ISSN: 3033-4136

DOI : https://doi.org/10.36399/gla.pubs.351604

Simplifying Compliance: The Role of AI and RegTech

FRIL

Financial Regulation Innovation Lab

FinTech Scotland®

University of Glasgow

University of Strathclyde Glasgow

Iain MacNeil, School of Law, University of Glasgow
Mark Cummins, Strathclyde Business School, University of Strathclyde
Alessio Azzutti, School of Law, University of Glasgow
Chuks Otioma, Adam Smith Business School, University of Glasgow

We acknowledge funding from Innovate UK, award number 10055559.

Corresponding authors: Alessio Azzutti, Iain MacNeil, Chuks Otioma Adam Smith Business School, University of Glasgow, Adam Smith Building, 2, Discovery Place, Glasgow, G11 6EY, UK
Email: alessio.azzutti@glasgow.ac.uk; iain.macneil@glasgow.ac.uk; chuks.otioma@glasgow.ac.uk

Mark Cummins Strathclyde Business School, University of Strathclyde, 199 Cathedral Street, Glasgow G14 OQU
Email: mark.cummins@strath.ac.uk

Financial Regulation Innovation Lab

Who are We?

The Financial Regulation Innovation Lab (FRIL) is an industry-led collaborative research and innovation programme focused on leveraging new technologies to respond to, shape, and help evolve the future regulatory landscape in the UK and globally, helping to create new employment and business opportunities, and enabling the future talent.

FRIL provides an environment for participants to engage and collaborate on the dynamic demands of financial regulation, explore, test and experiment with new technologies, build confidence in solutions and demonstrate their ability to meet regulatory standards worldwide.

What is Actionable Research?

FRIL will integrate academic research with an industry relevant agenda, focused on enabling knowledge on cutting-edge topics such as generative and explainable AI, advanced analytics, advanced computing, and earth-intelligent data as applied to financial regulation. The approach fosters cross sector learning to produce a series of papers, actionable recommendations and strategic plans that can be tested in the innovation environment, in collaboration across industry and regulators.

Locally-led Innovation Accelerators delivered in partnership with DSIT, Innovate UK and City Regions

Department for Science, Innovation & Technology

UKRI Innovate UK

GLASGOW CITY REGION

FRIL White Paper Series

Simplifying Compliance: The Role of AI and Regtech

Alessio Azzutti* Mark Cummins** Iain MacNeil* Chuks Otioma*

** University of Glasgow*

*** University of Strathclyde*

March 2025

Abstract: The Financial Regulation Innovation Lab (FRIL) is dedicated to simplifying compliance through emerging technologies, with Artificial Intelligence (AI) representing the latest evolution in regulatory technology (RegTech). Building on previous research and industry engagement—including workshops, blogs, webinars, and a micro-credential course—this White Paper presents key considerations for the conceptualisation, design, and implementation of AI-driven compliance systems. We begin by examining the nature of regulatory rules and the compliance process before exploring the complexities that challenge AI deployment. The discussion then shifts to Generative AI (GenAI) as a cutting-edge innovation, analysing its capabilities and relevance to compliance functions. A focused use case on GenAI in robo-advisory services illustrates AI's potential in asset management, where conventional AI is already well-established. Finally, we consider the broader organisational implications of AI adoption, emphasising the opportunity to view compliance as an embedded and adaptive function able to evolve and respond to changing stakeholder expectations and regulatory frameworks.

TABLE OF CONTENTS

1. Introduction 1
2. The Nature of Regulatory Rules and Compliance 1
3. Compliance in a Complex world: The Context for AI Adoption 3
4. AI Capabilities in Regulatory Compliance 8
4.1 Current Applications of AI in Compliance Systems 8
4.2 Strategic Considerations in AI-Based Compliance Systems 9
4.3 Generative AI (GenAI) - A Step Change in AI-Based Compliance Systems 11
4.4 Designing GenAI-Based Compliance Systems 12
4.4.1 Capabilities mapping across the compliance process 12
4.5 Business Considerations across the Compliance Process 14
4.6 Design Principles across the Compliance Process 15
4.7 Use Case Discussion: GenAI and Robo-Advisory Services 16
4.7.1 GenAI and XAI in robo-advisory services 16
4.7.2 Framing AI within robo-advisory firms and value chains 17
5. From AI Governance to 'Embedded Compliance' 21
5.1 Challenges for Compliance Alignment 22
5.2 Seizing the AI Opportunity: Multi-Layered Governance and Process-Based Compliance 23
6. Outlook and Challenges 26
About the Authors 27

1. Introduction

One of the key strategic themes of the Financial Regulation Innovation Lab (FRIL) is simplifying compliance through the use of emerging technologies. In this context, Artificial Intelligence (AI) represents the latest stage in the evolution of regulatory technology (RegTech) and builds on earlier digital initiatives which have encompassed activities such as identity verification, regulatory reporting and money laundering detection. Our research and engagement on this issue have to date comprised a workshop with industry participants and a related blog,[1] a webinar, and a micro-credential course[2] which presented a systematic examination of the role of AI in compliance, encompassing academic research and practical insights from the FinTech community. In this White Paper we build on and extend our prior work to present an overview of key issues for consideration in the conceptualisation, design and implementation of AI systems for compliance. We start by considering the nature of regulatory rules and the fundamentals of the compliance process. We then move on to consider various forms of complexity in the compliance environment which pose challenges for AI implementation. Our attention then shifts to the topic of Generative AI (GenAI) as the frontier of AI innovation to date, identifying capabilities and mapping these onto the business context and the compliance process. This is linked to a use case discussion on GenAI in the context of robo-advisory services, a domain of asset management where conventional AI is already well-established. We conclude by considering the potential for AI to be deployed in an organisational setting in which compliance is embedded in core business processes and is responsive to stakeholder expectations and regulatory change.

2. The Nature of Regulatory Rules and Compliance

While many regulatory rules are made by financial regulators such as the Financial Conduct Authority and Prudential Regulation Authority in the UK, there are also obligations for financial firms arising from broader statutory regimes, such as data protection and consumer protection. Moreover, in the case of common law jurisdictions, there are also principles and rules that may be applicable to financial relationships, products and services. Perhaps the most important is the concept of fiduciary duty, which arises in any relationship of trust and requires a duty of loyalty on the part of the fiduciary towards the constituent. Agency is a common example, in which the agent owes a duty of loyalty to the client which requires the interest of the client to be paramount. This duty is strict and is not limited by the operation of quasi-fiduciary regulatory rules, such as the new Consumer Duty framework that has recently taken effect in the UK. Thus, the first key task (Figure 1) in framing a strategy for regulatory compliance is to undertake horizon scanning across all the relevant legal obligations that are triggered by a firm's activities.

[1] FinTech Scotland, 'AI and RegTech: Industry Insights on AI in Financial Regulation' (*FinTech Scotland*, 13 August 2024) <https://www.fintechscotland.com/ai-and-regtech-industry-insights-on-ai-in-financial-regulation> accessed 14 March 2025.

[2] University of Glasgow, 'Microcredential in AI and RegTech' (*Zenodo*, 9 October 2024) <https://doi.org/10.5281/zenodo.15017951> accessed 14 March 2025.

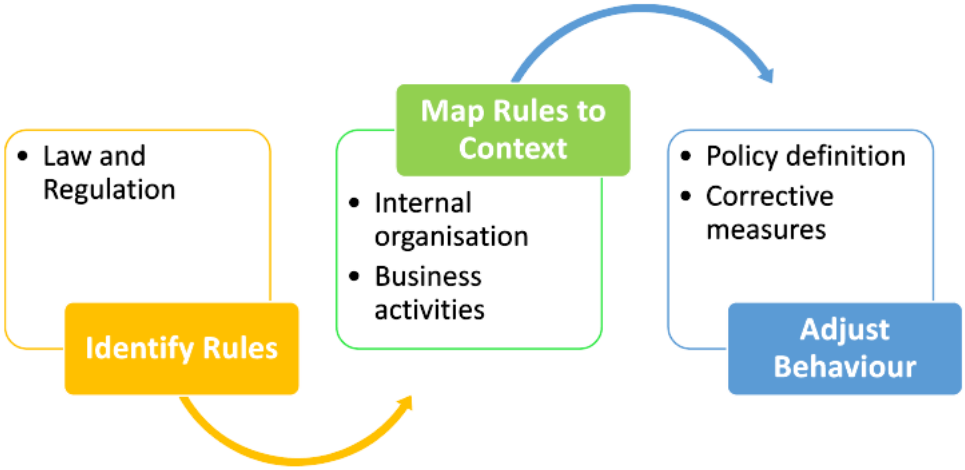

Figure 1 The Fundamentals of Compliance

The second stage (Figure 1) in the compliance process is to understand the nature of rules. Rule type represents a structural dimension of rules that is independent of the content of the rule. Thus, the same rule may be framed as different rule types and have different compliance implications. It follows that it is important to understand both the rule type and the content of the rule in order to determine the compliance response. In our AI & RegTech webinar we identified several types of rules as follows:

• ***Mandatory rules***: this is the basic type of regulatory rule and requires simple compliance, albeit that it needs to be interpreted and mapped on to the relevant context in which a firm operates.

• ***Default rules***: these rules are subject to adjustment by the contracting parties. There are many examples in corporate law but much fewer in financial regulation due to the need to protect retail customers.

• ***Comply or explain rules***: these rules do not require strict compliance, but instances of non-compliance need to be explained. They are based on the premise that disclosure and market discipline can ensure that rules are either complied with or that better solutions are adopted in specific contexts.

• ***Voluntary codes, standards, guidance***: such rules are not binding in their nature, but they can have some legal effect in certain situations, such as where parties incorporate them by reference in their contracts or where regulatory rules refer to guidance as behaviour that is compliant with rules that pose compliance risks through their open-ended formulation.

The third stage (Figure 1) in the compliance process is to adjust behaviour to comply with the relevant rules. In some instances, the required action may be clearly signalled by the regulatory rules (e.g. reporting) but in others there may well be some discretion for regulated firms to choose how they implement the rule (e.g. FCA Principles for Businesses in the UK).

Understanding the compliance process is crucial to framing a strategic approach to the use of AI in support of compliance activities. Two further points merit consideration. One is that the recent introduction of Consumer Duty in the UK marks a shift in the regulatory approach from a focus on inputs by firms to an emphasis on outcomes for consumers. That requires a more prominent role for monitoring consumer outcomes and ensuring that appropriate data is available to evidence positive outcomes. Another is that the

increasing focus on corporate purpose in the context of the rise of ESG suggests that compliance may need to go beyond legal and regulatory rules to integrate the values and expectations that firms set for themselves in dealing with customers.

The need to frame the role of AI in compliance by reference to a holistic model of compliance is supported by the recent experience in the context of the provision of finance for car purchase in the UK. Such transactions are often structured such that the car dealer also acts as a credit broker on behalf of a lender and thereby falls under the relevant provisions of the Consumer Credit Act 1974 and the conduct of business rules made by the FCA (CONC in the FCA Handbook). However, the residual role of the common law on fiduciary duty in such transactions was made clear by a recent Court of Appeal decision[3] which focused on disclosure of commissions paid by lenders to credit brokers. The Court of Appeal held that such transactions may give rise to a fiduciary duty between the credit broker and customer, requiring full and adequate disclosure of any commission payment, as well as prioritisation of the customer's interests. If breach of fiduciary duty is established, lenders will likely face liability for repayment of commission to the customer. The aggregate potential liability across the UK banking system from this potential liability is estimated at £23bn, making it the most significant compliance failure since the case of payment protection insurance (PPI).[4]

Thus, the key starting point is that organisations are subject to a spectrum of different compliance obligations, including both externally imposed regulations and internally established aims and controls. While, in principle, organisations are to some extent free to determine their 'optimal' level of compliance, they inherently assume non-compliance risks associated with it. Furthermore, misunderstanding or even disregarding a rule effectively transforms it into a retained compliance risk. Acknowledging compliance as a structured yet fluid spectrum of obligations compels firms to engage with their regulatory environment in a more deliberate and informed manner. The challenge extends beyond mere adherence to individual rules; it involves deciphering the intricate web of legal and regulatory requirements, internal governance structures and (ethical) values, strategic priorities and decision-making that collectively shape the scope and function of compliance systems.

3. Compliance in a Complex world: The Context for AI Adoption

At its core, regulatory compliance is a multi-objective optimisation problem[5]—one that requires firms to align their business operations with an evolving regulatory framework while balancing strategic goals, risk tolerance, and externally imposed constraints. The compliance landscape is inherently complex, shaped by the interplay of four interwoven dimensions—(a) financial, (b) regulatory, (c) organisational, and (d) technological. To navigate this complexity effectively, firms must first delineate the

[3] *Johnson v FirstRand* (and related cases) [2024] EWCA Civ 1282. The Supreme Court will hear an appeal in this case in April 2025.

[4] See further Kana Inagaki et al., 'UK Motor Finance in Disarray after Court Rules against Hidden Commissions' (*Financial Times*, 6 November 2024) <https://www.ft.com/content/444c1dac-4e7e-4480-b920-f5689548c0c7> accessed 14 March 2025.

[5] See further Seongbeom Park, Hyunju Lee, and Dowon Kim, 'Regulatory Compliance and Operational Efficiency in Maritime Transport: Strategies and Insights' (2024) 155 *Transport Policy* 161 <https://doi.org/10.1016/j.tranpol.2024.06.024> accessed 14 March 2025.

precise boundaries of their compliance space—a prerequisite for integrating regulatory obligations into business processes while proactively managing non-compliance risks. Without this foundation, compliance efforts risk becoming fragmented and inefficient, particularly in large and complex organisations. As will be further explored, AI solutions are increasingly regarded as key enablers of better regulatory governance, offering the potential to mitigate complexity across the four dimensions and ultimately achieve better compliance outcomes.

a) *Financial complexity*

The financial system is a highly dynamic and complex ecosystem, shaped by an ever-evolving network of market actors—each driven by distinct business objectives, strategic interests, and individual preferences.[6] Financial complexity has intensified over the past few decades, fuelled by a series of interrelated developments, including globalisation, liberalisation, and financialisation. The expansion of cross-border financial activities, the progressive deregulation of capital flows, and the growing influence of financial logic across various sectors have deepened market interconnectedness while amplifying systemic vulnerabilities at all levels of the financial system.[7]

Firms typically encounter diverse compliance challenges arising from financial complexity, with their nature and intensity varying across business contexts. To illustrate, organisations engage in various market relationships, as defined by the underlying contractual agreements. Whether between firms and clients (B2C) or among firms themselves (B2B), these relationships are unique to each financial institution and, collectively, contribute to the degree of financial complexity a firm must manage.

Some sources of financial complexity—and the compliance uncertainty they generate—are endogenous to firms and, thus, can be managed internally by organisations. One example is the adoption of less complex (and opaque) product designs, which can typically benefit transparency. By contrast, other sources of complexity are exogenous to firms' specific business activities, including the corresponding financial relationships with clients and other business stakeholders. These include market-wide interdependencies, macroeconomic shifts, as well as regulatory changes.

b) *Regulatory complexity*

As discussed in Section 2, another key dimension of complexity arises from the continuous expansion and increasing sophistication of financial regulation. As regulatory frameworks evolve, complexity grows. In the words of Gai et al regulatory complexity refers to regulatory requirements that vary across contingencies at a highly granular level, often leading to substantial non-linearities and unpredictability in their effect. This complexity is further exacerbated by heterogeneity across jurisdictions, market segments, and business lines.[8] An additional layer of regulatory complexity results from emerging technology-specific regulations, which in many areas supplements—but do not yet replace—the well-established principle of

[6] See further Stefano Battiston et al., 'Complexity Theory and Financial Regulation' (2016) 351(6275) *Science* 818 <https://www.science.org/doi/full/10.1126/science.aad0299> accessed 14 March 2025.
[7] See, e.g., Steven L. Schwarcz, 'Regulating Complexity in Financial Markets' (2009) 87(2) *Washington University Law Review* 211 <https://wustllawreview.org/wp-content/uploads/2021/10/87.2.1.pdf> accessed 14 March 2025.
[8] Prasanna Gai et al., 'Regulatory Complexity and the Quest for Robust Regulation' (2019) ESRB Reports of the Advisory Scientific Committee No 8, July 2019 <https://www.esrb.europa.eu/pub/pdf/asc/esrb.asc190604_8_regulatorycomplexityquestrobustregulation~e63a7136c7.en.pdf> accessed 14 March 2025.

technology neutrality.[9]

A clear example of this trend is the growing regulatory focus on technological aspects of financial services. Over the past decade, technology-specific regulations have expanded across key areas, including, for instance, industry-specific frameworks for payments (e.g., Payment Services Directive 2) and investments and trading (e.g., Markets in Financial Instruments Directive II). Additionally, new rules address operational resilience (e.g., Digital Operational Resilience Act), cybersecurity (e.g., Network and Information Security Directive 2), and emerging technologies such as AI (e.g., EU AI Act) and DLT/blockchain (e.g., DLT Pilot Regime and Markets in Crypto-Assets Regulation - MiCA). Another rapidly evolving regulatory domain is financial data governance, which has developed into multi-layered regulatory architecture, with each instrument serving distinct policy objectives.[10] Therefore, the way in which organisations adopt and integrate technology directly determines their technological complexity and has a significant impact on their compliance burden.

Despite being a widely recognised phenomenon, regulatory complexity lacks a universally accepted definition or measurement framework.[11]

c) *Organisational complexity*

Organisational complexity arises from a firm's internal structure, governance, and operational dynamics.[12] Organisations function as complex, adaptive systems where both human and financial capital as well as other resources, including technology, are integrated into hierarchical structures, interdependent relationships, and coordinated activities. Their directions are regulated by internal governance mechanisms, which influence how firms respond to external pressures and engage with key stakeholders (e.g., consumers, competitors, suppliers, regulators, etc.).[13]

This third dimension of complexity, thus, relates to internal organisational factors. At a macro level, it manifests in a firm's business scale, scope, and reach—such as its product differentiation and global footprint. At a micro level, complexity emerges in the daily challenges employees face, including unclear role definitions, cumbersome processes, and resources constraints.[14]

Organisational complexity not only affect operational efficiency but also creates barriers to aligning business strategy with regulatory

---

[9] See Alessio Azzutti, 'AI Governance and Algorithmic Trading: Some Regulatory Insights from the EU AI Act' (2024) 41(1) *Banking & Finance Law Review* 133 <https://dx.doi.org/10.2139/ssrn.4939604> (Preprint version) accessed 14 March 2025.

[10] See Douglas W. Arner, Giuliano G. Castellano, and Ēriks K. Selga, 'Financial Data Governance' (2023) 74(2) *UC Law Journal* 235 <https://repository.uclawsf.edu/hastings_law_journal/vol74/iss2/2> accessed 14 March 2025.

[11] See Jean-Edouard Colliard and Co-Pierre Georg, 'Measuring Regulatory Complexity' (2024) SSRN Preprint 1 <https://dx.doi.org/10.2139/ssrn.3523824> accessed 14 March 2025.

[12] See, e.g., Simon Okwir et al., 'Performance Measurement and Management Systems: A Perspective from Complexity Theory' (2018) 20(3) *International Journal of Management Reviews* 731 <https://doi.org/10.1111/ijmr.12184> accessed 14 March 2025.

[13] Kevin J. Dooley, 'A Complex Adaptive Systems Model of Organization Change' (1997) 1(1) *Nonlinear Dynamics, Psychology, and Life Science* 69 <https://doi.org/10.1023/A:1022375910940> accessed 14 March 2025.

[14] Julian Birkinshaw and Suzanne Heywood, 'Putting Organizational Complexity in Its Place' (*McKinsey & Company*, May 2010) <https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Organization/Our%20Insights/Putting%20organizational%20complexity%20in%20its%20place/Putting%20organizational%20complexity%20in%20its%20place.pdf> accessed 14 March 2025.

requirements, thus complicating effective compliance. Often-discussed challenges in this regard include: (i) defining compliance responsibilities within complex organisational structures and hierarchies to prevent role overlaps and accountability gaps; (ii) embedding compliance into business operations by default to streamline processes, minimise bottlenecks, break down data siloes, and prevent information overloads, thereby improving coordination and consistency throughout the compliance lifecycle; and (iii) managing increasingly complex and often conflicting reporting obligations across business units, operational functions, technological systems, regulatory jurisdictions, and external stakeholders.[15]

d) *Technological complexity*

Technological complexity refers to the tendency of ICT systems, networks, and infrastructures to grow increasingly complex over time. This phenomenon results from the interplay of three intertwined developments: (i) path dependency, as technological progress builds upon existing socio-technical frameworks; (ii) the growing sophistication and capability of technology applications; and (iii) the deepening interconnectivity between technologies, amplifying system complexity and network effects.[16]

A major source of complexity is the integration of new technologies into legacy systems—many of which were never designed for cloud computing, AI, or blockchain solutions. Financial institutions still too often rely on outdated ICT infrastructures, creating risks related to operational inefficiencies, cybersecurity vulnerabilities, and compliance bottlenecks. For instance, firms still operate COBOL-based mainframes to implement real time transaction processing and other AI applications.[17]

Technological sophistication itself is another driver of complexity. For instance, the domain of financial AI applications has evolved through multiple waves and generations.[18] Unlike traditional rule-based AI systems (often referred to as 'Good Old-Fashioned AI'), advanced models—such as those based on machine learning, deep learning, up to the latest GenAI architectures—introduce additional governance challenges. These include increased opacity, greater autonomy, concerns over output reliability, and even unpredictable emergent behaviour.[19] Especially in high-stakes applications—such as consumer-facing use cases (e.g.,robo-advisors, which we examine as a use case for AI in section 4) and critical back-office functions (e.g., AML/fraud detection and regulatory compliance)—firms must ensure robust technology governance frameworks. However, these efforts are further complicated by a growing shortage of skilled professionals in AI, cybersecurity, and RegTech, all of which

[15] See further Tom Butler and Leona O'Brien, 'Understanding RegTech for Digital Regulatory Compliance' in Theo Lynn et al. (eds), *Disrupting Finance* (Palgrave Pivot 2019) <https://doi.org/10.1007/978-3-030-02330-0_6> accessed 14 March 2025.

[16] See, e.g., Tom Broekel, 'Measuring Technological Complexity – Current Approaches and a New Measure of Structural Complexity' (2018) arXiv Preprint 1, pp. 7-9 <https://doi.org/10.48550/arXiv.1708.07357> accessed 14 March 2025.

[17] COBOL (Common Business-Oriented Language) is a high-level, English-like programming language developed specifically for business data processing. Its verbosity enables programmers to use a readable, easily maintainable language that can function across mainframe computers and operating systems. See Chrystal R. China and Michael Goodwin, 'What Is COBOL?' (*IBM*, 19 April 2024) <https://www.ibm.com/think/topics/cobol> accessed 14 March 2025.

[18] See Azzutti (n 9) above, discussing the phenomenon from an algorithmic trading perspective.

[19] E.g., Iñaki Aldasoro et al., 'Intelligent Financial System: How AI is Transforming Finance' (2024) BIS Working Papers No 1194, 4-8 <https://www.bis.org/publ/work1194.pdf> accessed 14 March 2025.

renders technological change management even more challenging.[20]

Lastly, the interconnected nature of digital financial markets adds another layer of complexity. As financial systems become increasingly integrated, interdependencies between networks, platforms, and institutions contribute to systemic risk. This is particularly evident in highly computationally intensive domains such as financial trading, where AI algorithms may often interact in unpredictable ways, sometimes amplifying market volatility and triggering flash crashes. These interactions can also lead to emergent behaviours, such as autonomous AI manipulation and algorithmic collusion.[21] Similarly, in digital finance and FinTech ecosystems, vulnerabilities at a single point—such as a cyberattack or data breach—can rapidly propagate across entire networks, disrupting both national and cross-border payment systems, including decentralised finance (DeFi) platforms.[22]

***

As illustrated by the four dimensions above, complexity is an inherent feature of the compliance space in which financial firms operate. However, complexity should not be viewed as an intractable constraint. Instead, firms should strive to adopt a complexity-informed approach to compliance. This requirement first entails acknowledging the interdependencies between financial, regulatory, organisational, and technological dimensions. Based on this understanding, it then requires researching effective ways to integrate compliance management into broader strategic, operational, and technological frameworks. While firms can proactively manage some sources of complexity through business process management (BPM), governance adjustments, and regulatory engagement, others demand adaptive capacity rather than direct control. Amid an increasingly complex compliance world, RegTech solutions—especially those based on AI—are today proposed as critical tools to optimise compliance efforts.[23] When properly integrated within organisations, we believe AI tools can support financial institutions in mitigating certain dimensions of complexity. Thanks to AI, organisations may better understand and address complex regulatory demands, streamline processes, and deal with multiple forms of risk—all this with greater accuracy and efficiency. Ultimately, AI's true potential as a core RegTech technology depends on its demonstrated capabilities, together with fundamental governance aspects. It is precisely on this key issue that we shift our focus below.

---

[20] See, e.g., Muhammad Daffa Firiza et al., 'The Role of RegTech in Automating Compliance and Risk Management' (2024) *2024 12th International Conference on Cyber and IT Service Management (CITSM)*, Batam, Indonesia, 2024 <https://doi.org/10.1109/CITSM64103.2024.10775610> accessed 14 March 2025.

[21] See Alessio Azzutti, Wolf-Georg Ringe, and H. Siegfried Stiehl, 'Machine Learning, Market Manipulation and Collusion on Capital Markets: Why the "Black Box" Matters' (2021) 43(1) *University of Pennsylvania Journal of International Law* 79 <https://scholarship.law.upenn.edu/jil/vol43/iss1/2> accessed 14 March 2025.

[22] The growing integration between TradFi and DeFi introduces new risks, increasing the fragility of interconnected digital financial ecosystems. Cyberattacks on DeFi platforms, for example, can trigger ripple effects on centralised exchanges (CEXs) and financial institutions with DeFi exposure. A notable example is the $1.5 billion heist in February 2025 by the North Korean Lazarus Group on the Bybit exchange, which disrupted both DeFi liquidity pools and cross-border payment systems. Federal Bureau of Investigation, 'North Korea Responsible for $1.5 Billion Bybit Hack' (26 February 2025) <https://www.ic3.gov/PSA/2025/PSA250226> accessed 14 March 2025.

[23] See further Ross P. Buckley, Douglas W. Arner, and Dirk A. Zetsche, *FinTech: Finance, Technology and Regulation* (Cambridge University Press 2024) ch 4.

4. AI Capabilities in Regulatory Compliance

In this section, we first draw on insights from practitioners on current applications of AI in compliance systems. Next, we turn our attention to strategic considerations in AI-based compliance systems, exploring the particular benefits and limitations of GenAI as the current frontier of AI innovation. This sets the scene for a more detailed capabilities mapping of GenAI across the business context and compliance process, building on the earlier discussion of the fundamentals of compliance and complexity. In the last part of this section, we integrate insights from robo-advice as a use-case for GenAI in the light of its leading role in conventional AI implementation.

4.1 Current Applications of AI in Compliance Systems

Primary research perspectives from practitioners in the financial services industry revealed that current applications of AI in compliance systems are revolutionising how financial services organisations manage regulatory requirements. The current use of conventional AI models, largely based on machine learning (ML), offer practitioners unparalleled capability to analyse large complex datasets in order to generate actionable insights for compliance teams. The ability of AI to sift through vast amounts of structured and unstructured data quickly and accurately is shifting organisations' processes and procedures towards meeting compliance obligations, enhancing efficiency in several key areas. For example, AI-driven transaction monitoring systems analyse vast datasets in real-time to detect anomalies as potential fraud and money laundering, improving alert precision and reducing false positives. Natural Language Processing (NLP) automates regulatory reporting and document analysis, streamlining compliance with evolving legal requirements. Communication surveillance tools monitor internal communications, decoding complex trader jargon to detect illicit activities. AI also strengthens Know Your Customer (KYC) and Anti-Money Laundering (AML) processes by automating identity verification and assessing customer risk profiles through diverse data sources. By integrating AI and ML into compliance operations, financial organisations are proactively managing risks, swiftly adapting to regulatory changes, and allocating resources more effectively, ultimately creating more resilient compliance frameworks.

The practitioners highlighted though that this immense capability comes with its own set of challenges. One priority issue that was flagged is the necessity for financial services organisations to track data sources and address issues related to data quality. Ensuring the integrity and reliability of data is paramount for the effective functioning of AI in compliance systems. Furthermore, these concerns are heightened when data is handled by third-party vendors. There is a general apprehension about the security and privacy of data when it leaves an organisation's premises. Consequently, many organisations prefer to keep their AI operations in-house to maintain control over their data. That said, a Bank of England and FCA report[24] on AI development and uptake in UK financial services in 2024 shows that one-third of all AI use cases in financial services are implemented by third party providers — marking an increase from 17% recorded in 2022 — albeit this is clear evidence that most of the current AI implementations are conducted in-house.

Of course, concerns about the use of AI models in general, but particularly for compliance systems, goes beyond data. A commentary by

[24] Bank of England and Financial Conduct Authority, 'Artificial Intelligence in the UK Financial Services - 2024' (2024) <https://www.bankofengland.co.uk/report/2024/artificial-intelligence-in-uk-financial-services-2024> accessed 14 March 2025.

AI at Wharton,[25] emphasises the necessity for robust governance frameworks to manage potential risks, categorising them into data-related issues, AI/ML attacks, testing and trust concerns, and challenges in respect of AI regulation compliance. The paper provides a structured approach to AI governance, focusing on interpretability, discrimination, and risk mitigation, while acknowledging that strategies should be tailored to each organisation's unique context.

These concerns demand a prudent approach to deploying AI models to leverage the capabilities and exploit the opportunities. Despite the advanced capabilities of AI, practitioners viewed human intervention as indispensable. Humans need to be "in the loop" to oversee AI applications, ensuring that the insights generated are accurate and relevant. This human oversight is crucial for validating the AI outputs and making informed decisions based on those insights.

4.2 Strategic Considerations in AI-Based Compliance Systems

The adoption of AI is evolving from isolated, team-specific use cases to a more strategic, company-wide approach. This is fundamentally changing how AI systems are being designed, particularly when applied for regulatory compliance purposes. Corporate AI strategies are increasingly being integrated into overall corporate strategies. This shift indicates a growing recognition of the value that AI can bring to various facets of the organisation, prompting a more holistic and integrated implementation strategy. As noted by the Initiative for Applied Artificial Intelligence,[26] a company's corporate strategy and AI strategy must be closely linked to ensure AI initiatives create real business value. The AI vision, established under the AI strategy, should align with the company's overarching goals and serve as the foundation for identifying relevant AI use cases. Use cases must be carefully selected based on their ability to drive strategic objectives, ensuring that AI is not implemented in isolation. Additionally, enabling factors such as organisational structure, talent, technology infrastructure, and external partnerships must be in place to support and scale AI initiatives.

Practitioner views from FRIL's roundtable event confirmed that the design and compliance of AI systems play a critical role in ensuring these technologies remain effective, transparent, and trustworthy, with a strong focus on explainability, fairness, and the balance between in-house development and third-party vendor solutions. The discussion underscored the importance of responsible AI adoption and the need for robust governance frameworks.

Explainability emerged as a fundamental requirement in AI system design, particularly for financial institutions and FinTech firms that rely on AI for decision-making. Participants emphasised that the ability to articulate how AI models generate outcomes is a key differentiator among third-party vendors. In the competitive landscape, FinTech companies increasingly prioritise the transparency of their AI/ML solutions, using explainability as a trust-building mechanism. Beyond mere compliance, explainability enhances confidence among users and regulators, ensuring AI systems function as accountable tools rather than opaque "black boxes". This is especially crucial for AI-driven textual data analysis, where clarity in model interpretation is essential for credibility and adoption.

This call for explainability links directly to the concept of model governance and organisational efforts to ensure that AI models

[25] Artificial Intelligence/Machine Learning Risk & Security Working Group (AIRS), 'Artificial Intelligence Risk & Governance' (n.d.) <https://ai.wharton.upenn.edu/white-paper/artificial-intelligence-risk-governance> accessed 14 March 2025.

[26] See AppliedAI, 'Elements of a Comprehensive AI Strategy' (2023) <https://www.appliedai.de/en/insights/elements-comprehensive-ai-strategy> accessed 14 March 2025.

are robust, transparent, and compliant with regulatory standards. As noted by Bowden et al.[27], and with reference to an article appeared on Deloitte Insights[28], financial services firms must implement robust model governance structures to ensure effective oversight of AI systems. Given the inherently opaque, "black box" nature of AI models, they introduce distinct model risk exposures that require careful management through existing model risk frameworks, adapted to account for these new challenges. Deloitte identifies a three-tiered approach to governing AI models with a priority on explainability. The first line of defence involves model developers, who must integrate explainability into AI model deployment, whether the system is developed in-house or sourced from an external provider. These developers are responsible for embedding Explainable AI (XAI) techniques to meet the firm's established explainability standards. The second line of defence consists of model validators and risk managers, tasked with assessing AI models from an explainability standpoint, validating their outputs, and defining appropriate usage conditions based on explainability levels. Finally, the third line of defence comprises the audit and compliance functions, ensuring that the explanations generated by XAI models are clear, justifiable, and comprehensible to internal users and external auditors.

Embedding fairness and mitigating bias in AI systems formed another central theme of discussion. Practitioners acknowledged that AI models can inadvertently reinforce human biases, potentially leading to discriminatory outcomes. However, bias extends beyond human decision-making – model and data bias were identified as equally significant risks. Data bias, in particular, can distort analysis and produce misleading results, impacting decision-making across an organisation. To address this, the importance of model lineage was emphasised, ensuring that the origins, evolution, and underlying datasets of AI models are well-documented and auditable. The discussion reinforced the necessity of strong model governance, which serves as a safeguard against biases while promoting ethical AI practices. Ensuring fairness in AI systems requires ongoing oversight, transparent validation methods, and mechanisms to rectify biases as they arise.

In the design process, organisations need to consider the trade-off between in-house AI development and third-party vendor solutions. Large financial services firms often favour in-house development due to the complexity of their operations and the need for bespoke AI solutions tailored to their internal taxonomies. Internal development provides greater control over model customisation, compliance, and risk management. However, third-party vendors must clear a high bar to meet the rigorous standards of financial organisations *vis-à-vis* the third-party vendors' regulatory readiness.

Despite these challenges, there is potential for a hybrid approach according to the practitioner view. Standardisation across the industry could enable smoother integration of third-party solutions with in-house AI systems, fostering greater interoperability. Open-source AI tools may be a viable alternative, provided their licensing terms align with industry requirements. Open-source platforms offer opportunities for standardisation, innovation, and collaboration while maintaining a level of control and compliance. Ultimately, firms must

[27] James Bowden et al., 'Explainable AI for Financial Risk Management' (2024) FRIL White Paper Series <https://www.strath.ac.uk/media/departments/accountingfinance/fril/whitepapers/Explainable_AI_For_Financial_Risk_Management.pdf> accessed 14 March 2025.

[28] Alexey Surkov, Val Srinivas, and Jill Gregorie, 'Unleashing the Power of Machine Learning Models in Banking through Explainable Artificial Intelligence (XAI)' (*Deloitte Insights*, 17 May 2022) <https://www2.deloitte.com/us/en/insights/industry/financial-services/explainable-ai-in-banking.html> accessed 14 March 2025.

strike a balance between proprietary development and external partnerships, ensuring that AI solutions align with both operational needs and regulatory expectations.

4.3 Generative AI (GenAI) - A Step Change in AI-Based Compliance Systems

The exploration and phased implementation of GenAI within financial services organisations is ongoing, driven by advances in Large Language Models (LLMs) since the emergence of ChatGPT. Our insights from industry suggest that currently, GenAI is primarily applied in low-risk, low-materiality use cases, such as generating profit and loss commentary or assisting developers as a co-pilot. It is also increasingly used to support routine tasks within Microsoft Office, enhancing productivity and efficiency. Despite these advantages, human oversight remains crucial to ensure the reliability and credibility of AI-generated insights. Decision-makers must maintain confidence in AI outputs through continuous monitoring and validation, reinforcing the need for responsible AI governance.

From a regulatory perspective, GenAI presents opportunities to tailor regulatory frameworks to specific companies, offering more customised compliance approaches. At the same time, organisations can leverage AI to implement internal controls that align with these regulations. However, while AI can assist in interpreting complex regulatory requirements, human expertise remains essential to ensure full compliance and proper understanding of tailored regulations. The balance between AI-driven automation and human judgment will be critical in shaping the responsible adoption of GenAI in financial services.

GenAI offers significant advantages in automating compliance processes, yet its adoption presents notable challenges due to its nascent nature. We draw on the outline of GenAI capabilities and risks as set out by Zhang et al. (2025) to frame our analysis.

The benefits of GenAI in this space span multiple capabilities. From a functional perspective, GenAI enhances compliance by supporting document summarisation, enabling organisations to generate concise and insightful summaries of regulatory texts, internal policies, and legal documents. With careful prompt engineering, AI can generate alternative document summaries that vary in focus, format, and structure, tailored to different compliance needs. GenAI also provides data visualisation capabilities, allowing users to efficiently interrogate and structure compliance-related data, generating chart-based representations of numerical data and tabularising textual content for easier interpretation. This improves the integration of quantitative and qualitative information into meaningful compliance assessments. Furthermore, AI enables multiple source analytics, supporting the analysis of compliance-related requirements across an organisation or even across multiple organisations within a corporate group. Such a comparative analysis aids in identifying anomalies, inconsistencies, and risk areas, ensuring a more robust compliance framework. Additionally, GenAI supports customised report generation, where users can interactively tailor compliance reports, dictating format, structure, language, and tone to meet regulatory or internal requirements. AI systems can also be trained on past reports to maintain consistency in writing style and presentation.

Beyond these functional capabilities, GenAI offers several technical capabilities that enhance its scalability within compliance frameworks. These include response speed and agility, where system performance can be optimised based on an organisation's hardware capabilities, balancing processing speed and computational efficiency. GenAI also supports multiple version choice and algorithmic flexibility, enabling the use of domain-specific

models tailored for regulatory and compliance applications. A user-friendly interface further enhances adoption, ensuring accessibility for a wide base of compliance professionals. Additionally, scalability and upgradability allow organisations to expand AI deployment while periodically updating models to incorporate new regulatory developments, user feedback, and evolving risk factors.

Despite these advantages, GenAI also presents a set of challenges and risks, particularly in regulatory compliance settings. Data privacy is a critical issue, especially when using public GenAI models, where confidential or sensitive organisational information could be exposed. One mitigation strategy is the adoption of localised AI models, although this does not fully eliminate risks. Embedded bias is another concern, as GenAI models are trained on large-scale internet-based datasets, limiting an organisation's ability to fully control or mitigate inherent biases. This presents regulatory and legal risks, particularly if AI-generated compliance insights are used in decision-making or policy enforcement.

Another major challenge is robustness, as GenAI systems can produce hallucinations – false or misleading information – if trained on poor-quality or incomplete datasets. Ensuring AI reliability in compliance requires continuous monitoring, validation, and governance mechanisms. Additionally, explainability remains a persistent issue, as GenAI models rely on complex deep learning architectures, making it difficult to justify or audit AI-generated compliance outputs. Given increasing regulatory scrutiny around AI transparency, organisations must ensure that AI-driven compliance insights are interpretable, traceable, and justifiable. Lastly, cybersecurity risks remain an evolving concern, with potential threats including adversarial attacks, where input data is manipulated to distort AI outputs, and jailbreaking threats, which attempt to bypass ethical and regulatory safeguards. While shifting from public to private AI systems can mitigate some of these threats, organisations must remain vigilant in monitoring emerging security vulnerabilities.

While GenAI presents considerable potential in compliance by enhancing efficiency, automation, and analytical capabilities, its deployment must be carefully managed. A responsible implementation strategy should prioritise data integrity, model reliability, explainability, and regulatory alignment, ensuring that AI serves as a trusted enabler rather than a compliance risk.

4.4 Designing GenAI-Based Compliance Systems

4.4.1 Capabilities mapping across the compliance process

The effectiveness of GenAI in compliance systems is underpinned by its functional and technical capabilities, which vary across the different phases of the compliance process. Figure 2 illustrates this capability mapping. These capabilities determine the extent to which AI can support regulatory processes, ranging from strong applicability in rule identification to moderate and ultimately weaker applicability in later compliance stages. This variation reflects the evolving complexity of compliance tasks, as well as the increasing reliance on human judgement and organisational decision-making.

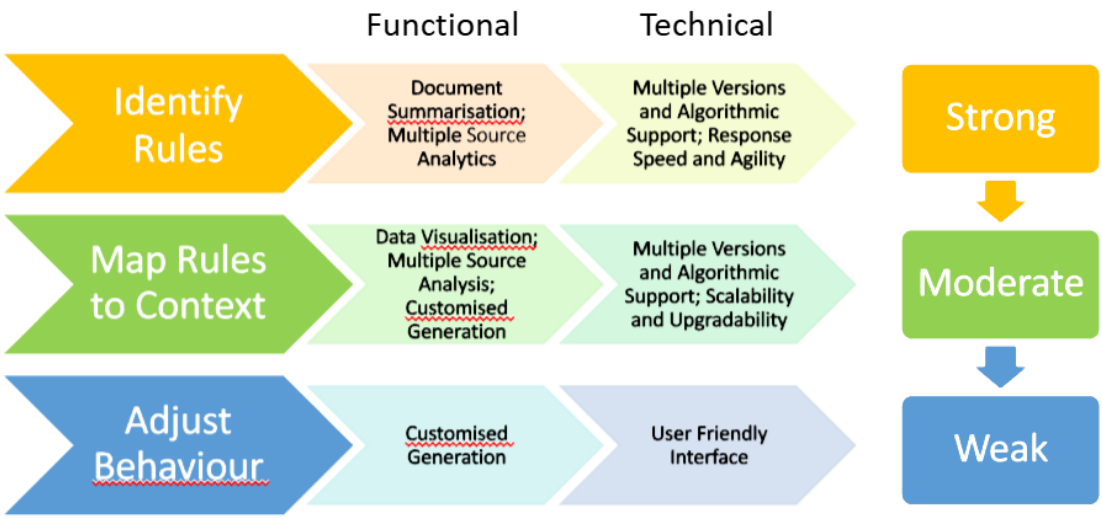

Figure 2: GenAI Capabilities Mapping across the Compliance Process

At the rule identification stage, GenAI demonstrates strong capabilities, particularly in automating regulatory intelligence processes. On the functional side, AI supports effective document summarisation and the ability to analyse multiple sources in parallel, enabling organisations to efficiently extract, analyse, and interpret complex regulatory requirements. On the technical side, GenAI offer multiple model versions and differing algorithmic supports to meet compliance professional requirements. Furthermore, response speed and agility ensure adaptability in fast-changing regulatory landscapes. This phase benefits most from AI-driven automation, as the tasks primarily involve processing structured regulatory data with minimal contextual complexity.

As the GenAI application progresses to the rule mapping stage, its capabilities become moderate, as the process demands greater contextual understanding and alignment with internal frameworks. Functionally, AI supports data visualisation, multiple source analysis and customised generation, enhancing the ability to integrate external regulatory insights with internal risk and compliance structures. From a technical standpoint, AI offers again offer multiple versions and algorithmic support from which to choose, while scalability and upgradability provide the flexibility needed to refine compliance interpretations over time. However, as this phase involves greater organisational complexity, human oversight becomes more critical, limiting the extent to which AI can operate autonomously.

By the time AI is applied in the behavioural adjustment phase, its capabilities are at their weakest, as this stage requires significant human-led decision-making. Functionally, AI contributes to customised generation, supporting policy drafting and compliance communication. However, technical capabilities in this phase are primarily limited to ensuring a user-friendly interface, reflecting the need for compliance professionals to interpret and act on AI-generated outputs. While AI can assist in structuring compliance interventions, final decisions must be made by risk and policy experts, reducing the scope for full automation.

This framework underscores the diminishing role of GenAI across the compliance process, transitioning from a highly automated tool for regulatory intelligence to a supporting mechanism for policy implementation. By leveraging AI's strengths while recognising its limitations, organisations can design compliance systems that balance automation with accountability, ensuring that AI remains

an enabler rather than a replacement for expert-driven compliance governance.

4.5 Business Considerations across the Compliance Process

The application of GenAI in compliance systems must also be guided by key business considerations to ensure its responsible and effective use. In this context, three critical factors – business risk, business materiality, and human intervention – vary across the compliance process and influence how AI should be deployed to support regulatory adherence while maintaining oversight and control. Figure 3 visualises these business considerations across the compliance process.

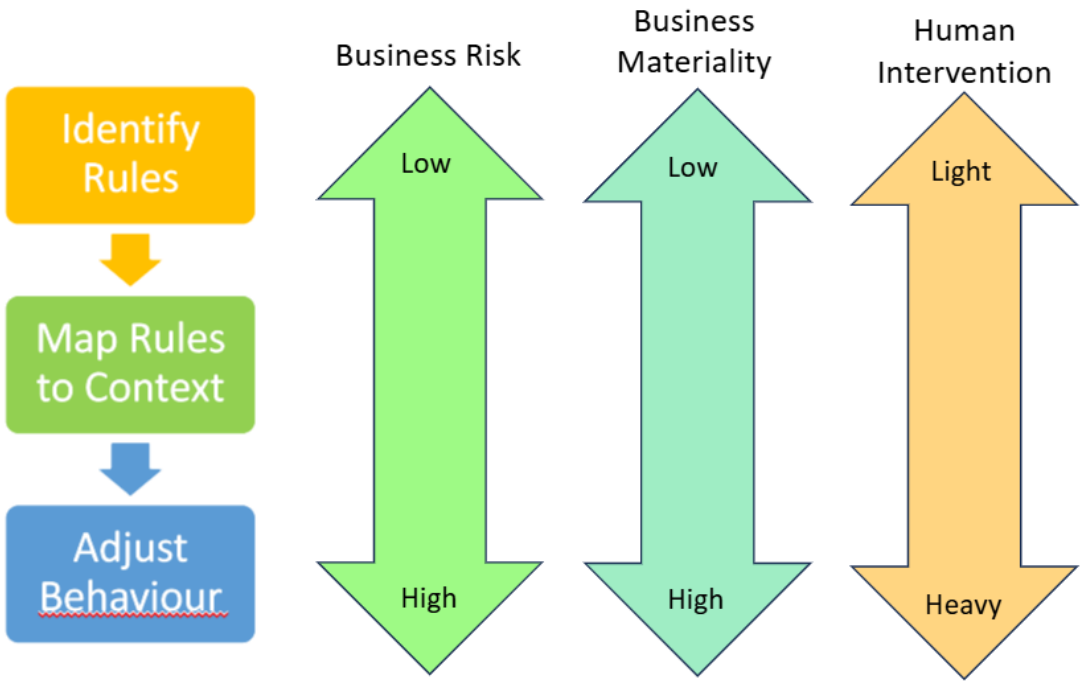

Figure 3: GenAI Business Considerations across the Compliance Process

At the rule identification stage, AI primarily extracts and analyses laws, regulations, and industry standards. Since this phase focuses on gathering publicly available regulatory information rather than making organisation-specific decisions, business risk and materiality are relatively low. As a result, human intervention is minimal, with AI able to operate autonomously in identifying and summarising compliance obligations. However, human oversight remains necessary to validate AI outputs, ensuring their accuracy and contextual reliability through the application of domain expertise.

As AI begins to map rules to organisational context, the complexity increases. Aligning external regulations with internal structures, business models, and risk frameworks introduces greater business risk and materiality, as misinterpretations at this stage can have significant consequences. Human intervention becomes more pronounced, with compliance professionals actively reviewing AI-enabled insights to ensure contextual accuracy and regulatory relevance. AI plays a crucial role in streamlining rule classification and interpretation, but human judgement remains essential to refine and validate its outputs.

When it comes to adjusting behaviours, AI-generated recommendations directly shape policy decisions, risk controls, and corrective actions. This is where business risk and materiality peak, as errors at this stage could result in regulatory breaches, financial penalties, or reputational harm. Consequently, human intervention is at its highest, ensuring AI recommendations align with risk management strategies and regulatory expectations. Compliance teams must critically assess AI-generated outputs, applying expert judgement to validate policy changes before they are implemented.

This framework highlights the need for a balanced approach to AI adoption in compliance. While AI enhances efficiency and automation, its role must be carefully managed in relation to business risk, materiality, and the required level of human oversight. By tailoring AI's involvement at each stage, organisations can harness its benefits while ensuring robust governance, transparency, and regulatory alignment.

4.6 Design Principles across the Compliance Process

To ensure responsible AI deployment, three critical design requirements – explainability, trust, and the internal/external orientation of AI applications – must be carefully managed across the compliance process phases. Figure 4 overviews these design principles across the compliance process.

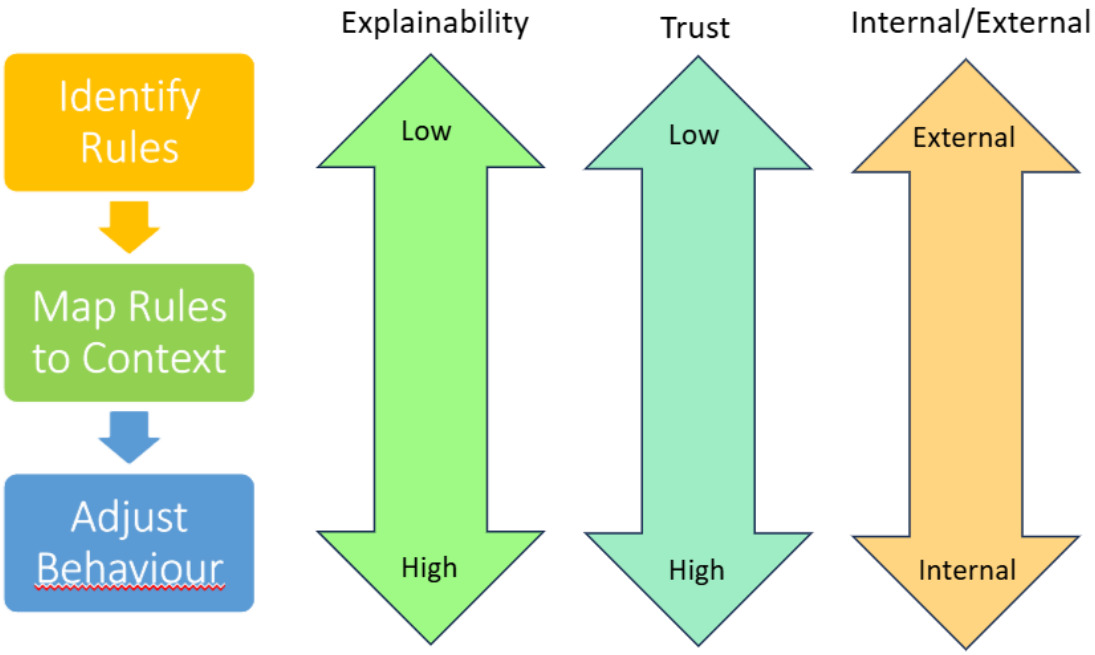

Figure 4: GenAI Design Principles across the Compliance Process

In the first phase, identifying rules, the primary focus is on gathering and interpreting external laws and regulations. Here, the system operates at the external end of the spectrum, drawing from regulatory frameworks and industry standards. Since this phase involves well-documented legal requirements, AI's role is primarily focused on retrieval and classification rather than complex decision-making. Hence, the need for explainability is relatively low – regulations are typically explicit and structured – as compared to later stages

where AI may engage in interpretative or risk-based assessments. However, trust in AI-generated outputs remains crucial, as organisations must be confident that AI is accurately identifying all relevant rules, including rule type and scope for discretion in the regulatory response.

In the second phase, mapping rules to context, the AI system must interpret regulations within the organisation's specific operational environment. This phase introduces greater complexity as compliance obligations are mapped onto internal processes, business activities, and risk profiles. Consequently, the need for explainability increases, as stakeholders require clarity on how the AI interprets and contextualises regulations. Likewise, trust becomes even more critical, as decisions made at this stage materially influence compliance strategies. The system naturally shifts toward a more internal orientation, ensuring that compliance measures align with corporate structures and workflows.

In the final phase, adjusting behaviors, AI-based recommendations inform policy definitions and corrective measures, directly influencing organisational actions. At this stage, the highest level of explainability is required, as AI-generated decisions must be transparent, auditable, and justifiable to internal and external stakeholders, in particular regulators. Trust must also be at its peak, as compliance professionals and regulators depend on these outputs to guide decision-making. The focus remains primarily internal, as compliance policies and risk mitigation strategies are implemented within the organisation. Only at a later stage can such AI-assisted decisions be translated into external communication, especially for reporting purposes to regulatory authorities.

4.7 Use Case Discussion: GenAI and Robo-Advisory Services

Having discussed the transformative nature of GenAI and its potential to advance compliance systems for financial services organisations, we take the opportunity in this section to discuss how GenAI is being deployed in the wealth management domain, with specific focus on robo-advisory services. In particular, we assess GenAI's key capabilities, the complementary role of XAI in promoting transparency and trust, and the governance challenges associated with AI integration in this domain.

4.7.1 GenAI and XAI in robo-advisory services

Robo advisory services represent one of the key areas in which GenAI is transforming data capabilities in fintech and financial services sector. Thanks to its ability to parse diverse, even unstructured data — including text, images and voice — GenAI has contributed to easier, more efficient and richer data, which enables investment advisors to personalise recommendations for clients.[29] This means that GenAI has potential to address, in significant ways, the robo-advisory practice in which simple questionnaires are used to collect data on how a potential client's financial situation, financial history, goals, risk tolerance and related behaviour might shape investment decisions. GenAI leverages diverse and Big Data sources that complement the self-reported data gathered through questionnaires. Accordingly, it enhances robo-advisory capabilities across all stages of client profiling, portfolio scanning and matching, as well as asset rebalancing to align with the evolving market conditions, and circumstances and goals of clients.

GenAI offers two key streams of data insights and business process support in this regard. In

[29] Ernst & Young highlights these capabilities in financial services. See Kostis Chlouverakis, 'How Artificial Intelligence Is Reshaping the Financial Services Industry' (*Ernst & Young*, 26 April 2024) <https://www.ey.com/en_gr/insights/financial-services/how-artificial-intelligence-is-reshaping-the-financial-services-industry> accessed 14 March 2025.

one stream, it enhances client profiling, search for investment opportunities for clients and follow on realignment needed to adjust investment and risks to changing client profiles. In another stream, it affords robo-advisers the enhanced capability to integrate existing regulations, laws and standards into the rich client-relevant data and tested business processes — including also regulation horizon scanning— that inform investment advice and recommendations. That way, GenAI provides scope for improving business processes and for reducing the risk of noncompliance in robo- advisory services.

However, GenAI typically faces the challenge of algorithmic transparency as the processes and rationales that inform data output can be unclear. This fundamental black-box problem means that recommendations that are based on GenAI might be difficult to interpret. In the context of robo-advice, this raises compliance challenges as robo-advisory service providers must ensure that clients understand what informs the investment recommendations and decisions they get. Another layer of complexity is that such recommendations, even in instances where they are clear and easy to interpret, must be based on processes and systems that are familiar with and that take into account clients' circumstances and characteristics.[30] Yet, the tendency of GenAI to hallucinate means that its data output and recommendations based on it can be misleading hence it raises the risk of recommendations and decisions that are unrelated to the characteristics and circumstances of the expected client.

In this regard, XAI complements GenAI to improve the capability to disclose and clarify the rationale behind data output.[31] This makes XAI vital to addressing problems related to accurate and reliable data and improved client understanding of automated investment recommendations, which in turn can contribute to maintaining regulatory compliance and higher social acceptance of AI systems with potential for improved business growth of robo-advisory services.[32]

4.7.2 Framing AI within robo-advisory firms and value chains

The integration of AI into investment advisory processes means that an investment services firm needs to assess its current level of technological advancement and complementary competences. This allows the firm to (re-)design its infrastructure, evolve business operations, processes and service offering/delivery in line with emerging technological opportunities in a seamless way. In light of the fast-paced technological advances—particularly those related to AI—there are three key elements to which firms need to give special considerations to keep abreast with the market and deliver value to stakeholders, including clients:

a) Appropriate AI development and deployment strategies;

[30] For example, see the 'suitability' requirement in Article 25 of the EU Markets in Financial Instruments Directive (MiFID II), which sets out investor protection obligations for financial firms. The UK has retained this requirement post-Brexit. See Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments [2014] OJ L173/349.

[31] For an analysis of how the emerging field of XAI is helping researchers and practitioners addressing the "black-box" problem of AI, see Vikas Hassija et al., 'Interpreting Black-Box Models: A Review on Explainable Artificial Intelligence' (2024) 16 *Cognitive Computation* 45 <https://link.springer.com/article/10.1007/s12559-023-10179-8> accessed 14 March 2025.

[32] For a discussion on the role of AI explainability in fostering public trust in robo-advisory and a proposed model to address this issue, see Giulia Vilone, Francesco Sovrano, and Michaël Lognoul, 'On the Explainability of Financial Robo-Advice Systems' (2024) in Luca Longo, Sebastian Lapuschkin, and Christin Seifert (eds), *Explainable Artificial Intelligence* (Springer 2024), pp. 219-242 <https://doi.org/10.1007/978-3-031-63803-9_12> accessed 14 March 2025.

b) Skills and complementary competence building.

c) AI governance framework.

a) AI development and deployment strategies in robo-advisory services

AI integration into existing capabilities of investment advisory firms may follow the incremental innovation approach where new technologies are gradually embedded in existing operational infrastructure, knowledge base, routines, practices and structures. In this case, robo-advisory capabilities evolve in an organic way from existing firm capabilities. Where internal technological capabilities are strong, but a firm is hesitant to change legacy systems, for example, in traditional investment advisers — also where the robo-advisory services provider intends to externalise the risk of developing AI solutions — a technology outsourcing model may be considered. In this regard, outsourcing can take the form of buying part or the whole of an existing robo-advisory platform, allowing the firm to migrate its existing infrastructure, data, investment products and services to the new platform, while leveraging the capabilities of robo-advisers to create new products and deliver value to clients.

There are varying conditions under which investment advisory services may deploy partnership, in-house technology development and/or technology acquisition as a strategy to leverage the evolving robo-advisory technologies, while considering the risks of each strategy. For example, while partnership with a technology firm offers the advantage of quick AI development levers without shocking a firm's legacy systems (minimal organisational changes), it carries the risk of future conflict of objectives and co-dependency. In-house technology development has the unique advantage of gradually evolving existing technologies and organisational practices with new ones, also allowing the migration of existing customer base alongside the attraction of new customers. Caution is needed in this case to avert the risk of conflicting (old/new) technologies and products, which do not essentially offer significant benefit to the firm and customers. Like partnership, acquisition can serve as a quick way to leverage the latest AI advances in robo-advice, but it does carry the burden of having to work out how to integrate new/external models and technologies with (long standing) internal technologies, processes, practices and products.[33]

Whatever the model and process that a robo-advisory services firm applies, a level of in-house capabilities is helpful. This is particularly important for understanding the underlying processes and technologies that are at the core of products and services offered to clients. In-house capabilities are helpful, even in the case of technology outsourcing, for defining solution requirements in line with, for example, the firm's business goals, customer needs, internal policies and practices.

b) Skills and complementary capabilities for evolving robo-advisory services

The continuous development and improvement of in-house expertise and technological capabilities is consistent with evolving a business model that considers consumer capabilities. Having developed relationship with customers, or if new, having designed its approach to customer support, strong in-house competences position a rob-advisory services provider for a higher chance of delivering positive customer support and experience throughout the product cycle. This is especially applicable in times of deployment

[33] See Deloitte, 'Robo-advisors: Capitalising on a Growing Opportunity' <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/strategy/us-cons-robo-advisors.pdf> accessed 14 March 2025.

of new technologies, which come with uncertainties.

Robo-advisory services firms are transitioning to new technologies and ways of organising and delivering investment services. Existing and prospective clients may be unfamiliar with the new platforms and processes, which might leave them frustrated. This poses the risks of poor consumer experience and potential harm, as well as higher risks of non-compliance. To illustrate this, FCA Principles for Business (2025) presents competence building as a matter of principle such that a firm must conduct its business with due skill, care and diligence required to offer product or provide service to customers. Relatedly, the extension of those principles to cover consumer duty shifts the regulatory focus from firms' inputs to consumer outcomes.[34] Therefore, developing AI-relevant skills and complementary competences is not only useful for efficient internal processes but also for compliance with regulatory rules and guidance.

The need to have human in the loop to complement AI systems in robo-advisory services underscores in-house capabilities building, which in turn challenges the existing configuration of skills in robo-advisory firms. Indeed, human-supported robo-advisory services tend to be the common practice at this stage. For example, robo-advisory platforms such as Moneyfarm, Etoro and Robobox are semi-autonomous systems – they use human assistance in the robo-advisory recommendations and decisions.[35] The question then arises as to the knowledge and skills that the human complements of robo-advisors should possess to provide efficient and effective support and oversight.

Competence building and reconfiguration can take different measures. For example, there is an added value if compliance officers are trained in AI essentials in the domain in which the firm uses AI solutions/robots, financial/investment advisers trained in AI and compliance essentials, sales and business strategy groups trained in AI and compliance essentials; as well as technical teams, including IT units, (re-) trained in AI, compliance and business/finance essentials.

The Bank of England and FCA's report finds that while AI is being increasingly applied in financial services (around 85%), there is the challenge of understanding of AI models and technologies among firms.[36] For example, nearly half of the respondents (46%) have only a partial understanding of AI technologies, especially when developed by a third party. This observation sends a signal to work around the challenge of internal AI knowledge and skills development to ensure that teams have the essential understanding needed to conduct internal processes, exercise controls and to provide support to clients.

c) Governance framework for AI and data practices in robo-advisory firms and value chains

Robo advice is a data-driven enterprise, and it is increasingly engaging of a network of firms, which provide specialised support in the development and/or implementation of AI systems and delivery of products and services. Integration of AI into advisory services, including the complex value chains that underpin them, therefore challenges existing IT and related technology governance in robo-advisory firms.

[34] Financial Conduct Authority, *Principles for Businesses* (March 2025) <https://www.handbook.fca.org.uk/handbook/PRIN.pdf> accessed 14 March 2025.

[35] See Domenica Barile, Giustina Secundo, and Candida Bussoli, 'Exploring Artificial Intelligence Robo-advisor in Banking Industry: A Platform Model' (2024) *Management Decision* (ahead of print) <https://doi.org/10.1108/MD-08-2023-1324> accessed 14 March 2025

[36] See Bank of England and Financial Conduct Authority, cited earlier.

• ***AI leadership and internal coordination in robo-advisory firms***

The changing data and infrastructure requirements, as well as privacy and security concerns necessitate a clear (re-)definition and (re-)development of governance frameworks, controls and check systems, including mechanisms to ensure internal team coordination and regulatory compliance.

Measures entail defining and implementing a data framework; what data, who has access, how data is used, and who oversees data transactions to ensure that data use and related practices and processes are aligned with organisational policy and strategies. This also means making provision for IT/AI leadership. The internal governance framework focuses on in-house teams such as the IT group, business, finance, administrative and compliance teams who are under the supervisory mandate of the in-house IT/AI governance executives. In addition to this, AI governance framework ensures alignment with broader regulatory requirements— for example, technology and data principles, standards and laws— which are crucial to responsible AI practices and good outcomes for stakeholders, including clients.

The UK Information Commissioner's Office and The Alan Turing Institute joint work[37] offers guidance to AI-relevant teams and senior management on why effective support for AI explanation is crucial and how to conduct it. This underscores the importance of AI essentials across teams, including data protection officers and compliance teams, IT teams and other members of staff who play a role in explaining the processes and outcomes of AI decisions to individuals/clients in practice. Senior management is expected to provide leadership to ensure that appropriate procedures and policies are laid out in the organisation to serve as a reference for various teams that are engaged in providing support to clients regarding AI processes and outcomes.

• ***Governance of AI and data value chains in robo-advisory services***

As with business models that depend heavily on AI systems, the need for a sustainable AI governance framework is crucial to the conduct of robo-advisory activities. The enormous data requirements mean that the data stored can stay longer than the creator; data can be repurposed for uses different from the original objectives (for example by a third party), and data on an individual may contain information about another individual who is not the current focus and beneficiary of the intended product/service.[38] This captures the situation in the robo-advisor value chain where technology solution developers, programmers and financial services providers collaborate and share data to create platforms, and to deliver products and services.

In addition to the consumer experience and compliance improvements that come with responsible data (privacy) governance, there is the business and economic argument for a clear delineation of the boundaries of liability in the AI value chain to solve resource commitment and coordination problems among potential business partners. Put in a robo-advisory service context, firms which are expected to play different pivotal roles in the robo-advisory value chain may be unwilling to commit resources (including monetary

[37] See Information Commissioner's Office and The Alan Turing Institute, 'Explaining Decisions Made with AI' <https://ico.org.uk/media2/3a3br1tr/explaining-decisions-made-with-artificial-intelligence-all-1-0-39.pdf> accessed 14 March 2025.

[38] See Catherine Tucker, 'Privacy, Algorithms and Artificial Intelligence' in Ajay Agrawal, Joshua Gans, and Avi Goldfarb (eds), *The Economics of Artificial Intelligence: An Agenda* (University of Chicago 2019) 423-437 <https://www.nber.org/system/files/chapters/c14011/c14011.pdf> accessed 14 March 2025.

investment)[39] to setting up and running business initiatives where the boundaries of liability and mechanisms of redress are unclear.[40] Accordingly, working around privacy and security concerns can help to address the distributed risks (perceived or actual) associated with robo-advisory services. This has potential to increase social acceptance and reduce the cost of noncompliance.

Following our contextualisation of AI/GenAI's capabilities and the governance challenges surrounding its trustworthy adoption in the robo-advisory sector, we now turn to broader issues of compliance governance within organisations. In particular, we explore how financial institutions can transition toward an 'embedded compliance' paradigm. As we will argue, this shift is essential for fostering both trustworthy AI adoption in RegTech and promoting a more holistic, functionally integrated approach to regulatory compliance.

5. From AI Governance to 'Embedded Compliance'

Our research and engagement with the FinTech Scotland community highlight the dual nature of AI, which also manifests uniquely in the RegTech domain. While AI is often touted as a revolutionary technology for regulatory compliance, its responsible and trustworthy adoption presents new techno-organisational challenges for financial institutions—particularly as they already operate within an increasingly complex compliance landscape. Indeed, digital transformation presents organisations with a multi-alignment problem. Regardless of their specific use of AI, deployers must ensure that strategy, objectives, processes, and outcomes align with the multiple layers of normative rules that apply to them (Section 2). Crucially, this task demands dealing with four key dimensions of complexity that define firms' business environments—financial, regulatory, organisational, and technological (Section 3). While AI solutions may help firms overcome some of these complexities, they also introduce distinct governance challenges. However, different AI systems possess varying capabilities and inherent techno-methodical limitations, making some more suitable than others for specific domains of use (Section 4). A key distinction, for example, exists between consumer-facing AI and back-office AI applications, each raising distinct sets of governance—and regulatory—questions.[41] Given the heterogeneity of AI methods and capabilities, AI should not be treated as a mere IT upgrade. Its adoption may, in fact, necessitate a fundamental rethinking of corporate governance—one that incorporates AI governance as a core element rather than an ancillary concern.

This shift carries significant implications for the design of AI-augmented compliance programmes, which are now called to integrate AI governance principles with the foundational

[39] Note that this illustration primarily concerns the reluctance of supply-side stakeholders—such as partner producers, suppliers, and providers— to invest in (co-)development of AI enterprises offering platforms, products, or services. This should be distinguished from the willingness of platform clients (i.e. consumers) to invest via AI-enabled platforms, such as robo-advisers, albeit liability governance instruments are also important in shaping clients' investment decisions.

[40] For a comment on how unclear liability boundaries may discourage stakeholders in the AI value chain from investing in business initiatives, see Ajay Agrawal, Joshua Gans, and Avi Goldfarb, 'Economic Policy for Artificial Intelligence' (2019) 19 *Innovation Policy and the Economy* 139 <https://doi.org/10.1086/699935> accessed 14 March 2025.

[41] See Antontella Sciarrone Alibrandi, Maddalena Rabitti, and Giulia Schneider, 'The European AI Act's Impact on Financial Markets: From Governance to Co-Regulation' (2023) European Banking Institute Working Paper Series 2023 – No. 138, pp. 17-18 <https://ssrn.com/abstract=4414559> accessed 14 March 2025.

values of broader corporate governance. Our findings indicate that organisations, particularly large and complex ones, should move beyond siloed approaches. Strengthening cross-functional collaboration is essential to aligning strategic objectives, organisational infrastructure, resources, and processes with various stakeholder expectations. In this way, compliance functions—including those governing AI applications—become embedded within and across operational workflows and the wider organisational framework. This is precisely where the concept of 'embedded compliance', as we define it, comes into play. It represents an implementation of the holistic approach to compliance that we referenced in Section 1 as being necessary to cope with a complex environment. As a prelude to elaborating that concept, we recap on some of the persistent challenges organisations face in achieving effective compliance alignment, some of which are likely to persist in the AI context.

5.1 Challenges for Compliance Alignment

Research in compliance and regulation has long identified the risks and limitations that may typically undermine compliance effectiveness. In the highly regulated and complex financial services sector, compliance misalignment takes many forms. Yet, the underlying challenge for organisations remains the same: aligning their structures and operations withal relevant legal and regulatory requirements. Ambiguities may arise when translating legal principles and regulatory obligations into business protocols, including those related to compliance. In such cases, the true spirit of the law and how it is interpreted by regulated entities risk diverging into two different 'languages'. Even within the same organisation, various departments, units, and even individuals do not often share the same level of understanding and confidence in dealing with regulatory compliance. As a result, organisations may find it hard to translate regulatory requirements into clear, actionable policies, procedures, and functional activities. These uncertainties tend to intensify as firms grow in size, diversify their product and service offerings, expand their customer base, or integrate new technologies.[42] In turn, these difficulties can weaken compliance frameworks, increasing the risk of misalignment.

A similar situation arises when compliance goals are only formally fulfilled. While formal compliance programmes are essential, they often risk becoming mere box-ticking exercises if not reinforced by managerial values and a deep-rooted compliance culture. This viewpoint aligns with the notion of the organisation as a complex ecosystem in which managerial responsibility may take on a first-order role in orchestrating direction and ensuring cohesive functioning. For compliance to be truly effective, it must be aligned with organisational objectives and strategy and embedded into decision-making processes.[43] Without this alignment, organisations may risk falling into patterns of "creative compliance"—formally meeting regulatory requirements while circumventing their truly intended purpose.[44] This risk is particularly pronounced when compliance efforts focus excessively on outcomes rather than the *means* that lead to them—i.e. the interplay between human and

[42] See Kenneth A. Bamberger, 'Technologies of Compliance: Risk and Regulation in a Digital Age' (2010) 88 *Texas Law Review* 669 <https://ssrn.com/abstract=1463727> accessed 14 March 2025.
[43] See, e.g., Christine Parker and Vibeke Lehmann Nielsen (2009). 'Corporate Compliance Systems: Could They Make Any Difference? (2009) 41(1) *Administration & Society* 3 <https://doi.org/10.1177/0095399708328869> accessed 14 March 2025; Cary Coglianese and Jennifer Nash, 'Compliance Management Systems: Do They Make a Difference?' in Benjamin van Rooij and D. Daniel Sokol (eds), *The Cambridge Handbook of Compliance* (Cambridge University Press 2021) 571-593 <https://doi.org/10.1017/9781108759458.039> accessed 14 March 2025.
[44] See, e.g., Anna Donovan, *Reconceptualising Corporate Compliance* (Bloomsbury Publishing 2021).

non-human components within business processes. Such a risk is further exacerbated whenever, for instance, AI adoption in both business and compliance functions prioritise the objective of "optimisation against the system",[45] rather than fostering a genuine commitment to the broader goals of financial regulation and its role in society. These examples demonstrate that compliance should not be solely seen as an external constraint but as an intrinsic organisational feature.

In certain cases, compliance misalignment is due to flaws in the integration of technology-related aspects of governance at the organisational level. Despite increasing investment in R&D, many organisations still struggle to effectively design, implement, and adapt technology in their compliance programmes. Integrating innovative solutions, such as those based on AI/GenAI, within pre-existing organisational settings and related digital infrastructures can be challenging. Achieving successful RegTech adoption requires IT systems, data governance, and analytics capabilities to be cohesively designed, combined, tested, and maintained as a single, unified whole. Among other things, this presupposes the availability of specialised expertise across multiple domains. Beyond these structural difficulties, organisations also contend with broader inefficiencies stemming from traditional approaches to regulatory compliance and reporting, which often fail to accommodate the techno-organisational requirements of RegTech.

To mitigate all the many possible sources of complexity—hence non-compliance risk—a shift in compliance philosophy is warranted. A positive compliance mentality involves not only acceptance of compliance obligations but also embedding compliance within core business processes. This approach is meant to foster a business culture aligned with both organisational and stakeholder expectations and ensure adaptability to regulatory change.[46] As detailed below, we envisage a paradigm shift towards what we term 'embedded compliance'—a model that integrates compliance by design into governance frameworks, business processes, and technological applications, aimed at ensuring superior compliance outcomes.

5.2 Seizing the AI Opportunity: Multi-Layered Governance and Process-Based Compliance

AI adoption does not automatically lead to positive compliance outcomes. Even after significant investments and resource deployment, situations of 'misalignment' between regulatory requirements, business objectives, operations, and technological capabilities may persist. Achieving compliance alignment requires a structured and strategic approach to AI adoption, since *ad-hoc* reliance rarely yields sustainable or reliable outcomes. This seems especially critical for AI applications employed for analytical and decision support tasks. Hence, rather than viewing AI as a standalone solution, a more prudent—and arguably more effective—approach would be to embed AI within a wider organisational strategy. To clarify, we are not suggesting that standalone AI solutions are inherently problematic. Many technology vendors excel at tailoring AI systems to the specific needs of individual companies. Our focus, however, is another: the integrated adoption of AI within organisations, especially those that identify with large and complex systems. Thus, this perspective does not exclude the role of AI vendors, but emphasises how AI interacts with internal processes, governance structures, and compliance frameworks. RegTech solutions

[45] See Jón Daníelsson, Robert Macrae, and Andreas Uthemann, 'Artificial Intelligence and Systemic Risk' (2022) 140 *Journal of Banking and Finance*, Article 106290, p. 6 <https://doi.org/10.1016/j.jbankfin.2021.106290> accessed 14 March 2025.

[46] See Saloni P. Ramakrishna, *Enterprise Compliance Risk Management: An Essential Toolkit for Banks and Financial Services* (John Wiley & Sons 2015), pp. 54-58.

should be understood as part of a broader digital transformation effort. From this perspective, AI governance becomes component of "digital corporate governance"[47]—a framework that is necessarily multi-layered, context-specific, and deeply embedded in the organisation's *ethos*. And it is exactly here that the notion of "organisational AI governance" comes in.

As Mantimaki et al. define it, AI governance refers to the "*system of rules, practices, process, and technological tools that are employed to ensure an organization's use of AI technologies aligns with the organization's strategies, objectives, and values; fulfils legal requirements; and meets principles of ethical AI followed by the organization*."[48] Framed in this way, AI governance is necessarily embedded within corporate governance, with each shaping and influencing the other as parts of a complex system. Adopting a more systematic view encourages a close examination of the synergies between the various components, including the organisation's (compliance) human capital, other resources including technological tools, rules, practices, processes, and outcomes. The interplay of these elements is ultimately responsible for regulating corporate behaviour. In this sense, AI governance cannot be divorced from broader governance frameworks. Instead, it is interwoven with corporate, information technology, and data governance, all of which significantly overlap with AI-related processes and requirements.

Given that many regulatory requirements focus as much on how companies operate as on what outputs they deliver, it follows that a significant part of the compliance obligations concern, albeit indirectly, the underlying processes that guide company behaviour. A stronger emphasis on process governance seems further supported by the need to deal with an increasingly networked financial services sector as well illustrated by the Open Banking and Open Finance paradigms. Our investigation into RegTech underscores the need to advance research and practice on organisational AI governance, particularly its interaction with regulatory compliance and its implications for BPM.

A well-established principle in compliance research is that BPM offers a structured methodology to design, document, and optimise organisational processes to achieve better compliance outcomes. When Business Process Governance (BPG) is incorporated, BPM goes beyond mere technical process improvements to ensure strategic alignment with corporate objectives, regulatory obligations, and risk management—often summarised under Compliance, Governance, and Risk (CGR).[49] In the context of AI, this combined perspective encourages organisations to re-evaluate how AI capabilities integrate into existing processes and governance structures rather than adopting standalone AI solutions in the hope of immediate transformative effects.

Adopting a CGR-integrated BPM approach entails recognising that effective AI deployment depends mostly on how organisational processes are designed and executed to accommodate AI's specific requirements. This orientation promotes thorough mapping of tasks, responsibilities, data flows, and decision points—all of which must be aligned with strategic objectives and

[48] Matti Mäntymäki et al., 'Defining Organizational AI Governance' (2022) 2 *AI and Ethics* 603 <https://doi.org/10.1007/s43681-022-00143-x> accessed 14 March 2025.

[49] See, e.g., Thomas Schäfer, Peter Fettke, and Peter Loos, 'Towards an Integration of GRC and BPM – Requirements Changes for Compliance Management Caused by Externally Induced Complexity Drivers' in Florian Daniel, Kamel Barkaoui, and Schahram Dustdar (eds), *Business Process Management Workshops* (Springer 2012), pp. 344-355 <https://doi.org/10.1007/978-3-642-28115-0_33> accessed 14 March 2025.

compliance obligations. By documenting and analysing these processes, complex organisations such as financial institutions can more accurately identify areas where AI solutions can add value. Data plays a pivotal role in this regard. From collecting and curating to analysing and reporting, compliance workflows are underpinned by a constant influx of structured and unstructured data. Properly designed processes, supported by expertly integrated information technologies (including AI), generate granular, timely, consistent, and context-rich data.[50] This, in turn, can further maximise the effectiveness of AI applications.

With the term 'embedded compliance', we refer to best practices where normative requirements are woven into organisational processes and procedures from the outset. Instead of treating compliance as a reactive, ex-post checkbox exercise, firms can embed compliance requirements *by design* through BPM and integrated or even augmented with CGR. To drive their digital transformation, firms can leverage various enablers—such as, for instance, platformisation, modularisation, outsourcing, and process automation—tailored to their specific organisational contexts. The optimal combination may differ across organisations, but the overarching goal remains the same: to ensure the strategic and operational alignment of people, processes, data, and AI within a cohesive governance framework.

Despite the opportunities above, it is important to acknowledge the challenges of this approach. Undertaking extensive organisational redesign can be resource-intensive, requiring considerable time, funding, and expertise. Organisations may find themselves restructuring core processes and eventually realise that the new design does not fully meet their needs. To mitigate such risks, for example, virtual realities—particularly 'digital twins'—enable organisations to model and simulate proposed changes prior to implementation. Although these techniques carry their own risks and limitations, they allow to virtually represent processes, data flows, and AI deployments and research their collective behaviour as complex system in a low-risk setting.[51] This additional governance layer may have a twofold effect. It may reduce uncertainty and cost while fostering more informed decision-making. As such, it may ultimately bolster the pathway toward 'embedded compliance' and sustainable AI adoption.

Some may view our proposal as at odds with the UK's growing emphasis on outcome-based regulation—exemplified by the Consumer Duty paradigm, which focuses on delivering positive consumer outcomes rather than prescribing specific inputs. In reality, the two perspectives are mutually reinforcing. Well-designed processes, reinforced by strong governance across all the mentioned layers, provide the foundation for structured and efficient organisations, ultimately ensuring more reliable outcomes—particularly when AI is involved in both business and back-office interfaces. Emerging AI regulations also emphasise the strong synergies among these factors, highlighting lifecycle and value chain governance as key principles—both inherently

[50] See further Nigel Adams et al., 'Addressing the Contemporary Challenges of Business Process Compliance' (2025) *Business & Information Systems Engineering* <https://doi.org/10.1007/s12599-025-00929-3> accessed 14 March 2025.

[51] See, e.g., Joseph J. Salvo, 'Welcome to the Complex System Age: Digital Twins in Action' in Noel Crespi, Adam T. Drobot, and Roberto Minerva (eds), *The Digital Twin* (Springer 2023) pp. 559-575 <https://doi.org/10.1007/978-3-031-21343-4_20> accessed 14 March 2025; Kalle Lyytinen et al., 'Digital Twins of Organizations: Implications for Organization Design' (2024) 13 *Journal of Organization Design* 77 <https://doi.org/10.1007/s41469-023-00151-z> accessed 14 March 2025.

process-oriented approaches.[52] While reconfiguring processes may require significant resources, this investment enables organisations to build a more resilient foundation for outcome-focused compliance. Overall, the ultimate objective for financial institutions is to truly maximise AI's transformative potential while aligning with corporate goals, consumer interest, and regulatory compliance.

6. Outlook and Challenges

Our survey of AI and RegTech suggests that there is considerable potential for AI to be deployed in the compliance process. We start our evaluation by characterising compliance as a three-stage process comprising rule identification, followed by mapping rules to the operating context, and concluding with adjusting behaviour. Rule identification encompasses both the structure and content of rules as well as the scope for discretion in the compliance response. We note that various forms of complexity are present in the operating environment and in principle represent challenges to which AI could respond. For example, the benefits of GenAI have already been noted across capabilities such as document summarisation, data visualisation, analytical insights and customised report generation (Zhang et al., 2025). Our evaluation focuses more specifically on the capabilities of AI across the three key stages of the compliance process.

At the first stage (identification of rules) we find that AI has strong capability even if human oversight remains necessary to validate AI outputs and ensure their accuracy. At the second stage (mapping rules to context) complexity increases along with business risk and materiality, and so the need for human intervention becomes more pronounced. At the third stage (adjusting behaviour) AI potentially has a more intrusive role in decision making with the result that risk and materiality peak as errors could result in regulatory breaches, financial penalties or reputational harm. Thus, critical review of AI generated outputs and recommendations would be required at this stage before they are implemented. These observations are supported by emerging practice in robo-advisory services, which are at the forefront of AI deployment in the financial sector. While AI enhances robo-advisory capabilities across all stages—from client profiling to portfolio scanning and matching—there remain challenges in terms of making investment decisions understandable to clients while also meeting regulatory requirements tailored to their individual characteristics and financial circumstances.

We conclude by proposing that the integration of AI into the compliance process should be considered in the context of an approach termed 'embedded compliance' in which close attention is paid to the integration of compliance into business processes. This will already be a familiar concept and ambition for many compliance professionals but AI and RegTech present new and evolving challenges that are likely to drive some fundamental changes in compliance practice. At this stage it is still too early to determine if AI can drive meaningful simplification in compliance as that depends as much on the complexity of regulation and the operating environment as it does on the ability of human experts to truly leverage the full capabilities of AI.

[52] This reasoning seems to be supported by UK policymakers as well. See UK Department for Science, Innovation and Technology, 'AI Management Essentials' (2024, public consultation) <https://assets.publishing.service.gov.uk/media/672a5706094e4e60c466d19f/AI_Management_Essentials_tool_Self-Assessment.pdf> assessed 14 March 2025.

About the Authors

Iain MacNeil is Professor of Commercial Law at the University of Glasgow. His teaching, research and consulting are focused on corporate governance, financial regulation and investment. He began his academic career after a decade working in financial markets. He has undertaken research and collaborated with colleagues in Australia, Canada, China, Hong Kong and the United States. Iain is a member of the editorial board of the Capital Markets Law Journal and has published widely. He has been at the forefront of the development of postgraduate taught programmes at the University of Glasgow, initiating the teaching of financial regulation and founding the LLM Corporate & Financial Law in 2009. As Head of School from 2015-2019 he piloted the introduction of a Common Law LLB and led a major expansion in staff recruitment. Beyond the University of Glasgow, Iain has several roles. He is a Trustee of the British Institute of International and Comparative Law (BIICL), Chair of the International Securities Regulation Committee of the International Law Association (ILA) and a member of the Advisory Board of the Centre for Business Research at the University of Cambridge. He is the Convenor of the Hong Kong RAE 2026 Law Panel and was Deputy Chair of the UK REF Law Panel in 2021. He has acted as Senior Adviser on several DG FISMA projects examining national compliance with EU financial sector Directives.

Email: iain.macneil@glasgow.ac.uk

Web: University profile for Iain Macneil

LinkedIn: Iain Macneil - professor of commercial law at University of Glasgow

Alessio Azzutti is a Lecturer in Law and Technology (FinTech) at the University of Glasgow, specialising in the legal and regulatory implications of AI adoption in finance. His current research focuses on AI risks (i.e. market manipulation and algorithmic collusion), AI governance, regulatory technology (RegTech), and supervisory technology (SupTech). Alessio's work is highly interdisciplinary and policy-oriented, engaging with regulators, policymakers, financial institutions, and DeFi market participants. His contributions have shaped debates on AI regulation and governance in finance, banking supervision, and regulatory compliance. Alessio is actively involved in international research networks, including the European Banking Institute (EBI), the European Law Institute (ELI), the Society for Advancement of Socio-Economics (SASE), and the International Public Policy Association (IPPA).

Email: alessio.azzutti@glasgow.ac.uk

Web: alessio azzutti (google.com)

LinkedIn: Alessio Azzutti - lecturer and researcher in Finance Law and Technology - University of Glasgow

Mark Cummins is Professor of Financial Technology at the Strathclyde Business School, University of Strathclyde, where he leads the FinTech Cluster as part of the university's Technology and Innovation Zone leadership and connection into the Glasgow City Innovation District. As part of this role, he is driving collaboration between the FinTech Cluster and the other strategic clusters identified by the University of Strathclyde, in particular the Space, Quantum and Industrial Informatics Clusters. Professor Cummins is the lead investigator at the University of Strathclyde on the newly funded (via UK Government and Glasgow City Council) Financial Regulation Innovation Lab initiative, a novel industry project under the leadership of FinTech Scotland and in collaboration with the University of Glasgow. He previously held the posts of Professor of Finance at the Dublin City University (DCU) Business School and Director of the Irish Institute of Digital Business. Professor Cummins has research interests in the following areas: financial technology (FinTech), with particular interest in Explainable AI and Generative AI; quantitative finance; energy and commodity finance; sustainable finance; model risk management. Professor Cummins has over 50 publication outputs. He has published in leading international discipline journals such as: European Journal of Operational Research; Journal of Money, Credit and Banking; Journal of Banking and Finance; Journal of Financial Markets; Journal of Empirical Finance; and International Review of Financial Analysis. Professor Cummins is co-editor of the open access Palgrave title *Disrupting Finance: Fintech and Strategy in the 21st Century*. He is also co-author of the Wiley Finance title *Handbook of Multi-Commodity Markets and Products: Structuring, Trading and Risk* Management.

Email: mark.cummins@strath.ac.uk

Web: University profile for Professor Mark Cummins

LinkedIn: Mark Cummins - Professor of Financial Technology - University of Strathclyde | linkedin

Chuks Otioma holds a PhD from Maastricht University, the Netherlands. He is part of the Financial Regulation Innovation Lab (FRIL) team at Adam Smith Business School (University of Glasgow), where he works in the theme of financial technology and responsible innovation, with focus on firm capabilities building for the development and deployment of consumer-focused products and services, and the governance of risks associated with digital business models. He has been a Researcher at UNU-MERIT, the Netherlands, where recent engagements include a project on innovation trends in Sub-Saharan Africa with focus on why and how digitalisation policies and regulations can integrate the elements of economic competitiveness, inclusive development, and green transitions. Part of his research and knowledge exchange engagements has been implemented with and through a secondment to Lund University, Sweden. Chuks has experience in the private sector, development practice and research-based policy advisory service, including roles in telecommunication industry in Nigeria, and at International Telecommunication Union (ITU), UN specialised agency for ICTs.

Email: chuks.otioma@glasgow.ac.uk

Linked-in: https://www.linkedin.com/in/chuks-otioma-42652a75/

Get in touch

FRIL@FinTechscotland.com

FinTech Scotland®

University of Glasgow

University of Strathclyde Glasgow