



Regulatory Compliance and Financial Crime Risk Management

Enabling Growth. **Managing Risk.**



Compliance Advisory, Managed Services, Assurance and Outsourcing

DCM is a specialist Regulatory Compliance and Financial Crime Risk Management Consultancy, providing Compliance Advisory, Assurance, Managed Services, and Outsourcing to regulated firms tackling complex, high-risk change.

We bring the capabilities, skills and passion of our people to manage your business operations comprehensively. DCM's business model is built around speed, flexibility, and specialism.

Renowned for our expert-led, scalable response teams, DCM supports organisations through major transformations, regulatory enforcement actions, and rapid growth phases.

We work with an international client base comprising global Banks, Fintechs, EMIs, Brokers, Payment firms and Crypto firms.

Assurance & Advisory

Managing Regulatory intervention and enforcement (s166 and VREQ) providing boards and regulators with structure, momentum and confidence. We deliver AML Health Checks, Framework validation, System Assurance, Business Wide Risk Assessments and consultation on AI deployment. Our work covers change and transformation, target operating model design, and complex advisory including Anti-Fraud, AML, Sanctions, ABC, and CTF. We also support end-2-end EMI Licencing applications, and provide consultation on evolving Regulations such as Consumer Duty, Operational Resilience, Safeguarding and CASS15 Preparedness.

Rapid Response Deployment

Immediate intervention at scale to manage Remediations, complex and High-Risk EDD, operational backlogs, Merchant Onboarding, volume spikes, and on-going alert management. Our rapid response services benefit those organisations experiencing fast growth, facing regulatory scrutiny, remediating a variety of Audit findings, or embarking on a transformation. Efficient delivery with our known and trusted teams with the right skills and cultural fit.

Specialist Services

Managed Services & Outsourcing

Specialist led onshore and offshore operational delivery across the full AML control framework and change and transformation domains. Our work includes execution of High Risk CDD/ KYC, transaction monitoring, and Target Operating Model design to maturity. We embed within existing governance structures to provide scalable and quality assured execution.

Business-wide Risk Assessment

Conducting, delivering and simplifying the BWRA. Providing validation on the existing design and execution including review of controls, inherent risks, inputs and results. Ensuring clear alignment with external factors and regulatory expectations. Delivering a robust, defensible BWRA, enhancing governance and risk oversight.

Fractional FC Expertise

Senior financial crime leadership support delivered on a structured, part time basis, including pre launch AML health checks, retained MLRO deployment and rapid mobilisation to oversee KYC, CDD and TM.

Advisory Partner

Expert support delivered on a structured, part-time basis, including pre-launch AML health checks, retained MLRO deployment and advisory on in-focus regulatory topics, for example; Failure to Prevent Fraud, Safeguarding, Operational Resilience, CASS 15 Preparedness and The Consumer Duty. Providing flexible expertise when and where it's needed.

Licensing Applications

End to end support for regulatory authorisation applications globally. Including framework design, documentation preparation, supervisory engagement and regulatory liaison. Guidance throughout the application lifecycle to navigate regulatory expectations and achieve successful authorisations.

Assurance Reviews & Audits

Independent financial crime and regulatory health checks, 2nd Line QA, audits and control effectiveness reviews across AML, sanctions, fraud and transaction monitoring. Including framework enhancement, tuning & optimisation assessments, and remediation support, with actionable insights for executive and board oversight.

Sanctions Advisory

Specialist Sanctions Advisory services including Sanctions risk event management, applicability assessments, risk assessments and remediation to ensure compliance in complex cross border environments. Practical advice to strengthen sanctions controls and support effective regulatory compliance.

Rapid Response Deployment

Structured, time critical team mobilisation to stabilise control environments, address remediation requirements and respond decisively to regulatory or operational pressure.

AI Preparedness

Assessment and governance support to ensure emerging AI and automation tools within financial crime environments are controlled, transparent, and defensible under regulatory scrutiny, enabling organisations to innovate with confidence while meeting evolving regulatory expectations.

System Calibration

Independent review and optimisation of transaction monitoring and screening systems, including parameter tuning, threshold validation and structured effectiveness assessment. Enhancing detection effectiveness and regulatory confidence.

As firms look to emerging technologies to support growth, manage costs and strengthen control, how must the compliance function evolve?

Across the AFB membership there are firms of all shapes and sizes. Some are global operators with large UK teams. Others are smaller, more specialist institutions with lean departments aligned to the scale of their business. The future of the compliance function will look different in each organisation. What is common to all is that compliance functions will need to help firms assess, implement and govern emerging technologies in a way that supports business objectives while maintaining effective control.

Compliance will need to become the function that helps firms understand, explain and trust emerging technology.

The use-cases for emerging technologies across firms are vast. AI is moving into onboarding, monitoring, financial crime controls, customer interaction, risk assessment, reporting, operations and management information. The question is no longer whether banks will use artificial intelligence, intelligent automation or agentic systems, because they already are. The question is whether firms can make informed decisions about where these technologies fit, how much reliance should be placed on them, and how they should be monitored once embedded.

There is no one right answer. Different firms will move at different speeds. Some will be comfortable with more automated or agentic models in defined areas. Others will prefer human in the loop arrangements for longer, particularly where decisions affect customers, financial crime outcomes, regulatory reporting or senior management accountability.

This reflects the reality of banking. Firms have different business models, cross-border regulatory obligations, risk appetites, group arrangements, technology dependencies and levels of operational maturity. A tool that is suitable for one organisation may not be suitable for another. The important point is that those choices should be conscious, evidenced and capable of being explained.

This is where compliance has a central role to play. Not as the owner of technology strategy. Not as a blocker of innovation. But as an informed participant in assessing suitability, risk, control and ongoing assurance.

The starting point should not be the technology itself. It should be the needs of the business. Some firms may be trying to improve speed. Others may be looking for consistency across fragmented processes. Some may want stronger management information. Others may need to increase monitoring capacity without materially increasing headcount. In each case, the technology question should follow the business question.

Where emerging technology is well matched to a genuine business or control need, the upside can be significant. Intelligent tools can help teams review more information, identify risk patterns earlier, compare documents more quickly and summarise regulatory developments. In fragmented processes, technology can strengthen governance reporting and improve consistency of oversight. For firms operating with leaner teams, this can create real productivity gains and help focus attention on the risks that matter most. It can allow a smaller function to operate with greater impact without pretending that technology replaces judgement.

This upside will only matter if the firm understands what it is relying on, what risks are being introduced and how those risks will be managed. Compliance teams, and the scope of their responsibilities, will need to adapt to meet that demand

Continue Reading...



A tool that digests regulatory publications is not the same as a tool that recommends changes to customer risk scoring. A system that prepares committee packs is not the same as a system that prioritises monitoring alerts. A workflow assistant is not the same as an agentic control mechanism. Treating all emerging technology as the same will either slow down useful adoption or understate the governance needed for higher risk use cases.

A more useful distinction is between support, influence and action. Some technologies support human work by gathering, summarising or organising information. Some influence decisions by recommending outcomes, prioritising cases or identifying exceptions. Others may begin to take action by initiating workflows, escalating issues or adapting processes based on context. Each category requires a different level of oversight.



That is where Board risk appetite becomes important. Some Boards may be comfortable with greater automation where the use case is narrow, the controls are clear and the outputs are tested. Others may want human review preserved across a wider set of activities. Some may be willing to experiment internally before moving into customer lifecycle processes or core financial crime controls. For firms operating in the UK as part of a larger group, local strategy may also be affected by group priorities, with UK-specific use cases shaped by wider considerations.

We have reached a transitional stage in the adoption lifecycle, with different risks and rewards attached to different approaches. It will ultimately fall to compliance leadership teams to help firms understand how to respond.

This includes understanding the difference between agentic AI, human in the loop tools and machine learning decision engines. Full agentic models may offer greater operational leverage, but they require stronger confidence in system behaviour, auditability, escalation, resilience and accountability. Human in the loop models may feel safer, but they are not risk free. If human review becomes passive, rushed or overly dependent on system output, the control may be weaker than the governance model suggests. Machine learning is often the starting point, with a decision-making engine applying outcomes based on learned inputs and set criteria. However, where learning is continuous, firms will need to understand how feedback is being incorporated and how parameters are being controlled.

These risks are not insignificant nor are they insurmountable. The challenge will be demonstrating meaningful control over outcomes.

For compliance functions, this is a critical area of future focus. It will not be enough to ask whether a tool works at implementation. Firms will need to understand how it continues to operate once embedded, including how it responds to changes in data, user behaviour, business volumes and vendor updates. Workarounds may emerge. AI hallucination is a real risk. As with any system that becomes familiar, reliance can grow gradually as trust builds. A tool that was originally used to support judgement may, over time, become the judgement in practice.

[Continue Reading...](#)

Effective monitoring and governance will determine whether adoption succeeds or creates unmanaged exposure. Regulators will expect firms to explain what the technology is doing, what decisions or processes it affects, what data it relies on and how its outputs are tested. Firms will also need to demonstrate who is accountable for monitoring performance, challenging outcomes and escalating concerns.

This is particularly important for UK operations of international groups. Local teams may rely on group systems, shared services, overseas technology infrastructure or vendor arrangements agreed elsewhere. As with other systems used today, this can be efficient and appropriate, but it does not remove the need for local understanding. Where technology influences local regulated activity or control outcomes, firms need to be able to explain why they are comfortable with it and how they maintain effective control.

This does not mean duplicating group governance or creating unnecessary friction. It means understanding where group arrangements are sufficient, where local overlays are needed and where clearer evidence of oversight is required.

Rather than assessing each tool in isolation, firms should develop a cohesive view of where emerging technology is already being used, where it is likely to be used next, what problems it is intended to solve and what level of reliance is being placed on it. This broader view allows firms to identify where technology can safely create leverage, where adoption should be limited and where governance needs to mature before further deployment.

A firm with no clear approach to emerging technology will struggle to move confidently. Each proposal becomes a bespoke debate. Each risk feels new. Each approval depends too heavily on individual judgement. That slows adoption and creates inconsistency.

By contrast, a firm with a clear assessment approach can move with greater confidence. Objective criteria can distinguish between low-risk support tools and higher risk decision influencing systems. Board and management risk appetite can inform where human review remains necessary. Operational and regulatory risk assessments can explain why one use case is acceptable while another requires more caution. A clear strategy can help firms engage Boards, group functions, senior management and regulators from a position of clarity.

Compliance can provide the structure needed to adopt increasingly complex technology. Not simply to use technology. Not simply to approve it. But to facilitate better choices about how technology should be assessed, governed, monitored and trusted.

The firms that benefit most from emerging technology may not be those that adopt the most. They may be those that best understand where technology meets the needs of the business, where it creates manageable risk and where human judgement remains essential. With growing regulatory interest in how firms are using emerging technologies, the real test will be whether testing, monitoring and governance arrangements prove to be effective controls when things go wrong.

The next iteration of compliance will be as a partner across the business, helping to define what to use, what to challenge, what to govern and, crucially, what to trust as firms adopt emerging technology to drive growth asymmetrically to cost.



Written by Managing Director,

Arthur Jiggins-Roffey

arthur.jiggins@dcmoperations.com

+44 (0) 7424 720924

Discover more insights online at
www.dcmoperations.com



FinCrime Unwrapped BRIEFINGS

info@dcmoperations.com

+44 20 3882 9626

www.dcmoperations.com



DCM