Baker McKenzie.

Regulatory Risk Management Risk Radar

Investment Banks | March 2025

Regulatory Risk Management

Overview of trends and recent developments

Cyber risk is one of the top issues for financial institutions. The sector is one of the most heavily targeted for cyber-attacks with this risk bound up with the need for third- and fourth-party due diligence.

- Operational risk and the need for increased resilience have become top priorities for financial institutions in recent years. This is due to increasing levels of digitalization, regulatory scrutiny, and stronger focus on environmental, social and governance factors. Moreover, regulators have been markedly less tolerant of both financial and conduct risk and the impact that they can have on financial markets and participants generally and, in the retail sphere, over the potential for consumer detriment.
- The digitization and sustainability megatrends are shaping the future regulatory environment in which financial institutions operate — the former by increasing regulators' expectations around the need for resilient systems and controls in the face of new operational and technological risk; the latter around a whole series of new obligations concerning reporting and disclosure. In both cases, institutions are exposed to significant enforcement and litigation risk.
- Following challenging periods in the economic cycle enforcement and compliance activity often increases. Stressed market conditions and recent laxer controls around remote working has likely facilitated a variety of forms of misconduct. This means it's more important than ever to maintain a focus on a business's control environment to mitigate the risks.
- Third-party service providers such as cloud services are fast becoming part of the financial infrastructure, but they present challenges in terms of systemic risk, data protection, secrecy, outages, security issues with cyberattack and concentration risk. The risks are further raised as they are often unregulated and based in third countries. Critical third parties are being added to the regulatory community.
- Most recently, there has been significant growth in the breadth and complexity of trade and financial sanctions. Banks must therefore be vigilant about identifying these risks by having the right systems, internal controls, transaction monitoring and testing in place to effectively screen transactions involving clients or their counterparties and implicating economic embargoes, designated persons or asset freezes. Internationally, the authorities increasing their cooperation and focus on compliance and enforcement.

Regulatory Risk Management

Summary of risks index

IT Disruption and Information Security

(Page 4)

- Cybersecurity
- Data privacy and protection
- Technology change risk

Talent Risk

(Page 5)

- Technology and talent management
- Inclusive workplaces
- Virtual workforces

Theft, Fraud and Conduct Risk

(Page 6)

- When the tide goes out
- Fraud and financial crime
- Conduct risk

Climate Risk

(Page 10)

- Physical and transition risks
- Greenwashing
- Data quality

Third-party Risk

(Page 9)

- Cloud computing
- Partnerships
- Operational risk

Geopolitical Risk

(Page 8)

- Operational and reputational harm
- International commerce / sanctions
- Taxation

Regulatory and Resilience Risk

(Page 7)

- Increasing levels of enforcement
- Operational resilience
- Increasing managerial responsibility

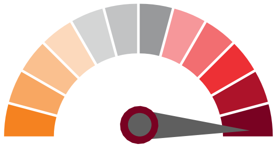
IT Disruption and Information Security

Risk Profile

Recent Trends and Developments

- The danger of IT disruption is consistently top of mind among risk managers due to the potential for outages and threats from different sources. The potential misuse of artificial intelligence (AI) to launch cyberattacks has only further heightened concerns.
- The risk of IT disruption has risen due to hybrid working arrangements that allow for multiple entry points for bad actors. In addition, emerging threats such as quantum computing could decode the current cryptography protecting data and other assets.
- Cybersecurity is also consistently identified as one of the main risks which is perceived to have grown in view of recent high-profile attacks — thereby accentuating vulnerabilities in systems and processes. Data privacy and cybersecurity issues are top concerns especially among financial institutions.

Risk Rating: **Very High**



Associated Risks

Cybersecurity

The average cost of a data breach in the financial industry is close to USD 6 million (statista). Digitization provides a fertile environment for cyberattacks, a risk ranked by many financial institutions and regulators as pre-eminent. There is growing complexity in legislation and regulation worldwide that is more challenging to manage. Reporting obligations are getting stricter. Again, there are recent and numerous examples of cyber incidents on market participants that are not themselves large, but which have a large-scale ripple effect. In a wider context, the financial sector has been the target of one in four such attacks in recent years. Many breaches would have been prevented but for better cyber-hygiene, for example failing to properly carry out risk assessments or say, deploy patches in a timely manner.

Data privacy and protection

Banks are increasingly data-centered businesses. The way in which businesses collect, use, share, store and disclose data is heavily regulated in many countries around the world. Yet data privacy and security regulation is still very much a moving target with many countries introducing comprehensive regulation for the first time and other countries with established regimes overhauling them to reflect the reality of the digital world and the growing use of AI. Financial institutions must reconcile their obligations under e.g., the EU GDPR or Californian CCPA with other sector specific regulations or face large fines.

Technology change risk

Technology in financial services is no longer limited to fintechs. Its adoption is a vital aspect of every bank's business model in responding to disruptive competitors, meeting higher customer expectations and reducing costs. A further driver is uptake of AI based solutions. Inevitably, installing new IT brings new opportunities, but also risks. Given the intensity of technology changes being put through at a fast pace with stretched resources, the usual risks may be heightened, especially where there are new technologies. Operational risk managers must design and put in place effective systems and controls to identify, manage and monitor them — during and after change.

Baker McKenzie Solutions — Key issues we advise on

- Data privacy and IT security compliance
- Technology transfers
- IP and technology auditing and due diligence
- AI, blockchain and related technologies
- Copyright, trade secret and patent protection
- Brand management
- Brand enforcement & disputes
- Data monetization
- Investigations into IT outages
- Cyber incident risk mitigation and response
- Advisory on policies, cybersecurity, e-business models and processes
- Application of regulatory and compliance obligations to new delivery channels and service offerings

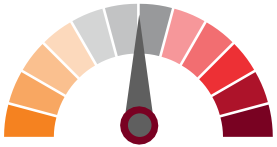
Talent Risk

Risk Profile

Recent Trends and Developments

- Financial institutions are being challenged on several fronts — from attraction to retention. Talent demand is a cost driver as firms compete for top talent.
- Business change impacts staff needs. The fast pace of change in the regulatory landscape specifically related to technology and ESG can create talent shortages, specifically those required for specialized roles and functions.
- Firms also note that there are not enough skilled employees to fill vacancies in certain critical functions such as those in first-line risk controls. Staff shortages may lead to some employers hiring less experienced staff or not being able to fill vacancies creating the potential for costly errors and oversights. Training and learning & development programs for bank employees are more important than ever.

Risk Rating: **Moderate**



Associated Risks

Technology and talent management

The impact of digital transformation means that banks must ensure that their workforce adapts to the new market environment re-skilling existing employees and recruiting new talent to boost innovation and productivity. Existing staff must adapt and upskill to acquire digital skills and work with new technologies or see themselves become redundant. In recruiting more digitally and IT trained staff, banks must compete against a range of businesses, including technology companies and fintechs to secure and keep the best talent. Global organizations are reviewing their reliance on non-compete clauses in some markets, especially the US, but may wish to develop a cohesive global approach.

Inclusive workplaces

Businesses of all types should ensure that all employees are treated equally and protected from bullying and discrimination. Whistleblowing processes should be effective, and employers have a duty to address their employees' well-being, health and safety. Banks and their senior managers may be held responsible for cultures that tolerate serious personal misconduct, bullying, racism or discrimination. In the US, executive orders targeting what is described as illegal DEI, which includes directing federal agencies to clamp down on so-called illegal discrimination from federal contractors and publicly traded corporations mean that many employers are now reviewing their global ID&E strategy.

Diversity data and targets

A key tool to drive forward ID&E is the collection of data on diversity and its reporting. This can relate to gender and ethnicity pay reporting and extend to sex or gender identity, socioeconomic background, religion, etc. An increasing number of businesses are being encouraged and even mandated to collect and disclose data by supervisors. While building trust between employers and employees is vital (frequently their consent is required), the collection and processing of personal data must comply with local data privacy laws, which vary considerably. In some jurisdictions, targets to address underrepresentation can be no more than mere aspirational goals. Moreover, failure to achieve a goal can open up a business to scrutiny. Amongst others the US is seeing a change of approach.

Baker McKenzie Solutions — Key issues we advise on

- Transforming the traditional employment model including new staffing models
- Remote working including employment regulatory
- issues, data privacy, trade secrets, tax and real estate
- Digital progress and its impact on the workforce including rise of automation and employee surveillance Immigration and mobility
- Recruitment and reward (including pensions)
- Management support on HR policies, data protection and compliance, diversity & inclusion, senior exits, disciplinarians, investigations, performance management, litigation and terminations

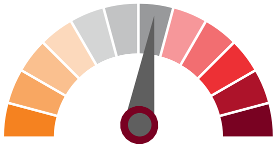
Theft, Fraud and Conduct Risk

Risk Profile

Recent Trends and Developments

- Growing reliance on digital and remote technology in daily operations and delivering services to customers has increased vulnerability to ever more sophisticated cyber-attacks and fraud.
- There is an increased focus on the importance of culture within financial institutions as a means of reducing conduct failings and better serving customers. Conduct risk represents systemic sectoral risk exemplified by consumer product mis-selling and continuing money laundering scandals. Regulators globally are paying special attention to this topic.
- With employee activism on the rise and corporate behaviour under increased scrutiny, together with whistleblowing regulation, organisations must ensure they implement compliant whistleblowing regimes across their operations.

Risk Rating: **Moderate**



Associated Risks

When the tide goes out

After stressed economic periods such as high inflation, rising interest rates and sluggish growth, enforcement and compliance activity usually increases. An analogy can be made to the tide going out to reveal wrongdoing that was previously hidden by business-as-usual activity. There is a likelihood of increased internal fraud and mis-selling coming to light. Additionally, new technologies are creating potential new avenues for unjust enrichment and even fraud. Besides ensuring technological defenses are kept up to date, investment banks should review higher risk past-business and activities to identify any misconduct, remediating when necessary and making appropriate disclosures to regulators to mitigate potential enforcement action and litigation.

Fraud and financial crime

Advancing technology such as artificial intelligence is providing new tools such as deepfakes to commit fraud, requiring the financial sector to update and strengthen its systems and controls; banks generally being more vulnerable than asset owners. Customer verification is another area of increasing risk, as bad actors work around technological barriers. Besides the long-tail of emerging pandemic era related frauds, Europe continues to see the ramifications of fraudulent cum-ex trading dividend schemes, while globally cybercriminals have committed fraud and theft on decentralized finance (DeFi) platforms. Money laundering and sanctions evasion continue to grow as does legal and regulatory liability.

Conduct risk

Conduct risk manifests itself in a variety of ways. For example, towards financial markets through market misconduct, including manipulative practices and insider trading; in respect of customers by mis-selling or failing to disclose conflicts of interest, as well as over issues touching on inclusion and diversity that can impact on a business' suitability to hold a financial services license. In respect of the approach taken by regulators, many financial institutions complain about the retrospective application of higher standards, especially over the duties owed to customers and allegations of mis-selling that can impose significant liabilities on businesses many years later.

Baker McKenzie Solutions — Key issues we advise on

- Compliance programs and training
- Data privacy rules related to automated checking for fraudulent activities
- Employment disputes and regulatory crossover
- Regulatory advisory/compliance
- Reputation management
- Whistleblowing and investigations
- Regulatory enforcement action
- Litigation and fraud recovery
- Mis-selling, market misconduct etc., and non-financial misconduct issues
- Cybersecurity including incident response and cyber fraud recovery

Regulatory and Resilience Risk

Risk Profile

Recent Trends and Developments

- Regulatory risk is continuously evolving. The possibility of large fines and penalties continue to concern risk managers. In addition, ever more resources are required for financial institutions to keep up with new regulations.
- Regulators' operational resilience principles are impacting investment banks — with business continuity teams focused on transitioning into becoming resilience teams. Model risk is also a continuing focus, where risk models for financial crime and credit risk are unable to anticipate sudden changes in the market or consumer behavior.
- In the US, we expect a lighter tough generally to regulation and, in particular, a less activist approach by the SEC with an end to what has been labeled as "regulation by enforcement".

Risk Rating: **High**

Associated Risks

Increasing levels of enforcement

The trend towards increasing regulatory scrutiny and, inevitably with it, enforcement has become clear in the years since the 2008 financial crisis and is now being boosted by firms' failings arising out of the sustainability and digital transformation megatrends. Nor is regulatory action coupled with significant sanctions, no longer just the preserve of authorities in the US, UK and Australia. Asian regulators are increasingly taking consequential steps. There are also a growing number of international standard- setting bodies, all driving standards up, pushing for new requirements. On financial crime, the FATF has been especially influential, latterly calling for more consistent and effective enforcement, most notably outside the US.

Operational resilience

Operational risk, resilience and impact tolerance are key regulatory priorities in recent years. This is linked to increasing levels of digitalization and outsourcing to third-parties in financial services. It is vital therefore for financial institutions to strengthen their resilience to risks including IT disruption. This involves identifying their most important services and understanding the systems and processes that support them, including any critical services that are outsourced, as well as assessing the impact of a failure, say an outage, and how quickly a system or process can be recovered or substituted. When services fail regulators are likely to ask questions and hold those responsible to account; this against a backdrop of new resilience regimes in the EU, Japan, UK and the US.

Increasing managerial responsibility

A number of financial centers have seen the creation of senior manager regimes to hold, individual senior managers to account for failures to take reasonable steps to prevent regulatory failures by their businesses. There are now clearer lines of responsibility when things go wrong. This may translate into more enforcement actions by regulators against individuals and financial institutions, most notably in jurisdictions other than the US, which has always been enforcement-led. It certainly appears to be making senior managers more cognizant of their duties.

Baker McKenzie Solutions — Key issues we advise on

- Regulatory advisory/compliance/licenses and registrations
- Outsourcing, risk management, disclosures, filing and reporting requirements including preparation of documentation and customer agreements
- Anti-money laundering and customer due diligence
- Advice on product offering, cross-border activities and market conduct offenses
- Financial and cyber crimes
- Cybersecurity incident preparedness and response
- Fraud & asset tracing
- Managing responses to regulatory questions, audits and investigations
- Understanding senior manager responsibilities and liabilities

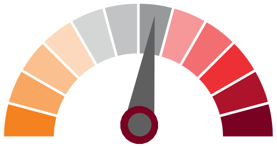
Geopolitical Risk

Risk Profile

Recent Trends and Developments

- Geopolitical challenges include ongoing US-China rivalry, and instances of armed conflict. Political and economic rivalries and national security concerns are affecting the ease of cross-border trade and investment. The imposition of sanctions on financial institutions and funds flows to customers have had a significant impact on business operations.
- Increasingly cyberattacks are being used by, and in support of, parties in geopolitical conflicts. Banks are natural targets for such attacks.
- The spotlight on tax havens and anti-tax avoidance initiatives continues to grow, increasing legal, compliance and reputational risk. Banks must balance customer relationships, expectations of privacy, information security and their public reputation.

Risk Rating: **Moderate**



Associated Risks

Operational and reputational harm

Recent geopolitical events, such as potential and actual armed conflict are having far-reaching and long-lasting effects on the operations of banks as they navigate a plethora of sanctions affecting themselves and their customers while attempting to facilitate international commerce. Financial institutions are also facing reputational risks for being on the "wrong" side of a conflict. Global instability is increasingly affecting the threat profile of banks, whose risk functions must identify their vulnerabilities, as they assess the likely effects of geopolitics on their business models and contingency plans.

International commerce / sanctions

Global supply chains are under pressure with businesses taking steps to boost their resilience and increase control. Here, payments throughout supply chains are being blocked or delayed because of sanctions and countermeasures, which also complicate syndicated lending. Banks must be vigilant about identifying these risks and mitigating their impact by having in place the right systems and controls to effectively screen against designated persons and asset freezes. Expect to see increased litigation from sanctions-related disputes with counterparties; the importance of reviewing terms and conditions for contractual protection is critical. Separately, there is the risk of protectionism, for example, over the "weaponisation" of tariffs, or market access to the UK and EU following Brexit that may be further complicated as their rules begin to diverge.

Taxation

International tax and transfer pricing structures in one jurisdiction are now more likely to be challenged by tax authorities elsewhere, with demands for even more data to substantiate their calculations. While exempt from the OECD proposals made under Pillar One, multinational investment banks will have to contend with the changing international tax landscape resulting from the implementation of Pillar Two. Not forgetting, the growing "social" element of responsible business practices and "Pay Your Fair Share" campaigns.

Baker McKenzie Solutions — Key issues we advise on

- Regulatory compliance and risk management: anti- bribery, corruption, sanctions & AML
- Customer and institutional relationship due diligence
- Licenses and registrations
- Disclosures, filing and reporting requirements; regulator questions, audits and investigations
- Cross-border commercial arrangements and agreements
- Sanctions and export controls; foreign investment reviews
- Product offerings; new market due diligence
- Tax risks (i.e., change in law, e.g., change to how carried interest is taxed etc.)
- Third-party supplier compliance

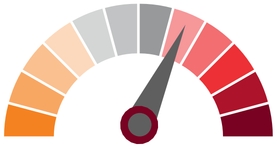
Third-party Risk

Risk Profile

Recent Trends and Developments

- Larger banks tend to have more third- party relationships, and having these brings additional risks. Regulators emphasize the importance of third- (and fourth-) party risk management to a company's operational resilience, especially given heightened cyber risk.
- As a general principle, while banks can outsource administration of their operations, they cannot outsource the risks nor their responsibilities. Regulators are also moving to regulate critical third parties, for example, the EU has recently enacted a Digital Operational Resilience Act (DORA) applied from January 2025.
- Cloud use also creates a grey area involving functions that banks continue to perform in-house and those that are outsourced to the cloud provider. Any uncertainty in the division of responsibilities can lead to costly mistakes.

Risk Rating: **Moderate**



Associated Risks

Cloud computing

Increasingly banks are using external cloud service providers. As well as risks to individual businesses, there are systematic risks because large cloud providers could be a single point of failure (i.e., concentration risk) when so many institutions rely on them. As cloud providers are unregulated and often sit in third countries, there are regulatory issues with supervisors requiring access and audit rights, augmenting the legal and regulatory tensions between all those involved. Increasingly, data localization restricts the ease by which data is transferred cross-border, thereby upping costs and, counter- intuitively, impeding regulatory oversight. Cloud as a critical third-party service is being brought within regulation for financial stability purposes.

Partnerships

Banks are using technology to rethink how they engage with customers at every interaction, from marketing and customer acquisition through onboarding, product setup, payments and transactions. Besides de-mediation and modularity, the rise of "banking as a service" and "banking as a platform" is also worthy of mention. They allow third parties partnered with licensed banks to include digital banking services in their own product offerings enabling, for example, the provision of payment and credit cards. Risks include loss of decision-making control, protection of IP, operational risk and reputational impact.

Operational risk

Financial institutions should prioritise an understanding of the systems and processes that support key services to customers, including those outsourced to third parties, especially financial market infrastructures and data vendors. They remain responsible to regulators notwithstanding any contractual provisions. As an example of third-party IT op risk, a bank recently experienced a technology malfunction due to its outsourced card processor, where IT services failed for hours during which time customers were unable to use their cards. The bank lacked adequate processes to identify and monitor these arrangements. The result — a fine and an even larger dent to its reputation.

Baker McKenzie Solutions — Key issues we advise on

- Outsourcing & cloud computing compliance and regulation
- Complex commercial contract structuring and negotiation
- Regulatory advisory/compliance
- Crisis and breach response and reputation management
- Data localization and international data transfer strategies
- Data management and monetization
- Copyright trade secret, and patent protection
- Managing responses to regulatory questions, audits and investigations
- Advice on product offering, cross-border activities
- Critical service providers

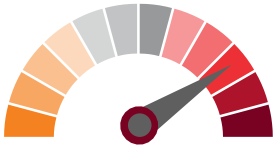
Climate Risk

Risk Profile

Recent Trends and Developments

- Climate litigation and enforcement represent a key risk for banks on climate change. Besides strategic litigation — claims that seek to influence strategy or business activities with respect to ESG issues — they face increased exposure not only when their statements are misleading or incomplete, but when their products and marketing do not align with public sustainability goals.
- Banks have become increasingly concerned about managing fragmented (and conflicting) sustainability reporting and disclosure standards, which are reinforced by legal requirements in some jurisdictions, especially the EU. Nonetheless, the new ISSB standards are mitigating such risks.
- In the US, expect to see claims against ESG investment policies, for example, for breach of fiduciary duty, or antitrust where banks collaborate over sustainability commitments.

Risk Rating: **High**



Associated Risks

Physical and transition risks

Transition risks arise when moving toward a lower-carbon economy, when carbon-intensive financial assets are revalued. Such transitions could mean that some sectors of the economy face significant changes in asset values or higher costs of doing business. It isn't that environmental standards are in themselves damaging the economy, rather the risk is from the speed of transition to a greener economy and how this affects certain sectors and financial stability. Prudential strength is at risk and the value of "stranded" investments could be reduced. Banks must increasingly have and disclose transition plans. EU banks must report on their Green Asset Ratio (the proportion of their financing aligned with the EU Taxonomy) despite concerns over the ratio's value.

Greenwashing

When making climate-related disclosures, it is important to understand the associated litigation and regulatory enforcement risks around greenwashing, putting in place appropriate mitigation strategies, including the use of relevant contractual terms to limit liability. Be prepared for increased scrutiny from regulators, shareholders and NGOs and stand ready to demonstrate the accuracy of disclosures and statements. Given the potential for confusion (especially for retail investors) resulting from the lack of common definition and standards, it is vital to clearly and consistently explain how terms are defined. Transition finance can move high emission and hard to abate economic activities toward net zero targets, but care is required to avoid "transition washing" if transition plans are not credible.

Data quality

Data quality is essential for sustainable decision making, reporting and disclosures. Historically, a lack of data and the necessary tools to interrogate it was a significant hurdle. Early approaches to sustainability due diligence were based on exclusionary screening and value judgements. Nowadays there are a wide number of non-financial metrics, methodologies and approaches and increased levels of disclosure by companies. Its importance is underlined by supervisors' steps to bring ESG data providers within regulation. Potential risks that arise, range from data security, its processing to its validation. Senior managers must ensure that there are processes in place to review and audit both metrics and data quality.

Baker McKenzie Solutions — Key issues we advise on

- ESG regulatory for financial institutions
- Advice on non-financial reporting/disclosure requirements
- Climate change law
- Sustainable Finance regulation
- Clean energy development and financing
- Energy Transition & Transition Finance
- Disruptive innovation
- ESG Litigation risk and enforcement for financial institutions
- Stakeholder activism
- Review and update ESG and governance frameworks

Regulatory Risk Management for Financial Institutions

Resources

An overview of the challenges facing the sector, and updates risk radars on fintech and digital transformation, sustainability and regulatory scrutiny, which describe the trends, developments and associated risks affecting financial services.

Visit the resource

Available on our Resource Hub, this provides a snapshot of the legal and regulatory position of cloud in key jurisdictions of interest for financial institutions.

Visit the resource

This guide considers what is greenwashing, the developing legal landscape and how financial institutions may mitigate the risk of reputational damage.

Visit the resource

The article explores the road ahead for artificial intelligence in financial services.

Visit the resource

Provides a comprehensive summary of regulations applicable to banks and other financial services companies around the world.

Visit the resource

FInsight, Baker McKenzie's Global Financial Institutions Podcast, provides recommendations and insights into sectoral developments and industry trends from Baker McKenzie's legal experts.

Available on: Soundcloud | Spotify | Apple Podcasts | Google Podcasts

Key Contacts

Vinod Bange
London
vinod.bange
@bakermckenzie.com

Christoph Kurth
Zurich
christoph.kurth
@bakermckenzie.com

Dani Fonseca Puggina
Miami
daniela.fonsecapuggina
@bakermckenzie.com

Philip Annett
London
philip.annett
@bakermckenzie.com

Karen Man
Hong Kong
karen.man
@bakermckenzie.com

Peter Chan
Chicago
peter.chan
@bakermckenzie.com

Georgie Farrant
Sydney
georgie.Farrant
@bakermckenzie.com

Caitlin McErlane
London
caitlin.mcerlane
@bakermckenzie.com

Sunny Mann
London
sunny.mann
@bakermckenzie.com

Band 1 – Global-wide, Intellectual Property
Chambers 2009-2025

Band 1 – Global-wide, TMT
Chambers 2025

Band 1 – Global-wide, Outsourcing
Chambers 2025

Band 2 – Global-wide, Banking & Finance
Chambers 2025

Band 1 – Global-wide, Employment
Chambers 2010-2025

Baker McKenzie delivers integrated solutions to complex challenges.

Complex business challenges require an integrated response across different markets, sectors and areas of law. Baker McKenzie's client solutions provide seamless advice, underpinned by deep practice and sector expertise, as well as first-rate local market knowledge. Across more than 70 offices globally, Baker McKenzie works alongside our clients to deliver solutions for a connected world.

bakermckenzie.com