# Three priorities for financial institutions to drive a next-generation data governance framework

Building a better
working world

# Executive summary

Increasing business consumption and volumes of data present both opportunity and risk. Open access to data and advancing data technology capabilities can create faster, customized services which firms and their customers increasingly have grown to expect. Emerging and advanced technologies that enable this opportunity, including cloud solutions and services-based architectures, also add complexity to the data ecosystem. Only technology and data-led solutions to monitor, analyze and protect data can match the scale and magnitude of these risks and enable their management. These next wave data management solutions can help mine, manage and protect data, but work needs to be done to evaluate just how this can be done safely and what oversight needs to be in place.

The control environment is more important than ever, as data governance is now a key element that regulators are scrutinizing closely, both in terms of the protection of data and as part of the wider challenge of maintaining operational resilience. Issues of data quality, privacy and security, and the accompanying threat of cyber-attack, have risen to the top of the supervisory agenda. The focus is not just on the firm, but also its use of third parties, cloud and the potential for external disruption caused by IT failure, poor security protocols or concentration risk arising from over-reliance on a small number of service providers.

The key business outcome is to improve and widen the impact of current data governance frameworks to take advantage of this explosion of data. This requires recognizing that these trends can also support the effectiveness and efficiency of traditionally manual activities. Using the increase in data volume to automate and scale data governance processes will reduce cost, lessen risk, and enable new opportunities. It will also support the ethical use of data, which is a priority outcome for regulators.

# Background

Data governance is an area of significant regulatory focus. Initial regulations, such as post-financial crisis regulatory reform (including the Basel Committee on Banking Supervision's standard number 239 (BCBS239) and the European Union's (EU's) Solvency II Directive), focused on data governance, quality and underlying risk management controls. More recent regulatory action has continued to drive change. Examples include: the European Central Bank's Data Quality Dashboard, the California Consumer Privacy Act (CCPA) and, most notably, the EU's General Data Protection Regulation (GDPR), which compels the industry to better manage the privacy of individuals' personal data. Effort is now required to embed data governance on a sustainable basis within financial services firms.

Recent regulations focus on how financial services firms are using data and whether this use is appropriate, and consistent with how it was originally intended to be used. With the advance of technologies and the drive to compete in the market with new data-driven industry entrants, firms are discovering new ways of utilizing data beyond what was originally intended. Examples of exploring such unintended uses of data can illustrate how those situations should be managed. Often firms do not know how their data is used, and by whom within the firm. There is an increasing trend of firms trying to explore new ways to monetize their data, adding extra pressure to innovate and sell the insights from the data they hold. This increases the risk of unintentional data abuse. Effective data governance provides transparency over the utilization and consumption of data, recognizing that analytical models are being used for more than traditional purposes, and far more data is being used to manage risk, track finances, sell more products, and advertise to customers.

### Unexpected outcomes driving change

Examples of unexpected outcomes from the proliferation of data and analytics that are driving regulatory attention include:

1. Significant data breaches, such as hotel stays, airline bookings, credit card details and personal information from social media sites
2. A European government's machine earning (ML) model to identify welfare fraudsters being ruled unlawful as it disproportionately targeted poorer citizens
3. Underwriting models in Europe discriminating on gender where job type was learned by ML models, followed by a US credit card launch which encountered gender bias issues
4. Third-party risks associated with the sharing of customer data, including recent data theft via service providers
5. Publicly-available chatbots being taught racially-biased concepts when they could learn from new data sources and human interactions
6. Reduction in the quality of stress-testing models with over-positive assumptions for new banking market entrants in the UK, leading to a run on a bank

# Governing the use of data

## Data governance must balance and accommodate protection and growth by managing risk appetite and supporting business ambitions.

To achieve growth, while protecting the organization, new approaches to scale data governance are required. Traditional approaches that included manual processes controlled and managed through spreadsheets with basic approvals are no longer sufficient. Data can be accidentally moved globally with the push of a button, or may be captured hundreds of times an hour through an Internet of Things (IoT) device, rather than once a year on product renewal. A well-controlled data environment can enable, rather than hinder, business outcomes.

### Protection data use cases

- Risk — valuation and stress testing, exception reporting, customer or member complaints, incident reports, conduct risk and market abuse, enhanced data quality monitoring, minimum capital requirements for market risk, and fundamental review of the trading book
- Finance — financial planning and forecasting, cost allocation and control
- Operations — customer or member service, case management (e.g., single customer view) complaints
- Regulatory reporting — accuracy, completeness, appropriateness and timeliness of regulatory reports, such as capital and liquidity reporting, transaction reporting, regulatory returns, client stock and asset records, customer fees and charges, stock exchange and clearing house reconciliations, "know your customer" (KYC), and legal entity identifiers (LEIs)
- Privacy and ethics — original versus current use of data, ownership and segregation of data, anonymization and tokenization of data where possible, controlling data flows, appropriate data sharing, and respecting local data privacy rules that include localization of data storage

### Growth data use cases

- Marketing and customer experience — customer or member insights, lifetime value, communications optimization, campaign management and automation, and contact preferences
- Pricing — underwriting, pricing models, predictive modeling, competitor pricing intelligence, next best offer, and personalized pricing
- Product development — customer or member segmentation, product configuration, product testing (test and learn), and budget allocation
- Sales and distribution — incentive and commission optimization, digital channel management, sales performance, and cross sell-opportunity identification
- Monetization — realizing the value in data to internal or third parties and generating benefits from this — whether through direct resale, cross-selling, rewards programs, improved offers or new business models

Ultimately, the goal of data governance in supporting the business is to ensure that high-quality governed data serves as the foundation for business use. Approaches to achieve this must evolve in response to an ever-changing data landscape where rapid change is the new normal. Typical data governance goals that we observe include:

- Providing trusted data through consistency of information across channels, lines of business, interactions, core metrics and metadata
- Enabling better decisions with a 360-degree view of the customer or a product, that is available when needed
- Ensuring quality data that can support generating and sharing analysis and actionable insights through

hypothesis-driven testing, which involves writing the test before the experiment

- Building trust in data, supported by clear reporting to key stakeholders, who can then act in a timely manner
- Innovating through clear key performance indicators for both digital and non-digital channels to identify growth opportunities and areas where protection is needed
- Ensuring safe, controlled use of data with recognized custodianship of critical and customer data
- Establishing data controls that are auditable, transparent, testable and applied to data once, after which that data should be classified as appropriate for similar use, without retesting
- Accepting that controls age so there is a need to apply periodic review, with accompanying sign-off of that review leveraging proper governance that assigns clear ownership for accuracy and completeness

Given the large number of challenges in data governance, and the regulatory focus, firms are prioritizing three areas that address both the protection and growth of data, as well as the regulatory agenda:

1. Protecting data privacy through enhanced access controls
2. Automating and extending data governance controls to next generation data fabrics and cloud platforms
3. Extending data governance to advanced analytics and decisioning, particularly artificial intelligence (AI) and ML, to build trust in these models and their outcomes

Some of these steps require firms to develop controls and governance ahead of regulation that is still emerging in relation to data analytics and AI/ML — and evolving rapidly but unequally across the world in the case of data privacy, big data, AI and the cloud.

# Focus 1

## Protecting data privacy through enhanced access controls

Firms frequently find that they do not know how or by whom within the firm the data they own is used. Traditionally, ensuring data privacy focused on role-based access control (RBAC) that restricted access to sensitive data to people who had a need to view or edit it to perform their jobs. While new models are automated, they require large amounts of training data sets, which can often challenge existing controls that would limit the use of production data. The use of the public cloud creates new challenges, primarily around the sharing of data, the geographic location of that data, and understanding a data's source or lineage, as data can be rapidly replicated multiple times. Challenges also occur in relation to the right of customers to be forgotten, per GDPR and similar regulations, as typically customer data is held across many systems and with many copies. It is proving incredibly difficult for firms to selectively destroy or obfuscate an individual's records.

Achieving compliance with privacy regulations and meeting customers' needs requires transparency in the storage, processing, control and distribution of private data. Modern data privacy controls are a growing trend, but are predicated on exponential growth in data sourcing and usage with more diverse uses of greater amounts of data. Organizations have begun responding to this paradigm shift in privacy regulations by revisiting their enterprise strategy, C-level accountability, and funding for programs related to people, technology, and new operations.

The introduction of open banking and open APIs (Application Programming Interfaces), which obliges the sharing of data to enable more data portability and increase market competition, is also creating data privacy challenges, particularly when data protection and data privacy regulations conflict with openness. While the implications

### Enterprise data privacy

Key drivers of enterprise data privacy:

- Increased public awareness of data breaches or exploits
- Significant reputational risk
- The recognition of the value of being a trusted brand
- Bias of models, disadvantaging minority populations, or even large groups of customers
- Accessibility of enhanced analytics
- Regulations, including those referenced previously (GDPR, CCPA, etc.)
- Cybersecurity expectations, including NYDFS – Cyber Security Regulation 23 NYCRR 500, ISO 27001
- Emerging approaches to privacy, including the newly published ISO 27701 in 2019

This has led to the scope of data privacy expanding rapidly:

- Additional information is being classed as personally identifiable information (PII)
- New customer privacy rights are being given by legislation
- There are stated regulatory intentions for greater transparency over usage, including informed consent
- Customers' desire for more control over their data

As a result, regulatory expectations have increased to consider ongoing compliance, the traceability of data, the detection of data movements and leaks and a focus on the deletion of data, or links to an individual, when it is no longer required. Failure to meet these expectations can lead to large fines and damages. Therefore, organizations need to move beyond regulations by defining their own data privacy framework, recognizing that local regulations will take time to catch up and embrace the opportunity to enable good commercial outcomes. Data governance is key to this.

are understood at a conceptual or theoretical level, they still need to be addressed in practice. Such practical decisions will not just affect data directly associated with an individual that may be more clearly controlled and shared, but also the surrounding metadata; for example the significant metadata that will be generated by autonomous vehicles and will be needed for automotive insurers.

Future regulations are likely to give individuals increased ownership of their data, which will affect transfers and use of their data. Firms should be working to define digital data rights and standards, particularly in how they will protect individual privacy.

Effective data governance requires transparency over the storage and consumption of data. However, traditional risk-based approaches that managed control libraries and applied retrospective controls are not sufficient to manage the complexity of data privacy. This occurs as technologies, innovations, and use cases become more and more sophisticated and difficult to manage. Establishing a GDPR-like "privacy by design and by default" (meaning processing of personal data must be done with data protection and privacy in mind at each step) requires a structured approach and new capabilities along the entire data lifecycle. This is like a traditional "process and controls" approach, but requires more forward-looking interpretation and consideration. For example, not allowing the data collected by a mobile app to be used for individual analysis may seem sensible on launch, but will greatly hinder an organization's future use of that data to make better offers to their customers.

# Focus 2

## Automating and extending data governance controls to next generation data fabrics and cloud platforms

As with data privacy, new data platforms present new challenges in terms of the storage, sharing and movement of data. There is ongoing debate among the industry and regulators about whether the cloud creates a completely new challenge for data governance, is merely an extension of existing technology practice or provides new opportunities to use modern technologies to solve these challenges. It is now commonly accepted that the same regulations and controls are required either on premises or in the cloud, and will have continued examination, but the cloud offers the opportunity to apply more automated controls to address concerns and regulation. Particularly for new entrants to the market who are "cloud native" (i.e., only use public cloud technologies), this potentially provides these new entrants with a competitive advantage if they can automate controls and reduce costs, while being able to properly use their data. In contrast, traditional players have the advantage of mature control and compliance frameworks and expertise.

Key controls are needed to:

- Move data, while avoiding control gaps and ensuring a consistency of controls.
- Automatically tag atomic information (i.e., the lowest level of detail possible) held in the cloud to make it useful for subsequent enterprise reporting.
- Adopt a micro-services-based approach to manage metadata and quality across the data fabric, which allows different applications and consumers to use common services where those services are fine-grained and the protocols are lightweight.
- Monitor to ensure that controls are maintained over time; for example, European data subject to GDPR does not accidentally leave the EU through monitoring of metadata tags, or to demonstrate that specific controls were implemented to automatically identify and protect sensitive data, such as passport numbers.

Typical use cases that can be better addressed in the cloud include: shadow IT (business teams acting as technology teams to develop technology, with fewer controls in place), and data classification (tagging data on entry or creation and taking it through the lifecycle with appropriate controls, including encryption). Ultimately, this is a good opportunity to improve data governance through cloud control as there is "nowhere to hide" since a single cloud framework can be applied automatically across all technology on the cloud. However, this also recognizes that the exposure of such technology presents new risks that will be more exposed, including concentration risk associated with a small field of enterprise-ready public cloud providers.

### Cloud governance framework

A well-formed data governance framework for the cloud needs to consider the following:

- Regulation – What controls are required to be compliant across regions, and what industry standards should firms follow?
- Visibility – How do firms evidence that the necessary controls are in place?
- Data classification – How should data be classified? How should different classifications be handled?
- Risk management – How should operational risk be measured and reported?
- Data governance – What micro-services are needed to manage data fabric?
- Change management – How do firms keep abreast of changing global regulations?

The maturity of big data architectures has led to increasingly granular data submission requests from regulators. Where once one large European regulator requested monthly submissions of hundreds of items of data, they now receive over 50 million daily submissions, including granular trade-level data that must be analyzed and stored in a data lake. However, while the financial services industry has lagged others in using the cloud, the main blocker has been clarity over the required controls to be compliant in the cloud. Such blockers particularly focus on international data transfer regulations, despite many regulators being supportive of a multi-cloud strategy due to its increased resilience over traditional technologies.

The requirements for data quality and governance on the cloud have not shifted — a banking organization still needs to comply with BCBS239. However, firms are realizing that more specific requirements are needed. They are wrestling with the challenges associated with defining criticality and thresholds in analytical models driving decisions or notifications, which are appropriate for both a traditional architecture and a cloud-based architecture, and whether a single threshold is appropriate for both.

Meanwhile, the amount of information available in a data fabric or data lake architecture means that it is possible to offer a higher quality of data from such architectures, with a focus on completeness, reconciliation and monitoring capabilities. Vendors offer the ability to identify and manage such information and provide different “views” of data quality, including differentiated user access to either “raw” data that has just arrived, through to “conformed” data stores where data is available for wider consumption with a guaranteed level of quality.

# Focus 3

## Extending data governance to advanced analytics, particularly AI and ML, to build trust in these models and their outcomes

Rapid innovation in AI/ML is not only driving business transformation, but also highlights unique challenges and risks related to the governance of data:

- AI/ML applications are becoming more powerful and accessible as firms increasingly use big data, low-cost computing and access to open source algorithms.
- There is rapid innovation in AI/ML as firms, or new entrants, develop new products, drive business transformation, improve customer experience and achieve operational efficiency.
- Meanwhile, regulators and the industry have recognized challenges, such as explaining to humans so they understand what is being done and why, transparency (the ability to inspect and reproduce), data privacy (respecting law and consumer expectations), bias (avoiding systemic prejudice), ethics (fair use of data), consumer protection (treating consumers fairly) and data-related systemic risks.

In developing a data governance framework to manage the challenges posed by the rapid acceleration and scaling of the use of AI/ML globally from small prototypes three years ago and the decisions that could affect growth and protection, firms should:

- Establish an AI/ML governance framework that addresses, data-related risks of the AI/ML eco-systems in aggregate; provides cross-functional oversight and transparency; considers a risk-based approach for implementing controls; conducts pre-mortem analysis running worst case outcomes against AI-use cases; focuses on delivering trusted outcomes and develops centralized capabilities (platform, data, skill-sets).

### What are the risks of AI?

Previous financial crises highlighted risks from over-reliance on models and from the introduction of complex products without an understanding of their limitations and performance under stress. As a result, to scale AI, risks should be addressed at two levels:

- Micro AI/ML application level (e.g., transparency, conduct)
- Macro AI ecosystem level – risks due to the convergence and dynamic interaction of risks (e.g., infrastructure risk, third-party risk, adversarial attacks) – making the aggregate impacts more widespread and perpetuated at a greater speed

On the positive side, much focus has been on individual (micro) scenarios, on the ethical use of AI – without supervision such algorithms may discriminate in ways that are illegal and immoral (e.g., racial bias, gender discrimination) or may be risky (e.g., reducing credit risk management or making bad investment choices).

The technology industry has responded positively to try to address these issues with technical solutions. However, organizations need to proactively embrace addressing these issues holistically (macro). Otherwise, they risk facing increasing regulation, data localization that prevents data from being shared across borders, and a public backlash that will reduce many of the positive benefits of AI for humanity, particularly the automation of repetitive work and potential new innovation.

- Embed AI/ML governance in the overall business strategy (i.e., return on investment should account for the cost of governance) with a clear AI/ML framework that addresses key risks and customer concerns, particularly ethics.
- Achieve firm-wide awareness of the AI/ML governance framework through training programs and communication.

To do so, firms can rely on the underlying technical implementation of the AI/ML governance framework, which is automatically included within a model inventory and used in regular testing. The framework should include early risk assessments — based on an understanding of AI/ML techniques — and use cases to which new technologies are being applied. Importantly, to ensure that the AI/ML governance framework identifies AI specific risks to the business which is then integrated into existing risk and control frameworks and model-governance processes. This framework ultimately should be automated and balance data value versus risk, mapped against clear business outcomes and benefits. As AI/ML technologies advance and become more accessible, and therefore become an integral component of business functions, achieving this level of integration and automation will be imperative. We see an increased focus on the trust that AI/ML models can provide.

# Next steps

## Framework for managing change

Globally, regulators and the industry have focused consistently on strong and clear leadership and effective governance that monitors common standards applied across a firm. As businesses shift from regulatory transformation to data-driven innovation, CDOs will continue to provide traditional protection and governance in addition to playing a strategic leadership role in driving growth through digital transformation and technology innovation.

Ideally, data governance frameworks should be aligned with emerging industry standards, particularly since financial services are increasingly moving toward common standards and capability frameworks and will need to share parts of their data using open application program interfaces (APIs).

## Framework components

Firms should undertake the following steps to resolve the inherent risks of data governance:

1. **Build simpler data architectures that enable these concepts:**
    - A controlled data ingestion framework that tags and tracks data throughout an organization
    - A micro-services-based approach to create efficient, repeatable approaches to onboarding data to a common data fabric
    - Profiles that understand and classify data as it enters the architecture or is processed
    - Automatically cleansing and improving data using AI algorithms
2. **Enhance, automate and integrate data quality controls to:**
    - Allow for an understanding of the limitations of data, but also what it can be used for, and when, including a refresh of existing privacy frameworks to capture fast evolving legislative developments
    - Ensure AI and ML risks can be addressed through automated, context-aware data quality ratings
3. **Apply new controls and thought processes to AI and ML**
    - Perform risk assessments on AI/ML techniques and use cases
    - Ensure existing model governance is extended to cover relevant AI/ML applications that will be used in production
    - Extend data governance to connect to model governance
    - Establish relevant three lines of defense over the groups who will be responsible for AI/ML models, including those classified as "innovation" teams
    - Develop robust oversight processes for high-risk models, particularly those that could have a customer or regulatory impact
4. **Create an integrated data governance and control framework for the next generation data platforms**
    - Ensure that the integrated cross-functional risk and control framework of models, data, operational risk and compliance incorporates new technologies and concepts
    - Enhance existing risk and control frameworks to incorporate AI and cloud-specific risks
    - Extend the application of this framework to cover the cloud, noting that requirements have not changed but the technology has shifted
5. **Refine the operating model and capabilities**
    - Decide on the level of centralization within the firm that is appropriate to manage data governance — choosing between a centralized and de-centralized model or a hybrid, such as hub-and-spoke that has become increasingly popular
    - Establish relevant capabilities across the firm that are focused on data management and governance, applying relevant controls within a data platform or infrastructure
    - Build a team with relevant modern cloud and data skills through a relevant training and hiring strategy

# Conclusion

To properly leverage the opportunity and risk of increased data volumes and new data technologies, firms must develop their data governance framework and focus on improving controls and ethical use of data. This will be the minimum expectation of regulators, who are increasingly cognizant of the disruptive impact and security threat posed by weak data governance and protection.

Due to recent high-profile cyber-attacks and data breaches in both the financial and non-financial sectors, supervisors will have limited tolerance for firms that remain passive. A shift to a proactive strategy is essential, with enhanced capabilities in:

- Privacy frameworks
- Data traceability and detection
- Data deletion and erasure
- Cybersecurity
- Data and analytics growth and innovation
- Digital transformation
- Data security and controls
- Ongoing assurance and compliance monitoring
- Governance, identification and allocation of executive responsibility

Strengthening these capabilities across the business will enable a data governance framework that supports key business outcomes focused on growth while demonstrating an approach to data that is protective and operationally efficient.

# Glossary

## Common terms used in this paper

Throughout this paper, we have used the following terms that are changing the data environment:

- **Types of data**
  - **Structured data** – clearly defined data types whose pattern makes them easily searchable.
  - **Unstructured data** – data that is usually not as easily searchable, including formats like audio, video, and social media postings.
  - **Streaming data** – data that is continuously generated and processed rapidly.
  - **Metadata** – information about data, which in this paper is taken to include not just a direct record but the surrounding data that adds context to it. For example, a customer's trip information (destination, time, cost) can be much more valuable if it also includes associated information on lifestyle, social connections and mobile device details and location.
- **Uses of data**
  - **Model** – analytics-driven calculations that recommend an outcome for subsequent action based on an equation against a specified data set. This calculation may be used for many purposes, including risk, finance, advertising, marketing and many others besides.
  - **Artificial Intelligence** – the use of computers to perform tasks normally performed by humans; for example, making decisions, visual perception and translation.
- **Structures and stores of data**
  - **Cloud** – a computing capability that is available on demand to end users.
  - **Data repository** – storage of data or information within an organization, hopefully computer readable.
  - **Data lakes** – storage of structured and unstructured data held in its raw or derived format to enable future business processing.
  - **Data fabrics** – a modern data architecture design pattern or reusable solution that makes data actionable by contextualizing it to "connect the dots" to other data sets.
- **Microservices** – loosely coupled services offering more dynamic abilities to swap capabilities into and out of an architecture more rapidly.

# For more information, contact the authors of this report:

**Chris Barford**
Advisory Data and Analytics leader, Financial Services
Ernst & Young Advisory Services Limited (Hong Kong)
+852 9666 6347
chris.barford@hk.ey.com

**Stuart Wallace**
Senior Manager, Financial Services Advisory, Ernst & Young LLP (UK)
+44 (0) 131 777 2816
swallace1@uk.ey.com

**Mahesh Shahapurkar**
Director, Financial Services Advisory, Ernst & Young LLP (UK)
+44 (0) 20 795 14025
mshahapurkar@uk.ey.com

**John Liver**
Partner, Financial Services
Ernst & Young LLP (UK)
+44 20 7951 0843
jliver1@uk.ey.com

**Marc Saidenberg**
Principal, Financial Services
Ernst & Young LLP (US)
+1 212 773 9361
marc.saidenberg@ey.com

**Eugène Goyne**
Associate Partner, Financial Services
Ernst & Young Advisory Services Limited
+852 2849 9470
eugene.goyne@hk.ey.com

# EY Global Regulatory Network executive team previous appointments

### Kara Cauter

**kara.cauter@uk.ey.com**

She has over 20 years' experience working in global professional services firms, advising banking clients on the implications of the regulatory agenda and designing approaches to effectively meet those obligations.

### Meena Datwani

**meena.datwani@hk.ey.com**

She has over 35 years' experience in government of which the last 23 years were in senior regulatory roles. She was the Executive Director of Enforcement and Anti Money Laundering Supervision at the Hong Kong Monetary Authority (HKMA). Prior to that she was the Executive Director for Banking Conduct and Chief Executive Officer of the Hong Kong Deposit Protection Board. She also served as Deputy General Counsel and before that Senior Counsel. Prior to the HKMA she was a Senior Government Counsel with the Department of Justice of the Hong Kong Government.

### Mario Delgado

**mario.delgadoalfaro@es.ey.com**

FROB (Spanish Banking Resolution Authority) Head of International Coordination and EBA and FSB representative; Spanish Ministry of Economy: Director of Office of the Secretary of State for the Economy in the Economic Affairs; Head of the Spanish Delegation in the Paris Club; Deputy Head of relations with the IMF.

### Marie-Hélène Fortésa

**marie.helene.fortesa@fr.ey.com**

Autorité de Contrôle Prudentiel (French Prudential Supervisory Authority); Association Française des Banques (French Banking Association); and French National Institute for Statistics and Economic Studies. She has also held senior roles at a global investment bank.

### Eugène Goyne

**eugene.goyne@hk.ey.com**

He has over 20 years in government and senior regulatory roles. He was previously deputy head of enforcement at the Hong Kong Securities and Futures Commission (SFC). Prior to the SFC, Eugène worked at the Australian Securities and Investments Commission and the Australian Attorney General's Department.

### Alejandro Latorre

**alejandro.latheron@ey.com**

Alejandro (Alex) has over 20 years of experience at the Federal Reserve Bank of New York in monetary policy, capital markets and financial supervision and regulation. He was a senior supervisor involved in the oversight of large and systemically important FBOs in the U.S. Prior to his role as a senior supervisor, he was involved in many of the Federal Reserve's financial crisis management efforts.

## John Liver

**jliver1@uk.ey.com**

Divisional Compliance Lead at Barclays; Head of Department, Investment Firm Supervision and prior roles in enforcement and supervision of investment management, life insurance and pensions at the UK Financial Services Authority and its' predecessors. He is currently EY/UK Financial Conduct Authority relationship lead.

## Shane O'Neill

**soneill2@uk.ey.com**

He has 20 years' experience in banking, capital markets, asset finance and prudential regulation in a variety of CFO, COO, strategy and planning, and regulatory roles. Following the financial crisis, Shane was Head of Banking Supervision at a Eurozone Central Bank for four years, during which he influenced significant restructuring, recapitalization and change in the banking sector and in credit institutions, and executed numerous stress tests and asset quality reviews.

## Keith Pogson

**keith.pogson@hk.ey.com**

Immediate past President of the Hong Kong Institute of Certified Public Accountants; more than 20 years of experience advising governments and regulators across Asia-Pacific on acquisitions, market-entry strategy and due diligence across banking, asset management and securities.

## Marc Saidenberg

**marc.saidenberg@ey.com**

Senior Vice President and Director of Supervisory Policy at Federal Reserve Bank of New York; Basel Committee Member and Liquidity Working Group Co-chair; involved in the development of supervisory expectations for capital planning, liquidity risk management and resolution planning.

## Scott Waterhouse

**scott.waterhouse@ey.com**

He was capital markets lead expert for large banks at the Office of the Comptroller of the Currency (OCC) and Examiner-in-Charge of the OCC's London Office. He coordinated the supervision of trading, treasury and capital markets activities including Dodd-Frank implementation and Basel Committee requirements.

# EY | Assurance | Tax | Transactions | Advisory

## About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation is available via ey.com/privacy. For more information about our organization, please visit ey.com.

## About the EY Global Regulatory Network

EY's Global Regulatory Network helps clients find solutions to their regulatory challenges, providing extensive experience, leadership and strategic insights on financial regulation. The network helps EY clients to understand and adapt to the impact of the changing regulatory landscape.

Led by John Liver and Marc Saidenberg, the network comprises more than 100 former regulators throughout the Americas, Asia and Europe, many with senior regulatory experience, including membership in the Basel Committee, the Financial Stability Board, the European Banking Authority, the Federal Reserve Bank of New York and the Japanese Financial Services Agency. The network helps clients to understand and adapt to the impact of the changing regulatory landscape, advising on such topics as:

- Capital and liquidity
- Recovery and resolution
- Governance
- Risk culture and controls
- Structure
- Conduct

Learn more at ey.com/grn.

EYG no: 001225-20Gbl

BMC Agency
GA 1014762

ED None

In line with EY's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

**ey.com/grn**