Clifford Chance

April 2026

Thought leadership

AI, cyber and ESG: where financial services risk is heading

AI, cyber and ESG: where financial services risk is heading

Key takeaways

1. As financial services firms rapidly scale the use of AI and the global regulatory rulebook for AI evolves, firms are strengthening AI governance and third-party controls to manage legal, financial and reputational risk.
2. Cyber security is a board-level legal and disclosure issue, as AI-enabled attacks, shorter reporting timelines and growing litigation reshape expectations of what "reasonable" controls look like.
3. Global ESG regimes are fragmenting as tougher and more detailed EU rules collide with US regulatory retreat, creating uncertainty for firms operating across borders.

As financial institutions face another year of regulatory, technological and geopolitical change, we explore three of the key areas that boards need to focus on now: AI, cyber and ESG. How is AI being implemented and what are the emerging legal and operational risks? Are organisations fully prepared for cyber threats, and how do they respond to cross-border incidents? How do firms navigate political divergence, shifting regulation and growing litigation around ESG issues?

Financial services and the rapid adoption of AI

The financial services sector is at the front of AI adoption, with many firms embedding AI tools into core workflows and across operations, customer engagement, compliance and risk management – although adoption varies significantly, with clear differences between larger institutions and smaller players and across different parts of the sector. More established use cases include financial crime and fraud prevention and credit decisioning, and growing use cases include cyber security, particularly anomaly detection. "The business case for AI use is not always efficiency, it can be things like consistency in decision-making or stronger risk controls through earlier detection of anomalies and issues," says Rita Flakoll, a Knowledge Director in Clifford Chance's Global Tech Group.

The use of agentic AI in customer service operations and back-office functions such as compliance and Know Your Customer (KYC) processes is growing. "Going forward, we are likely to see an increase in the use of multi-agent workflows, where networks of specialised agents work together on complex tasks. In onboarding, for example, agents may extract KYC data points, remediate missing information, summarise cases and produce first drafts of communications, with human oversight," says Flakoll. "Use cases that combine AI with distributed ledger technology (DLT) are also starting to develop," she continues. "We co-authored a report on this last year with Deutsche Bank looking at use cases such as AI-powered blockchain oracles and identity-enabled AI using blockchain wallets." Digital ID is another emerging area, with potential implications for AI use cases across identity, commerce and payments.

What are the legal risks around AI?

AI exposes financial institutions to a range of legal, financial and reputational risks. One key area is operational vulnerability, particularly where system compromise or failures are difficult to detect or where firms struggle to revert to alternative processes or suppliers. Dependency on AI systems also raises questions around accountability, especially where autonomous or agentic systems are making decisions.

There are risks around privileged or sensitive material, personal data and IP, and firms are having to revisit how they protect and govern that information. Careful vendor selection, appropriate contractual terms, data protection impact assessments and clear internal policies around AI use are among the controls that can help to manage the risk of AI tools transferring or using data in a way that compromises confidentiality or undermines privacy, IP and other rights and protections. Regulatory and compliance exposure is rising too, with new legal obligations coming into force and a broad set of regulators – from financial and securities bodies to consumer, data and antitrust authorities – all scrutinising AI use. Requirements cut across conduct, consumer duty, operational resilience, outsourcing, market abuse controls, data protection and model risk management, meaning that firms need documented governance and oversight, model testing and third-party contractual protections (for example, in relation to audit rights, incident cooperation, compliance with laws and restrictions on reuse of firm data) when deploying at scale.

"The good news is that financial services firms have a strong base to build from, given their long experience with quantitative modelling, algorithmic decision making and embedded model risk management frameworks," says Flakoll. "But AI systems are more complex, more interconnected and updated more frequently than earlier models. They are usually reliant on external suppliers and they are being used across a much broader range of products and services than before. These factors, together with evolving requirements on areas such as transparency, explainability and bias, mean that firms will need to carefully consider how they are managing those risks," she says.

"New AI-specific requirements are being layered on top of existing, wider AI-relevant laws. In some cases, there is uncertainty about how and when some of these will apply."

Rita Flakoll
Knowledge Director, London

Increasing AI regulation

Firms are dealing with a growing and increasingly complex set of AI rules. "New AI-specific requirements are being layered on top of existing, wider AI-relevant laws. In some cases, there is uncertainty about how and when some of these will apply," says Flakoll.

The US has a patchwork of regulation, especially at state level. California, Texas and Colorado, for example, have AI laws scheduled to come into effect this year. "Colorado's AI Act is one to watch because it deals with algorithmic discrimination and affects areas such as employment, lending and insurance, although its implementation has already been pushed back to June and could still shift," she says. At the federal level, lawmakers have introduced a broad law that addresses many key AI policy issues such as harm to children and intellectual property protection.

President Trump has also recently issued a National Policy Framework for Artificial Intelligence, urging Congress to adopt a law that protects against certain potential AI harms while also stressing the importance of promoting innovation, including reiterating the president's desire to pre-empt state laws that impose cumbersome requirements.

APAC continues to be active too. For example, South Korea and Vietnam have introduced new AI laws this year and China's already sophisticated AI regulatory framework may further develop following a recent announcement that legislative research on AI law is a priority for 2026. Singapore and other countries also have more AI guidance in the pipeline.

In Europe, the focus is on the AI Act. A further key tranche of the Act's requirements is currently scheduled to start applying from August 2026, including rules for high-risk AI systems. These can apply, for example, to AI systems used for evaluating creditworthiness, for life and health insurance risk assessment and pricing and certain recruitment and HR activities. However, it is unclear whether these obligations will enter into force as scheduled: the EU's Digital Omnibus package of proposals includes a delay to applicability of the high-risk AI rules, but the proposals remain subject to the trilogue legislative process, which can be lengthy. "Many firms have decided to press on with the work needed to comply with high-risk AI rules and wider risk management expectations. We are helping clients work through these and, more widely, how to deal with this fast-moving landscape – especially for operations across borders – including what a holistic approach looks like," Flakoll says.

AI and its impact on cyber security

Developments in artificial intelligence mean cyber security is at an inflection point, with the technology shaping up to have both offensive and defensive applications. "Financial institutions need to look at their response, and also at what types of attacks can be carried out against them," says Megan Gordon, a Partner in Clifford Chance's global Data Risk team, based in Washington DC. "AI has unfortunately brought down the cost and how smart you need to be to carry out a cyber-attack."

On the one hand, AI advancements mean more cyber risk. For example, criminals can now employ AI- engineered deepfake videos that impersonate CEOs or other senior managers to convince employees to make unauthorised wire transfers. "When it comes to wire instructions for financial institutions or changing wire instructions for suppliers, companies need to rethink how their authentication processes for those types of payments work," says Gordon. AI coding assistants may also be weaponised, making it easier to deploy ransomware.

On the other hand, AI is also a tool organisations can use to enhance their cyber security, for instance, to identify threats more quickly. Indeed, it may soon become a tool that organisations cannot afford to ignore as expectations of what reasonable cyber security controls look like rapidly change. "This is something that's not only going to be coming up in terms of enforcement actions, but also private litigation cases over the next year," says Gordon. "Expect disputes over whether controls are reasonable in light of known AI-enabled tactics. Verification procedures, identity controls, approval workflows – all those things need to be re-examined in light of AI."

Rising expectations around disclosure

The US is moving towards faster and more formalised cyber disclosure and reporting expectations driven by a combination of SEC rules and action by state attorneys general. Contractual requirements are also pushing in the same direction. "In the US in particular, and really all over the world, we see cyber security disclosure requirements in contracts saying, 'you will disclose promptly' or 'you will disclose immediately'," says Gordon. "What is considered reasonable or prompt has really changed. You need to move faster and more formally. The amount of time you have to identify materiality and carry out notification analysis has shrunk."

Regulators are increasingly examining whether incident disclosures and public statements are consistent, as well as whether companies are meeting – or have everything in place to meet – their contractual obligations.

Deploying AI tools should go some way towards helping organisations shorten reporting timelines, but changing expectations may still present difficulties. "There's going to be an increased tension between speed and accuracy," says Gordon. "Careful handling of preliminary facts and evolving assessment is really critical."

"There is an increasing issue in cyber security where there's a one-to-many impact. You see a ripple effect."

Megan Gordon
Partner
Washington DC

The ripple effects of third-party cyber risk

Many cyber incidents stem from widely used vendors, be they managed service providers, cloud providers, identity providers, data processors or software providers. "There is an increasing issue in cyber security where there's a one-to-many impact," says Gordon. "One service provider is hit and it then hits a lot of different financial institutions and a lot of different companies. You see this ripple effect." An example of this occurred in November 2025, when an attack on a key technology provider for the US mortgage market had knock-on impacts on several lenders.

As a result, contracts with vendors are coming under renewed scrutiny, and companies are adopting a greater focus on vendor diligence. While third-party risk is nothing new in the world of cyber security, Gordon expects it to loom larger in 2026. "Expect more contract or tort claims on this, and, following widespread vendor incidents, you can also expect a lot of disputes about indemnities, limitations on liabilities and insurance coverage," she says.

When cyber claims become a legal risk

Private litigation regarding cyber security is here to stay and is particularly active in the US. "Litigation has always been about what is in the disclosure and what companies say they are doing, but now there's also going to be things tied to AI: how companies are using AI, whether or not they're using personal data with respect to AI, and how they're using it with respect to their cyber security controls," says Gordon. "A lot of companies are very excited that they are now able to say they are using AI as part of their cyber security controls. But how they're doing that and what type of information is in their public statements can also lead to litigation on the back end if there is a cyber security incident."

National security legislation is also feeding into litigation, especially in the US. "We are now seeing compliance with national security laws become an issue for private litigation," says Gordon. "If you aren't complying with those controls, it could also have a cyber security or privacy impact on customers."

These developments underscore the need for organisations to keep response plans up to date and preserve a clear and defensible record of their decision-making, escalation processes and remediation efforts. It's also important to have legal, communications and risk functions coordinate tightly on anything that might later be scrutinised by regulators, insurers and plaintiff attorneys. "Take a look at your public disclosures," says Gordon. "If you were in court, how would you defend those? How would you say, 'yes, we are actually doing that'? Is there any puffery, or statements that maybe aren't as defensible?"

ESG risks for financial services – SFDR 2.0

In terms of European ESG regulation, the biggest development is the radical overhaul of the EU's Sustainable Finance Disclosure Regulation (SFDR), which first came into force in 2021 and applies sustainability disclosure and reporting requirements to financial products managed and marketed throughout the EEA.

The regulation has been criticised for being overly burdensome, for creating additional expense and for being too complex for investors to understand. The European Commission's proposal for SFDR 2.0 seeks to address this through several substantive changes, the most significant of which is the proposal to move away entirely from a disclosure-based regime to a system of three categories for sustainability-related financial products – a transition category, an ESG basics category and a sustainable investment category. Each category will come with exclusions on the types of investments permitted for products, as well as threshold requirements for the number of investments of a particular type needed to qualify for the respective labels.

"The proposals raise a lot of practical questions for the industry. Manufacturers of financial products and fund managers will need to think about what categories they want their funds to fit into and which labels, if any, they wish to use," says Paul Ellison, a Clifford Chance Partner, based in London. While some closed-end funds may be grandfathered into the new framework, a significant number of existing financial products will be in scope, necessitating 'mid-flight' adjustments, whereby they are mapped against the new criteria and any gaps are closed.

"There is still a whole European parliamentary legislative process to go through before these proposals become formal law. But on current proposals, it's expected a significant portion of products disclosing under Article Eight at the moment may not be able to meet the requirements for a category without making fundamental changes to their investment strategy," says Ellison.

"We could end up in a very strange situation where products have been marketed to existing investors on the basis of ESG credentials under Article 8, with disclosures prepared on that basis and the expectation for investors of receiving corresponding ongoing ESG reporting under SFDR, but with new investors being admitted to the same product on the basis of restricted sustainability-related disclosures. That's going to create some real mismatches for investor relations and reporting teams at a practical level," he says.

"We're not seeing a direct US equivalent of SFDR on the statute books or in the minds of the current US administration."

Paul Ellison
Partner
London

Regulatory retreat on ESG in the US

Across the Atlantic, the story of the second Trump administration thus far has been a mass reversal on ESG-related regulation. Last year saw the US's withdrawal from the Paris Agreement, cuts to green energy project funding, suspended leases for offshore wind projects and the termination of DEI mandates, among other things. The US Environmental Protection Agency (EPA) rescinded its Greenhouse Gas Endangerment Finding in February, with the unpicking of ESG regulation looking set to continue through 2026.

In addition, the Securities and Exchange Commission (SEC) has also withdrawn multiple ESG rule proposals from the prior administration. "We're not seeing, if you like, a direct US equivalent of SFDR or in the UK SDR on the statute books or in the minds of the US at least under the current administration," says Ellison. "We've also seen guidance on shareholder proposals which will make it easier for companies to exclude ESG-related proposals." The SEC has also moved to narrow the scope for actions against firms on the basis of ESG considerations – for example, greenwashing.

The low likelihood of the US aligning with international ESG reporting regimes any time soon, as well as the potential for sharp divergences between successive administrations, gives rise to investment risk. Even within the US, Ellison describes the landscape as "nuanced." Litigation activism both in support of and in opposition to state attempts to roll out ESG regulation is ongoing. "This isn't mono-directional – there's the federal position, there's the SEC position, but then there are states which are looking to do their own thing and bring their own enforcement action," Ellison says.

"All statements and marketing – especially the labelling and naming of the funds and any other products like bonds – need to be reviewed by the legal department."

Sunny Kapoor
Counsel,
Frankfurt

European greenwashing legislative developments

Greenwashing – products or services falsely promoted as being green or environmentally friendly – is under the spotlight in the EU. Last year, an asset manager was fined a multi-million-dollar sum following a greenwashing probe that spanned several years and multiple jurisdictions, underscoring the importance of compliance with ESG regulations. "It's not just a nice to have, it's a really serious issue," says Counsel Sunny Kapoor, a member of Clifford Chance's German and European Banking and Finance Litigation Group, based in Frankfurt.

The key development in this area is the EU's Empowering Consumers Directive – part of the European Green Deal – which Member States were required to transpose into national law by the end of March 2026, with the provisions coming into force from September. The directive is aimed at combating greenwashing towards consumers and sets out specific and detailed rules about what companies are allowed to do in terms of labelling or advertising their products, with non-compliance potentially leading to civil law claims or fines.

"This not only applies to the producing industry; it also applies to financial institutions and banks," says Kapoor. "All statements and marketing, and especially the labelling of the funds and the naming of the funds and any other products like bonds, need to be reviewed by the legal department and compared with the new provisions. It's not only a challenge for the marketing department, but also a real challenge for the legal department."

Contacts

London

Simon Crown
Partner

simon.crown
@cliffordchance.com
+44 207006 2944

Paul Ellison
Partner

paul.ellison
@cliffordchance.com
+44 207006 3207

Rita Flakoll
Knowledge Director

rita.flakoll
@cliffordchance.com
+44 207006 1826

Washington DC

Megan Gordon
Partner

megan.gordon
@cliffordchance.com
+1 202 912 5021

Frankfurt

Sunny Kapoor
Counsel

sunny.kapoor
@cliffordchance.com
+49 69 7199 1438

Singapore

Lena Ng
Partner

lena.ng
@cliffordchance.com
+65 6410 2215