that employees increasingly enter the workforce with a higher level of technology literacy, which will support functions in future-proofing their teams. Given the changing world in which Compliance functions need to operate, it is critical to understand the skill sets that will be required in the future, including as the composition of the compliance officer's role changes, and how staff gain these skills through on-the-job learning and training.

Compliance Culture

AI has the potential to drive an improved compliance culture across the organisation through enabling enterprise-wide dynamic monitoring that allows for "real-time" identification of issues or breaches. From our interviews, the improvement in compliance culture is not something that has been assessed given that AI implementation is still at an early stage: interviewees noted that it was difficult to be sure if changes already implemented had "moved the dial" on improving the compliance culture and that this was not the primary performance indicator driving their AI adoption. Using existing metrics for measuring risk culture or defining new ones could help an organisation understand the impact of AI on compliance activities and compliance outcomes and inform further investment.

Conversely, as discussed previously in this report, AI may pose challenges to a culture of accountability if employees become reliant on answers generated by AI. Embedding an accountability framework, using frameworks such as the UK Senior Managers & Certification Regime (SM&CR)[4] and Irish Senior Executive Accountability Regime (SEAR)[5], that ensures human assessment and decisions remain part of the process are critical. This will require senior executives to have sufficient understanding on where and how AI is contributing to, and impacting on, critical business decisions and being able to challenge their output.

From interviews and survey results, there is clearly an appetite for AI change even while firms are generally at early stages with their implementation. It was noted that people may be more comfortable with "classical" AI that has been around for longer, but more wary of newer technologies such as GenAI where the risks and potential have not been fully understood.

[4] https://www.fca.org.uk/firms/senior-managers-certification-regime

[5] https://www.centralbank.ie/regulation/how-we-regulate/individual-accountability-framework

Regulatory Considerations

While regulation of AI in financial services remains at an early stage, there is considerable governmental and regulatory interest in ensuring the appropriate and responsible use of AI technology.

In the past, regulators have adopted a “technology-neutral” approach, incorporating requirements around AI into existing regulatory and legal frameworks such as data privacy and protection, conduct of business requirements and regulations covering specific business activities (such as algorithmic trading). This includes EU regulations such as the General Data Protection Regulation[6] (GDPR) and Markets in Financial Instruments Directive[7] (MiFID) II, while principles advocated by regulators around client communications (such as those articulated in the FCA Handbook in the UK) are also applicable to AI. For example, Article 22 of the EU and UK GDPR laws restricts firms from making solely automated decisions that have a serious impact on the individual (such as credit applications). There are also more general requirements, beyond those specifically related to financial services, that may apply to the deployment of AI.

Accountability has been highlighted as a significant aspect of future regulatory debate, given the complexity of AI and its capacities for autonomous decision-making pose potential challenges to genuine accountability. Regulators emphasise the need for appropriate controls, governance, skills and understanding (including at the senior level); generally they expect this to be embedded into, and managed through, existing accountability frameworks rather than to introduce new rules entirely. Global accountability regimes have been in place for a number of years, including the SM&CR in the UK from 2016, the Manager-In-Charge[8] (MIC) regime in Hong Kong, the Australian Banking Executive Accountability Regime[9] (BEAR-2018) and the Monetary Authority of Singapore (MAS) 2021 Guidelines on Individual Accountability and Conduct[10] (IAS). More recently in March 2023, the Central Bank of Ireland (CBI) launched a Consultation Paper on regulations and guidance for the implementation of SEAR. While there does not yet exist an EU-wide individual accountability regime for banks more broadly, the EU has drafted an AI Liability Directive to complement the AI Act[11]. The Directive, if put into force, will apply to providers, operators and users of AI systems and sets out the liability framework in the event of faults in the output of an AI system or where the AI system has failed to produce an output.

As the use of AI has become ever more sophisticated and widespread, governments and regulators have started to consider the development of more specific regulatory frameworks and to issue greater levels of guidance, with the aim of providing more clarity to firms and supporting them in managing risks associated with AI. In fundamental terms, regulators in major jurisdictions have converged on a principle-led and risk-based approach, underpinned by a similar definition of AI aligned to that of the Organization for Economic Cooperation and Development[12] (OECD). However, there are emerging differences in the scope of regulation, the granularity of requirements and the level of prescription between jurisdictions which Compliance functions will need to understand, particularly where their firms operate globally. In addition, the implementation of existing regulatory frameworks may impact the development and deployment of AI (such as the impact of different jurisdictional requirements on data privacy and copyright).

[6] https://gdpr-info.eu/

[7] https://www.esma.europa.eu/publications-and-data/interactive-single-rulebook/mifid-ii

[8] https://www.hksi.org/development/activities/1009479-introduction-to-the-manager-in-charge-mic-regime-2022/

[9] https://www.apra.gov.au/banking-executive-accountability-regime

[10] https://www.mas.gov.sg/regulation/guidelines/guidelines-on-individual-accountability-and-conduct

[11] https://commission.europa.eu/business-economy-euro/doing-business-eu/contract-rules/digital-contracts/liability-rules-artificial-intelligence_en

[12] https://oecd.ai/en/ai-principles

The EU AI Act[13], for example, (a horizontal legislation covering all sectors that is expected to formally come into force in mid-2024 with a 24-month transition period, following negotiation between the Commission, the European Parliament and the Council) takes a more prescriptive approach than in other jurisdictions, with the regulatory obligations varying across four broad categories of risk including prescriptive requirements for providers and users of "high risk" listed use cases (including assessing creditworthiness). The EU's approach sets itself apart for a number of reasons, including: (i) a provision on very high-risk use cases and domains, such as social scoring and real-time biometric identification, for which the application of AI is deemed unacceptable; (ii) the development of an AI Liability Directive[14], which provides common rules for a non-contractual, fault-based liability regime for damage caused by AI; and finally, (iii) a set of provisions (still under discussion) which would affect providers of GenAI foundation models which cover areas such as model and data transparency and model design standards. This includes a more prescriptive approach regarding model risk, as the Act lists the types of models that will fall within its high risk category. Supervisory activities related to the Act will be carried out by existing authorities responsible for the supervision and enforcement of financial services legislation with whom firms will already be familiar.

Countries such as the UK and Singapore have adopted a more general principles-based framework, which aims to encourage innovative and technological progress while ensuring that associated risks are fully understood and sufficient risk management and controls are in place. UK financial services regulators have laid out the existing rules and frameworks to mitigate risks related to the deployment of AI (such as the SM&CR and model risk management requirements). For example, in the UK the Bank of England (BoE), the Prudential Regulation Authority (PRA), and the FCA released a discussion paper in October 2022[15] that emphasised aligning AI usage with existing regulatory priorities, specifically consumer protection, competition, data quality, and robust governance.

Model risk management is one area where regulators have broadly emphasised existing requirements for the testing and governance of models, including maintenance of inventories, regular testing, data integrity and review and approval processes. The PRA, for example, published a consultation paper for banks in June 2022 on model risk management, which set out its expectations that the proposals in the paper would also apply to models involving the use of AI technology and that, where there are unique characteristics of AI (such as the greater challenge in transparency and explainability), firms would use risk-based judgement on the adequacy of their approach within the context of their organisation. In their Supervisory Statement on model risk management principles from May 2023, the PRA proposed several principles that build on these expectations, including proportionate implementation and Senior Management Function (SMF) responsibility. In Europe, BaFin has previously adopted a similar principles-based approach in relation to the adoption of AI in certain business processes, publishing in 2021 supervisory principles[16] that laid out general principles for the use of algorithms in decision-making processes (noting the absence of a clear, industry-wide definition of AI at that stage).

The United States is more fragmented in its approach, with cross-sectional principles driven at the federal level (including public policy initiatives like the NIST (National Institute for Standards and Technology) AI Risk Management Framework[17] or the AI Bill of Rights[18]), but with other regulators and state bodies defining their own requirements. Interestingly, the Chinese government recently signalled that it would soften its previously relatively onerous approach to AI, including GenAI; however, it remains to be seen what the specific requirements and future framework will look like.

[13] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206

[14] https://commission.europa.eu/business-economy-euro/doing-business-eu/contract-rules/digital-contracts/liability-rules-artificial-intelligence_en

[15] https://www.bankofengland.co.uk/prudential-regulation/publication/2022/october/artificial-intelligence

[16] https://www.bafin.de/SharedDocs/Downloads/EN/Aufsichtsrecht/dl_Prinzipienpapier_BDAI_en.html

[17] https://www.nist.gov/itl/ai-risk-management-framework/crosswalks-nist-artificial-intelligence-risk-management-framework

[18] https://www.whitehouse.gov/ostp/ai-bill-of-rights/

There has been an increased focus by policymakers in the EU, US and elsewhere on putting in place a consistent and consolidated global framework for governing AI. The "Hiroshima AI Process"[19], which was announced during the G7 Summit in May 2023, stresses the importance of establishing common rules and standards, while leaving room for variation in approaches between countries. A Working Group with representatives from each G7 nation will be formed, in collaboration with the OECD and Global Partnership on AI (GPAI), to consider the development of interoperable standards. In the meantime, individual bodies will continue to define their approaches and await further guidance.

Prescriptive vs. Rules-based Regulation

As described above, there is a spectrum of global regulation with different balances struck by jurisdictions between granular, prescriptive requirements and outcomes-based guidance, with the differing approaches presenting advantages and challenges.

AI is a dynamic and constantly changing area where the context has a significant impact in the design, use and outcome, and therefore most regulators have tended towards a principles-based approach that will capture future regulatory requirements. Detailed rules-based requirements may be quickly rendered out of date with technological developments, could limit innovation and may be disproportionate if applied across too broad a spectrum of AI activities (for example, if requirements are expected to cover common AI tools such as algorithmic trading and advanced GenAI). While most of the risks associated with AI are now well-known and researched, new risks may emerge (such as the market impact of AI-generated fake news); therefore flexibility in regulation, based on an approach of proportionality, may be most appropriate.

However, principles-based guidance will require greater levels of judgement from firms, and from the Compliance function specifically as it advises the business on the appropriateness of its response, and it relies on a maturity in firms being able to define and measure appropriate outcomes.

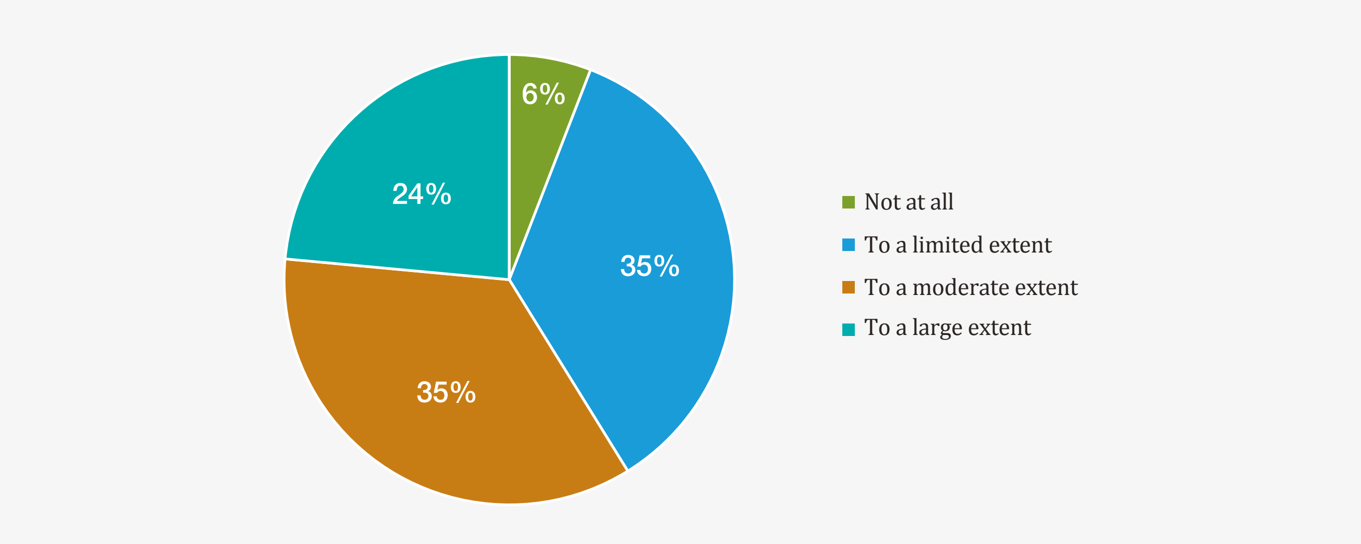
The Industry View

Our survey results and interviews indicated that the regulatory and governmental focus on principles aligns with firms' preferences for future regulatory frameworks, with a general consensus in favour of broader principles- and risk-based approaches that provide scope for innovation within appropriate guardrails. However, it was also recognised that this approach may present some challenges: in a highly regulated environment, mapping the requirements applicable to an evolving technology such as AI can be complex.

This complexity is reflected in the level of confidence firms reported around regulatory expectations. Although a majority of firms indicate a moderate or large degree of familiarity with regulatory sentiments on the use of AI, there is clearly appetite for further dialogue. The onus on firms to exercise judgement is a natural consequence of the technology-neutral and outcomes-based approach of many regulatory bodies; however, it may mean that firms see the incorporation of AI into business processes as more challenging. Some firms reported that they have tended to adopt a hesitant approach towards more sophisticated forms of AI as they are not comfortable that their approach would be compliant, for example, with requirements related to explainability and data privacy. In addition, where differences in regulatory approaches exist, firms can face challenges in consolidating and harmonising all requirements that are applicable to them, particularly where they operate on a global basis. One firm has developed a Compliance AI framework through scanning regulations of all countries where AI was to be deployed (including AI regulations that applied to other sectors) and creating a consolidated list of requirements and recommendations to be owned by different functions (including Compliance, IT and Risk); the volume of requirements demonstrates how challenging it can be to manage.

[19] https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/20/g7-hiroshima-leaders-communique/

Figure 7: **For the jurisdictions in which your firm operates, to what extent are you familiar with regulators' sentiments on use of AI in Compliance?**



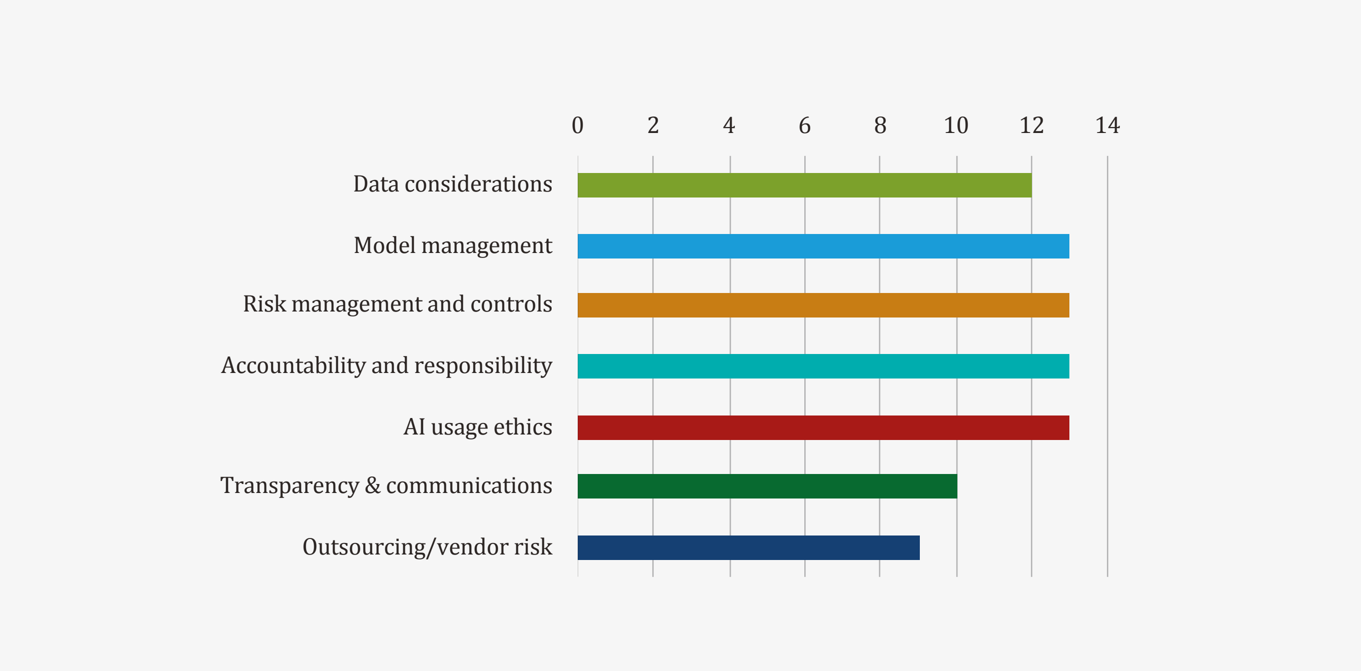
Multiple firms expressed an appetite for continued industry-wide collaboration in order to understand industry practice, benchmark their approaches against peers and align on expectations: for example, through the use of industry forums such as roundtables to understand industry practice and to benchmark their approach to risk management against peers. Firms are also establishing horizon scanning capabilities with a specific focus on AI regulation in order to better prepare for regulatory developments and understand changing sentiments in relation to AI.

Identifying Priorities for Future Regulatory Dialogue

Most firms anticipate further clarity in the future from regulators in the safe deployment of AI (for example through the publication of use cases) and, where respondents reported having had discussions with supervisors around the use of AI, they indicated a supportive attitude for AI usage as long as appropriate risk management frameworks and governance arrangements were in place.

While there is not a desire for comprehensive new regulations on AI, firms identified some specific aspects of AI deployment on which they would like further regulatory guidance. In interviews, firms indicated a desire for further clarity on areas where expectations around AI converge with existing frameworks (for example, data requirements or model risk management requirements).

Figure 8: **Which aspects of AI usage would you like to have more specific regulatory guidance on?**



Regardless of the regulatory approach taken within particular jurisdictions, the regulatory bodies interviewed emphasised the need for firms to take their own informed, risk-based judgement when it came to applying existing regulations, including anticipating regulatory expectations and responding to them appropriately. Therefore, seeking further dialogue with regulators, whereby firms outline their approaches and request feedback, may be more appropriate than formal guidance. Firms need to ensure that relevant employees understand the AI regulatory landscape and how it may differ from the requirements applicable to other aspects of their role. As noted above, this will have an impact on expectations of the Compliance function; as regulatory standards evolve, Compliance functions will play a critical role in supporting their organisations in interpreting, managing and complying with requirements.

> **“Firms need to ensure that relevant employees understand the AI regulatory landscape and how it may differ from the requirements applicable to other aspects of their role”**

Conclusions and Next Steps

The advancements in AI present exciting possibilities to transform the financial services industry, through enhanced use of machine learning and data analytics to drive better business outcomes and improve risk management. However, this progress does not come without risks and the Compliance function plays a critical role in providing informed and robust oversight to the business and in interpreting evolving regulatory expectations. While this may not fundamentally impact the role of the Compliance function, AI risks will need to be incorporated into frameworks, standards and policies and into compliance risk assessments and monitoring and considered across the entirety of the AI lifecycle. The Compliance function will also need to become more AI literate, in order to execute its 2LoD role effectively, and to collaborate with the 1LoD and 3LoD (3rd Line of Defence) to put in place comprehensive AI governance.

While global regulatory approaches have generally taken similar risk-based and principle-based approaches, the EU has gone further than other bodies in defining prescriptive provisions for particular use cases. Compliance functions will need to assess the impact of the emerging differences in approach across relevant jurisdictions and be proactive in ensuring their organisation meets these requirements. Generally, principles- or outcomes-based regulation places a greater onus on the Compliance function to interpret the regulation and provide advice to the business on suitable outcomes and involves working closely with the other two lines of defence to interpret and apply the guidance in the context of the business, and to put in place flexible guardrails that empower innovation. This approach to regulation (particularly in the UK and other jurisdictions that do not lay out prescriptive requirements) does however offer firms the advantage of flexibility given the fast-moving technology landscape.

As Compliance functions seek to be both more efficient and effective in executing their role as a strategic partner to the business and more agile in responding to external demands, AI also presents opportunities for the function to enhance its own processes and move towards an insights-led, data-driven approach to compliance risk management. Again, this may require an evolution in the skill and resource mix of the function with a greater focus on data analytics.

For ambitious firms, AI presents an exciting opportunity to transform the way compliance risk management is undertaken enterprise-wide through creating end-to-end solutions. While point solutions can address specific needs and challenges, they should be considered as part of a broader, coherent ecosystem that delivers transformative change.

> **"The advancements in AI present exciting possibilities to transform the financial services industry, through enhanced use of machine learning and data analytics"**

Next Steps for Compliance Functions

The majority of firms have started their AI journey, with leading firms now relatively mature in deploying AI across their organisation. By contrast, firms that are not currently investing in and embracing new technologies risk falling behind the curve in terms of evolving best practice. The rapid pace of change and potential impacts means that the Compliance function needs to be proactively involved in decision making and the design of solutions, acting as a key business partner in identifying and managing risks associated with AI. Chief Compliance Officers (CCOs) should be championing and driving the enterprise-wide innovation agenda, leveraging AI capabilities as part of their medium- and long-term plans in order to enhance the execution and efficiency of their compliance mandate and deliver technology-enabled change. Compliance skills (such as understanding regulation and an ability to assess compliance risks) will continue to be essential with respect to AI, but there is also a need for digital upskilling in order to effectively challenge the business and to realise the potential of AI in the enhancement of compliance processes. Delivering this change agenda will require collaboration and the breaking down of silos across the organisation.

In light of this, we end our paper with a series of recommendations aimed primarily at our member firms seeking to enhance their AI capabilities, but with broader relevance to other industry stakeholders. Taking action now will enable you to get ahead of the curve and transform the way that you undertake compliance across the organisation, as well as proactively identify and manage associated risks.

- **Get your governance right and embed accountability:** Robust AI governance practices need to be established around AI, or incorporated into existing governance and risk practices as appropriate, in alignment with internal organisational and external regulatory principles. This could include reviewing or developing inventories of AI systems, documenting their origin, training and data inputs, and ensuring compliance with ethical guidelines. It is also essential that you define accountabilities and interaction models in relation to technology risk (AI) governance, including how the Compliance function engages and gets adequate line of sight across all activities.

- **Understand your firm's AI risk exposure:** While AI risks are considered as part of existing frameworks, the Compliance function plays a key role in the development of an enterprise-wide view of risks associated with the deployment of AI. These risks will also need to be incorporated into existing compliance frameworks and risk practices as required (for example, compliance assessments and monitoring). Putting in place a central taxonomy that defines potential AI risks and harms, as well as examples of how they might manifest in specific use cases, would drive consistency and alignment across the firm, and should include consideration of the time horizon of these risks, including short, medium and long term.

"The rapid pace of change and potential impacts means that the Compliance function needs to be proactively involved in decision making and the design of solutions"

- **Build AI into the Compliance function's transformation agenda:** Compliance transformation plans should include consideration of how automation and technology can be used to enhance the performance of the function. Point solutions to specific problems will not deliver sustainable transformation; instead, solutions should be considered as part of, and incorporated into, a broader ecosystem.

- **Collaborate effectively with teams across the organisation** to deliver a technology-enabled, end-to-end approach to compliance risk management: Transformation cannot be delivered into siloes, and instead requires collaboration across the lines of defence with the Compliance function as a critical player in the process from the beginning. A starting point could be the consolidation of the AI use cases currently deployed or planned across the key stages of the compliance risk management process in order to identify any gaps or potential synergies.

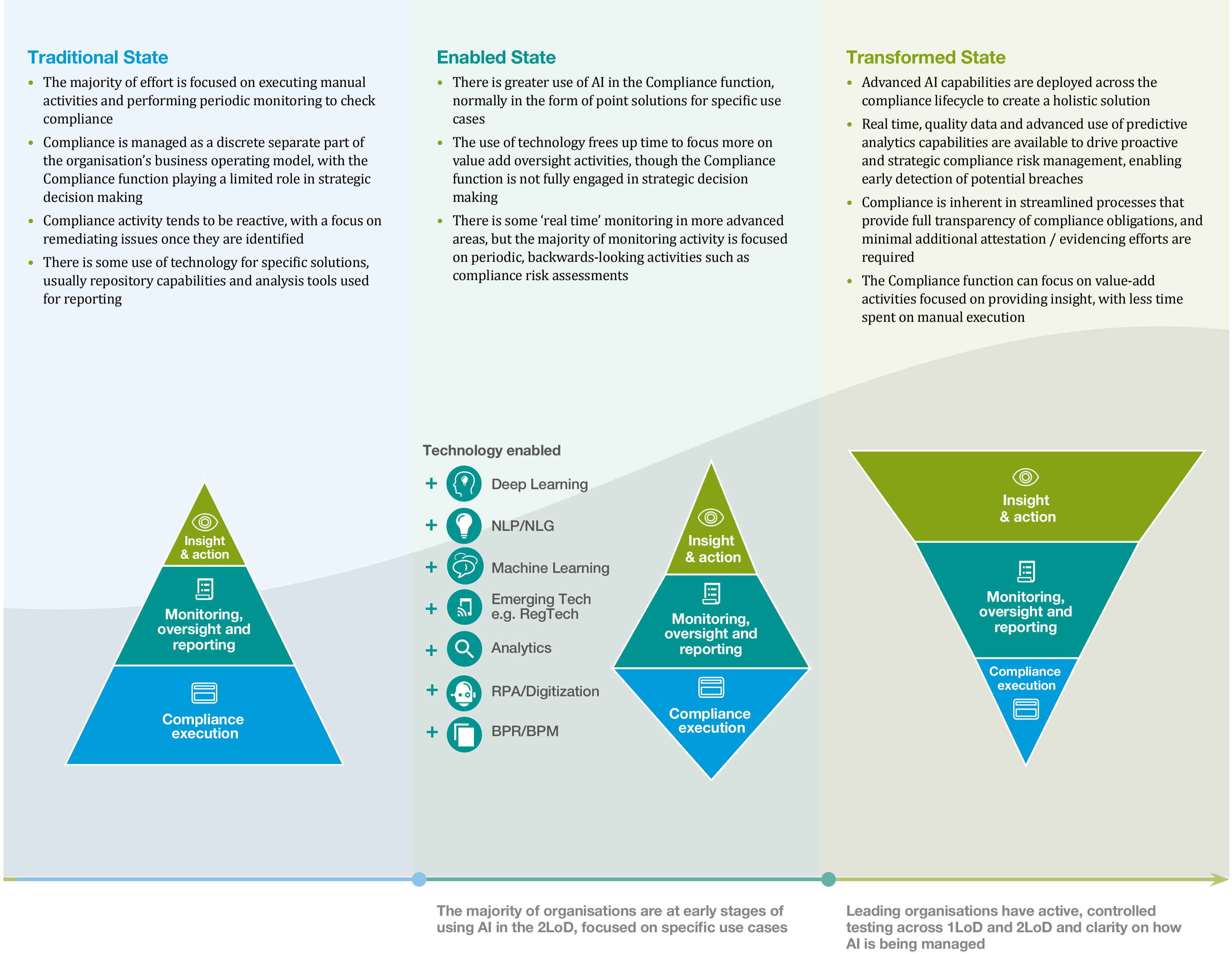
- **Plan for your future Compliance function:** In order to future-proof your Compliance function, you need to develop a forward looking view of the skills that will be required in the future, and assess where there are currently gaps. This will support a robust plan for training and recruitment to ensure that the function has the skills to carry out its 2LoD responsibilities in an evolving technology landscape.

- **Demonstrate and quantify the impact of compliance transformation:** AI has the potential to enhance compliance outcomes through real-time monitoring and preventative controls. In order to demonstrate the impact of changes, you should consider the use of existing or additional metrics (for example, in fraud or conduct) related to AI deployment that can demonstrate the impact of AI on the firm's compliance outcomes and drive future investment.

- **Engage effectively and contribute to public policy:** In the context of increased activity in the AI public policy and regulatory space, the industry needs to be active in providing input into, and shaping, these initiatives by collaborating and providing expertise through established channels. Industry collaboration, through industry associations and forums and other research initiatives, will also be critical in helping organisations to understand peer practice and develop a consistent approach to managing AI risks.

The Path to AI-enabled Compliance

Advancements in AI and automation have the potential to transform the way that compliance risk management is executed end-to-end across the organisation, a journey that can be led by a technology-enabled, future-proofed Compliance function.



Traditional State

- The majority of effort is focused on executing manual activities and performing periodic monitoring to check compliance
- Compliance is managed as a discrete separate part of the organisation's business operating model, with the Compliance function playing a limited role in strategic decision making
- Compliance activity tends to be reactive, with a focus on remediating issues once they are identified
- There is some use of technology for specific solutions, usually repository capabilities and analysis tools used for reporting

Enabled State

- There is greater use of AI in the Compliance function, normally in the form of point solutions for specific use cases
- The use of technology frees up time to focus more on value add oversight activities, though the Compliance function is not fully engaged in strategic decision making
- There is some 'real time' monitoring in more advanced areas, but the majority of monitoring activity is focused on periodic, backwards-looking activities such as compliance risk assessments

Transformed State

- Advanced AI capabilities are deployed across the compliance lifecycle to create a holistic solution
- Real time, quality data and advanced use of predictive analytics capabilities are available to drive proactive and strategic compliance risk management, enabling early detection of potential breaches
- Compliance is inherent in streamlined processes that provide full transparency of compliance obligations, and minimal additional attestation / evidencing efforts are required
- The Compliance function can focus on value-add activities focused on providing insight, with less time spent on manual execution

Technology enabled

- + Deep Learning
- + NLP/NLG
- + Machine Learning
- + Emerging Tech e.g. RegTech
- + Analytics
- + RPA/Digitization
- + BPR/BPM

The majority of organisations are at early stages of using AI in the 2LoD, focused on specific use cases

Leading organisations have active, controlled testing across 1LoD and 2LoD and clarity on how AI is being managed

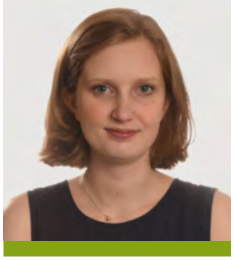
Glossary

Term	Definition
1st Line of Defence (1LoD)	Owns and executes risk mitigation in day-to-day business activities. Includes Front Office, Business Risk & Control, Operations and Technology teams.
2nd Line of Defence (2LoD)	Provides oversight and challenge to first line risk mitigation efforts, and develops risk management frameworks in response to performance and emerging threats. Includes Compliance and Risk functions.
3rd Line of Defence (3LoD)	Internal audit function, which is independent and conducts reviews of the overall compliance risk management framework (including of the Compliance function).
Algorithmic trading	An automated trading methodology in which computers are programmed to take certain actions in response to specific market conditions.
Artificial intelligence (AI)	The ability of machines to imitate human intelligence processes and comprises a number of different capabilities
Automation	The use of technology to perform actions with minimal human involvement.
Behavioural analytics	Collecting data on user behaviours in order to enable a holistic view of their activity and to gain insights by observing and analysing patterns or anomalies.
Chatbots	A computer application, utilising machine learning and artificial intelligence, designed to simulate human conversational dialogue.
Compliance culture	Shared values and behavioural norms within an organisation that promote ethical conduct and adherence to regulation.
Deep learning	A machine learning technique in which layers of neural networks are used to process data and make decisions.
Explainability	The degree of which AI and/or ML decision making processes, leading to the generated outputs, can be understood by humans at an acceptable level.
Front Office	An organisation's customer-facing operations, including marketing, sales and service departments.
Generative AI (GenAI)	The ability to create new written, visual and auditory content given prompts or existing data
Horizon scanning	The systematic monitoring and prediction of upcoming regulatory changes that could pose threats and/or opportunities to the organisation.
Know Your Customer (KYC)	The process of verifying a customer's identity and understanding the risks associated with their activities, in order to help prevent financial crime.
Large Language Model (LLM)	A deep learning algorithm that processes and utilises massive data sets.
Machine learning (ML)	A subset of AI that enables machines to learn from existing data and improve upon that data to make decisions or predictions.
Natural Language Processing (NLP)	The automatic manipulation of natural language, like speech and text, by software.
Scraping	A technique used to extract information, generally from websites, into user-generated reports.

Contacts

AFME

Louise Rodger
Director
louise.rodger@afme.eu
+44 (0)20 3828 2742



Fiona Willis
Associate Director
fiona.willis@afme.eu
+44 (0)20 3828 2739

Nicky Singh
Associate
nicky.singh@afme.eu
+44 (0)203 828 2760

PwC

Andrea Wintermantel
Partner
andrea.wintermantel@pwc.com
+44 7733 333 944

Balaji Krishnamurthy
Partner
balaji.krishnamurthy@pwc.com
+44 7590 352 503

Sarah Kidd
Senior Manager.
sarah.m.kidd@pwc.com
+44 7722 984 872

Alaister Moull
Director
alaister.moull@pwc.com
+44 7706 285 028

/ About AFME

The Association for Financial Markets in Europe (AFME) is the voice of all Europe's wholesale financial markets, providing expertise across a broad range of regulatory and capital markets issues.

We represent the leading global and European banks and other significant capital market players.

We advocate for deep and integrated European capital markets which serve the needs of companies and investors, supporting economic growth and benefiting society.

We aim to act as a bridge between market participants and policy makers across Europe, drawing on our strong and long-standing relationships, our technical knowledge and fact-based work.

Focus

on a wide range of market, business and prudential issues

Expertise

deep policy and technical skills

Strong relationships

with European and global policymakers

Breadth

broad global and European membership

Pan-European

organisation and perspective

Global reach

via the Global Financial Markets Association (GFMA)

afme/
Finance for Europe

London Office
Level 10
20 Churchill Place
London E14 5HJ
United Kingdom
+44 (0)20 3828 2700

Brussels Office
Rue de la Loi, 82
1040 Brussels
Belgium
+32 (0) 2 883 5540

Frankfurt Office
Neue Mainzer Straße 75
Bürohaus an der Alten Oper
60311 Frankfurt am Main
Germany
+49 (0) 69 710 456 660

Press enquiries
Rebecca Hansford
Head of Communications and Marketing
rebecca.hansford@afme.eu
+44 (0)20 3828 2693

Membership
Elena Travaglini
Head of Membership
elena.travaglini@afme.eu
+44 (0)20 3828 2733

Follow AFME on Twitter
@AFME_EU