



2019 Global bank regulatory outlook

Preparing for regulation
in the digital age



Building a better
working world



The 2019 annual bank regulatory outlook appears at a time when regulators globally are increasingly turning their attention from post-crisis reforms to a new set of emerging risks and priorities.

This shift reflects a regulatory and supervisory policy focus on the digital transformation of financial services and the challenges and risks presented by technological innovation, new market participants and evolving business models. Regulators are transforming too; trying to integrate new technology and data into their own supervisory processes, regulatory reporting and market oversight.

This outlook considers the new challenges for banks and regulators in evolving markets, while each also addresses a set of legacy issues. The key message for firms in 2019 is that the current regulatory transition signals a need to focus on the people, processes and technology to deliver a 21st century, digitized, fit-for-purpose risk and compliance framework.

1 A changing landscape for supervisors: the regulatory environment in 2019

Banks and regulators are operating in an environment that is subject to shifting dynamics. The changing digital landscape raises questions about the use and ownership of data and the boundaries of regulation, in light of differing supervisory approaches to new products and services. This is playing out against a geopolitical backdrop that is creating anxiety in the markets about the credit cycle and future conditions for growth and investment.

Regulatory standards and fragmentation

The supervisory and policy agenda is firmly in review mode. Global regulators are reviewing current rules and regulations with an eye toward making them more proportionate and transparent. As the chair of the Financial Stability Board (FSB) said in his letter to the G20 in November 2018, “Safeguarding progress does not mean defending all aspects of reform at any cost. In assessing what is working as intended and addressing any inefficiencies or unintended consequences, the FSB is tailoring not tapering.”¹ But there are signs that the consensus on post-crisis objectives is fraying. The implementation of global standards is incomplete and inconsistent across jurisdictions. In some cases, local rules are already subject to review or revision (e.g., in the US, the Federal Deposit Insurance Corporation recently indicated that it will consider easing requirements for resolution plans). It should be noted, however, that local adjustments are often driven by a desire to avoid a “one size fits all” approach that may otherwise cause small and midsize players to comply with rules that are designed for G-SIFIs (Global Systemically Important Financial Institutions).

Business drivers and new technologies

The increased velocity of the transformation agenda and emergence of new market participants, products, service providers and vendor utilities is unprecedented. The EY Global Regulatory Network explored some of the implications in its recent paper on regulation and technology-enabled innovation.²

Regulators and industry participants see significant opportunities to develop new tools to manage risks and enhance the efficiency, safety and soundness of firms and markets. Global and local policymakers are looking to harness and control the development, deployment and operation of new technologies. But the drive to build a more robust control framework in this digitizing landscape is exposing a number of new risks, which we examine in this paper.

Developing markets present opportunities

The growth of emerging market players with their own priorities is an increasing factor on the global stage. In developing economies where applications of new technologies are evolving quickly and are driven by new participants, FinTech is seen more as an opportunity than a challenge. China has several examples of fast adoption, such as commitment to large-scale use of the cloud and the switch from cash to electronic payments. It will be interesting to see what level of regulatory scrutiny accompanies faster implementation in Asia, and to what extent it influences the global agenda.

¹ “FSB Chair reports to G20 Leaders ahead of the Buenos Aires Summit,” FSB, November 2018

² “How can regulation keep up as technological innovation races ahead?,” EY, July 2018.

A dilemma: the scope of regulation

Having grappled with systemic risk issues and the lack of transparency that characterized the last crisis, supervisors are conscious that similar problems might appear elsewhere in the financial system. The current environment reflects a vibrant and innovative mind-set, but it is also populated by new entrants that have not been through a crisis or experienced seismic market activity; are not subject to the same level of oversight or expectation as financial market incumbents; or may be entirely outside of the existing scope of supervision.

Policymakers, therefore, must assess the existing supervisory framework and decide not only on the extent of the regulatory perimeter, but also the approach to regulation going forward (see sidebar, “Where next for regulation?”).

Questions they need to answer include:

- ▶ What set of rules should apply to new entities that take “bank-like” risks?
- ▶ How do you treat external entities that create vulnerabilities for banks due to their access to bank systems or external entities upon which banks become critically dependent?

- ▶ Should disruptors be held to the same standards as incumbents?
- ▶ Will a license or authorization relate to the type of entity or to the type of activity?

The growth of crypto-assets in the last few years illustrates some of the challenges. A consensus that such assets do not yet pose overall systemic risk is accompanied by an equally accepted view that offerings to the public of such assets generate issues around investor protection and financial crime that must be addressed. Lack of agreement on the definition and treatment of such instruments across jurisdictions means that, thus far, the response has been fragmented. Lessons from exploration and testing in regulatory sandboxes and other approaches could be coordinated further to deliver practical and consistent outcomes.

In any event, both regulators and banks are on a steep learning curve due to the fast-moving nature of technology and market applications. Regulators may need to adopt a more collaborative posture with the industry, rather than being a traditional rule giver, when setting standards for new products, services and participants.

Policymakers must decide not only on the extent of the regulatory perimeter, but also the approach to regulation going forward.

Where next for regulation?

Regulators, like the market participants they supervise, must find a way of operating effectively within the new landscape. Post-crisis, the priority for global supervisors was to address systemic issues across international markets and the often-accompanying lack of executive accountability. Now they must decide how best to regulate the new systemic risk presented by the adoption of new technologies, the impact of FinTech on the financial services sector and new nonfinancial market entrants.


Regulators will be looking into a number of issues, such as how they are set up to supervise, and how and what they are supervising. This may lead to a greater insistence on end-to-end chain management so that accountability is not outsourced, and may be a modification of the regulatory perimeter. The latter will depend on whether there is sufficient change to market business models to suggest that significant activity is being conducted beyond the reach of existing supervision.

Alternatively, could there be a move toward activity-based regulation? The extent of the

perimeter is often a result of the scope and type of institutions that national authorities want to capture. Traditionally that has centered on banks, brokers, insurers, asset managers, advisors and various combinations of these. However, in an industry that has seen a paradigm shift in the composition of its participants, with boundaries between regulated and unregulated activities becoming more blurred, a modified approach may be needed.

Historically, some jurisdictions have prioritized the identification of activities as the basis for their scope of regulation, although usually this has been accompanied by a licensing system by type of institution. In the future, a more flexible and proportionate system could allow activities to be undertaken by a wider range of institutions with a calibrated set of applicable rules. These could be shaped appropriately to new entrants depending on whether their role is as a service provider or a provider of services to incumbents. For example, new technology and data giants may be subject to certain conduct, governance and transparency requirements that previously applied only to the traditional financial sector.





2 Challenges for industry participants: legacy issues and evolving risks

Legacy issues: prudential agenda and post-crisis implementation

The largest banks in the world have significantly improved their capital and liquidity position since the crisis. The finalization of Basel III will continue, with a focus on assessing its impact rather than issuing further reforms on capital and liquidity. However, there is still some distance to travel. In terms of the fundamental review of the trading book for example, market risk models and systems will be overhauled, and the costs are difficult to quantify against the backdrop of uncertainty about final outcomes and possible non-uniform implementation in key jurisdictions. Cost and effort are likely to be substantial and may result in a move away from modeled approaches for all but the largest banks. For smaller institutions with more proportionate regimes, there may be different opinions on the criteria for determining what small and less complex means.

There has also been progress on major systemic risk issues of resolution and derivative market transparency, but of course there are still areas to address. Total loss-absorbing capacity and central counterparty clearing will be among the structural issues that continue to pose challenges to institutions and markets in 2019. A key question for governments and regulators is how to balance the time and effort devoted to fine-tuning the legacy risk agenda with the need to focus on new challenges such as cyber risk, operational resilience and data privacy. It would be

unfortunate if lack of attention to the new risk agenda resulted in an unforeseen major disruptive event while firms were focused on finalizing the last vestiges of the previous one.

Evolving risks: new issues on the radar

Banks need to manage and anticipate emerging risks. Digital transformation will help, but as our latest annual risk survey highlights, risk managers must quicken the pace at which they embrace and deploy new technologies.³ New tools and processes may provide substantial efficiencies and improve risk oversight if bank management and supervisors can become comfortable with their utilization as part of the overall business journey to digital transformation. We describe below some of the other journeys that firms must make in structures and processes, governance and controls, data management and protection, conduct risk and sustainable finance.

► New structures, new processes

With fundamental structural regulatory reform measures largely in place, the ongoing challenge is to make recovery and resolution work in practice, and validate that financial institutions meet expectations for operational continuity in resolution. And while regulators previously focused on resilience in extreme conditions, more attention is now being paid to less extreme disruptions and on resiliency in business as usual.

³ "Ninth annual EY/IIF global bank risk management survey: Accelerating digital transformation," EY/IIF, October 2018.

Supervisors also are focusing on legacy issues which were on the radar without satisfactory conclusion, and which have been carried forward in the new landscape. For example, booking models have been a source of contention for some time. In 2018, the European Central Bank (ECB) outlined its expectations,⁴ which will require banks to address practices that are linked inextricably to operational resilience and business continuity issues, such as remote booking with third-country entities or branches. Regulators in Hong Kong also are reviewing the remote booking issue.

The shift to alternative reference rates (ARRs) is a fundamental part of global benchmark reform. In recent months, regulators in the US and UK have asked firms to provide board-approved summaries of their assessments of key main risks relating to the discontinuation of interbank offered rates (IBORs) and the transition to alternative benchmarks. Regulators expect firms to consider a wide range of scenarios and impacts, including quantification of their IBOR exposures.

The transition will be a significant effort over the next few years for firms that have extensive exposure to IBOR-linked products and contracts. Although this is a very specific technical development, it has an impact on many parts of the banking operation, from front office, treasury, lending, valuation and market risk to IT systems, accounting, finance, legal and compliance.

The journey to more efficient structures

For booking models, the challenge for firms is to reconcile the relevant operational drivers, including capital and liquidity efficiency, tax considerations, client preferences, Brexit and any relevant structural requirements, such as intermediate holding company implementation, while adhering to legal entity governance obligations and external scrutiny from regulators. In doing so, firms will have to allay supervisors' concerns that structures may be too artificial or opaque.

As for reference rates, the move from IBOR to ARR necessitates management of contract continuity and product viability risk together with robust governance, including identification of a senior manager responsible for overseeing the analysis required and implementation of transition plans.⁵

⁴ "Supervisory expectations on booking models," ECB, August 2018.

⁵ See also "End of an IBOR era: key transition challenges for the financial services industry," EY, April 2018.

► Governance and controls: Enhancing the framework

Governance and risk management: In the shifting post-crisis regulatory landscape, several trends have emerged in recent years to enhance the governance and risk management framework:

- The emergence of greater executive accountability measures in certain jurisdictions
- An evolution in the three-lines-of-defense framework, including the transfer of risk ownership and management responsibilities to the first line
- Heightened focus on risk culture
- A revised approach to risk appetite to include nonfinancial risks
- Greater use of data management, advanced analytics, artificial intelligence (AI) and robotics in compliance and risk monitoring

As a result, regulators now expect to see a framework that has a more integrated risk control function, and more robust independent challenge by the second and third lines, combined with a more developed internal audit role to allow it to independently review the risk appetite framework and overall risk governance.⁶

Operational resilience and cyber risk: For many years, supervisors have issued rules and guidelines on systems and controls, business continuity, contingency planning, IT security, cybersecurity and so on. However, the era of digital transformation has brought these issues into sharper focus with the increased threat of cyber attacks and the internal challenges of enhancing or replacing legacy IT systems. These systems and staff perpetuate different classifications, inconsistent risk measures and the inability to aggregate data, while new technologies and products test the effectiveness of existing processes.

To supplement existing rules and guidance, regulators are now turning their attention to specific measures to strengthen operational resilience. In the US, the Office of the Comptroller of the Currency and the Federal Reserve have identified operational resiliency and cybersecurity as priorities in their 2019 bank supervision programs. In terms of cyber resilience specifically, the December 2018 Basel Committee report will be a guideline for future standards.⁷

Risk management frameworks typically focus primarily on the resilience of individual systems and processes, but UK authorities have challenged

To supplement existing rules and guidance, regulators are now turning their attention to specific measures to strengthen operational resilience.

⁶ See also "Ninth annual EY/IIF global bank risk management survey: Accelerating digital transformation," EY/IIF, October 2018.

⁷ "Cyber-resilience: range of practices," Basel Committee on Banking Supervision (BCBS), December 2018.

firms to improve their approach to end-to-end mapping of critical business services (including vendor resiliency), and to better align it to their operational risk frameworks.⁸ In terms of measurement and assessment, regulatory attention is likely to move toward enhanced stress-testing standards considering resilience, impact tolerances (including impact on end customers) and refining performance metrics.

Third-party risk management: This is another issue rising to the top of the priority list. As firms seek ways to reduce costs, outsourcing and the use of vendor services and cloud computing are now significantly more fundamental to their operations – making the need for a robust third-party risk management framework more essential than ever before.

Consequently, regulators are becoming concerned about financial institutions' increasing reliance on service providers to support some of their critical infrastructure, the use of the same providers by too many financial institutions, and the widespread use of the cloud. This is a new systemic concentration risk, which supervisors have yet to fully address. The recent UK paper⁹ is an early indicator of what supervisors' expectations will be, such as the requirement that outsourced providers meet the same requirements as internally provided services. Final guidelines on outsourcing also are expected from the European Banking Authority (EBA) in 2019.¹⁰

⁸ "Building the UK financial sector's operational resilience," Bank of England (BoE), Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA), July 2018.

⁹ "Building the UK financial sector's operational resilience," PRA, BoE and FCA, July 2018.

¹⁰ "EBA Draft Guidelines on Outsourcing Arrangements," European Banking Authority, June 2018.



The journey to enhanced governance and resilience

In risk governance, front-office staff need to be more fully trained on risk, and compliance officers are being called on to advise and support development of the control function on the front line. The second- and third-line control functions also must evolve and make greater use of new techniques and technologies. We have been exploring these challenges in our series of papers on regulation and technology-enabled innovation,¹¹ and we will discuss the implications for risk management in more depth in 2019.

Regulators will expect banks to position operational resilience squarely as a boardroom priority, alongside financial resilience. This is critical to enable the business to take greater ownership of resiliency preparation and oversight. Boards are reviewing resiliency, but have not yet tackled the full breadth and depth of the issue. Where they specifically focus on operational resilience, it is typically through a cyber or technology resilience lens or by looking at third-party dependencies. Some boards have not yet recruited directors with the necessary skills and capabilities to provide oversight and effective challenge. Boards will need to drive a cultural shift in their firms to consider the topic more holistically and move to a mind-set of: “This is very likely to happen, so let’s be prepared.” Key actions to strengthen operational resilience, both in-house and in using third-party vendors (especially as regards cyber risks), include:¹²

1. Establishing appropriate governance frameworks for resilience, with appropriate accountabilities and reporting lines
2. Identifying and assessing both the impact of and potential mitigants to potential resiliency threats
3. Designing and maintaining contingency plans to address any issues arising
4. Testing of processes/technologies for day to day resiliency as well as under stress conditions, including the efficacy of any contingency plans

In terms of third-party risk, firms still tend to undertake resilience testing without involving the key third parties they may depend on. This is an increasingly significant omission given their rapidly growing reliance on outsourced services, or on other parts of the organization in the case of larger groups. Many of the new service providers are operating in a partly regulated or unregulated space. What is their operational resilience capability? An end-to-end business services view of resilience is essential. Management should acquire a good understanding of the end-to-end capabilities and vulnerabilities of the operating environment, with regular updates provided to the board.

¹¹ “How can regulation keep up as technological innovation races ahead?,” EY, July 2018.

¹² See also “Getting serious about resilience: a multiyear journey ahead,” EY, 2018.

► Managing and protecting data are priorities

Regulators have made it clear that data is high on their agenda, and they will be increasingly demanding on this front, with more frequent and detailed reporting and ad-hoc investigations. The CEO of the UK Financial Conduct Authority (FCA), Andrew Bailey, has said; *“My assessment based on events over the last year or so is that data issues have been the fastest-rising risk on our landscape.”*¹³

Data management needs further work: Banking is a data-reliant industry. Banks require timely, accurate and meaningful data, and these requirements are equally important for supervisors, clients and markets. Clients are expecting user-friendly communication tools, and marketing departments are calling for more smart data. Investors and the wider market require greater access and transparency. All of this necessitates a more strategic approach for data governance and management. The BCBS Principles for effective risk data aggregation and risk reporting (BCBS 239), released in January 2013, were designed to generate an uplift in data quality and management, but this remains an area of focus for supervisors. There is still work to be done, as further automation of the middle and back office has the potential to be quite transformative.

Data privacy in sharp focus: Looking ahead, banks will not only have to better manage data, but also contend with more stringent demands for data privacy. The General Data Protection Regulation has been in force across the European Union since May 2018, and more data privacy regulation will surely follow in other parts of the world.

At the same time, open banking initiatives are taking hold in many jurisdictions, creating an immediate tension between data access and data protection, and raising questions around liability for data breaches. The regulatory perimeter issues mentioned earlier are brought into sharp focus, because financial firms providing data to third parties generally retain much of the privacy and security risks associated with how it is used, but do not benefit from any reciprocal obligation for those third parties to share their own data.

This area of regulation is essential to allow the customer to control their personal data, which will mean approaching the challenges somewhat differently in order to safeguard public policy objectives. If data privacy regulation becomes too onerous, it could compromise open banking or act as an effective barrier to entry for new participants. How regulators manage this trade-off between security and openness will be a crucial part of data regulation.

¹³ “Speech by Andrew Bailey at the Annual Public Meeting of the FCA, September 2018.

The journey to strategic and compliant data management

Significant investments have been made in storage and accessibility, but challenges in data stewardship still remain. Data architecture must be designed to harness data not just for regulatory and risk control purposes, but also to create increased analytical capabilities. The key steps to push through now are risk alignment, standardization of processes and aggregation of data from multiple sources. Machine learning, AI and Natural Language Processing can help to integrate customer, transaction and risk management data to support decision-making processes, but their application must be accompanied by the necessary enhancements in data lineage governance, data ethics standards, including ethics, and overall accountability for their use.

The old refrain of “let the data officer deal with that” is no longer a sufficient response. Institutions will have to develop an integrated data privacy framework with full risk management disciplines of assessment, tolerance, testing, metrics and monitoring with escalation up to board level, supported by entity-wide training and awareness programs. As part of the shifting risk ownership towards the first line of defense, data privacy should be embedded in business-line thinking.



► **Conduct risk and financial crime are constant threats**

Misconduct issues abound: Conduct risk is a perennial challenge, although at any point in time, there may be particular issues that take center stage. Regulators are as preoccupied as ever with misconduct issues, and the stream of enforcement cases in different jurisdictions shows little sign of abating anytime soon.

However, the message from the regulator that accompanies many of those cases is that the implementation of accountability regimes has made it easier to bring action and impose disciplinary measures. Initiatives to improve culture and ethics in the industry can go so far, but will have limited impact without a framework for accountability and enforcement to back them. For example, in Australia the Royal Commission Interim Report¹⁴ has been published at a time when the Banking Executive Accountability Regime (BEAR) has just been implemented. Initiatives such as BEAR will play a key role in addressing drivers of misconduct, such as incentive schemes linked to sales targets, conflicts of interest, ill-designed remuneration structures and absence of deterrent action.

In countries such as the UK, where the Senior Managers Regime has been in place for a little longer, there is evidence that practitioners accept its value in improving internal governance and making the job of compliance and risk management easier. Ultimately, the behavioral change that these regimes will drive will be determined by initial enforcement cases and perceived reasonableness of the regime in practice.

Regulators are as preoccupied as ever with misconduct issues, and the stream of enforcement cases shows little sign of abating.

¹⁴ Interim Report, The Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry, September 2018.

The journey to better conduct and crime detection

The challenge for the conduct agenda now is to move from setting the tone from the top to embedding positive culture and behavior throughout the firm. The recent report by the Group of Thirty emphasizes that *“Middle management in particular plays an integral role in embedding cultural reforms. Leading by example and ensuring that day-to-day activities at the front line are consistently aligned with company values is critical.”*¹⁵ Firms that apply such rigor will be better placed to drive positive change across their organizations.

In recent years, huge figures have been incurred – both in terms of costs and staff numbers – by firms responding to deficiencies in financial crime detection. This is the area with the greatest potential to leverage advanced technologies. It is now essential to make processes more efficient via the use of AI and machine learning in both client profiling and smarter transaction surveillance.

Financial crime is an ongoing threat: The fight against financial crime continues to be a global priority. In Europe, the EBA has published several regulatory technical standards on anti-money laundering and counter-financing of terrorism issues. The efficiency of national supervisors will be under scrutiny. No doubt this will mean increased pressure on financial institutions, which already have to deal with more complex sanctions regimes and increasing requirements to identify tax avoidance. In addition, the process of proper due diligence and risk assessment may lead to the unintended consequence of under-banked sectors, particularly in correspondent banking.

Sustainable finance – a new risk dimension: The demand for accountability is not only reaching deeper, but is also broadening in scope. Environmental, social and governance (ESG) issues, and in particular the sustainable finance agenda, will become a key element in firms' strategic planning and risk profiling. The September 2018 report by the Task Force on Climate-related Financial Disclosures noted that *“...the majority of the firms surveyed disclose information aligned with ... recommended disclosures.”*¹⁶ The disclosures so far vary in scope and quality, mainly describing climate-related risks and integration into risk modeling, rather than the financial impact on the company itself. A more prescriptive approach may be the next step, including possible inclusion of ESG in supervisory evaluations and stress testing. Regulators will be taking the proposals further in 2019.

¹⁵ “Banking Conduct and Culture: A Permanent Mindset Change,” remarks by Group of 30 Steering Committee Vice-Chair Gail Kelly, November 2018.

¹⁶ “Task Force on Climate-related Financial Disclosures: Status Report” FSB, September 2018.

3 The journey to a healthy risk and compliance framework

Change will be needed throughout and across entities, groups and their vendors. But it can and should be driven from the top.

At board level, greater diversity is becoming not just a regulatory expectation, but an operational necessity. Now boards must include individuals who understand not just financial risks and regulation, but also IT; models; KPI, MI and metrics; cyber; resilience; third-party risk management; financial crime; accountability; and the evolving agendas of technology and sustainable finance. The upside of executive focus on these challenges is the opportunity to break down silos and inject more skill diversity into corporate governance and risk oversight.

At a management level, now is the time to review and enhance:

- ▶ Operational committees, to deliver representative governance
- ▶ Risk frameworks, to achieve greater alignment and improved data quality
- ▶ New business and product approval mechanisms, to facilitate sound market and customer outcomes

The aim is to get the right stakeholders at the table to evaluate the risk implications on an end-to-end basis of operational, strategic and business decisions across the value chain, including the product life cycle, marketing, client segmentation, pricing and remuneration.

If boards and senior management take care not to underestimate the importance of legacy issues, become proactive about the future, build the right skills and develop new ways of working, they can deliver more agile and efficient risk and compliance frameworks equipped with the latest technologies, and new roles with new skill sets.

Boards and senior management can deliver more agile and efficient risk and compliance frameworks.

Further reading

"Ninth annual EY/IIF global bank risk management survey: Accelerating digital transformation" EY/IIF, October 2018.

"How can Regulation keep up as Technological Innovation Races Ahead?" EY, July 2018.

"As technology moves ahead, are utilities the upgrade you need?" EY, October 2018.

"As technology advances, will accountability be a casualty?" EY, December 2018.

"End of an IBOR era: key transition challenges for the financial services industry" EY, April 2018.

"Getting serious about resilience: a multiyear journey ahead" EY, 2018.

"EY's response to 'Building the UK financial sector's operational resilience'" EY, 2018.

"What's after what's next? The upside of disruption" EY, 2018.

"Fintech ecosystem playbook" EY, November 2018.

For more information, contact the authors of this report:



Michael Parker
EY Global Regulatory Analyst
Ernst & Young LLP (UK)
+44 20 7806 9617
mparker4@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
Executive Director, Financial Services, Asia-Pacific Regulatory Services
Ernst & Young LLP (HK)
+852 2849 9470
eugene.goyne@hk.ey.com

EY Global Regulatory Network executive team previous appointments

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 International Monetary Fund.

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.

Kentaro Kobayashi

kentaro.kobayashi@jp.ey.com

He spent 37 years as a financial regulator. He held positions in the National Tax Agency and later, Ministry of Finance (MOF), Japan's former financial regulator. After the establishment of the Financial Supervisory Agency (FSA) of Japan in 1998, he served as Chief Inspector and Inspection Administrator and continued to serve in this role after the FSA was reorganized into the Japan Financial Services Agency in 2000.

Alejandro Latorre

alatorre@ey.com

He spent over 20 years at the Federal Reserve Bank of New York, encompassing experience in monetary policy, capital markets, and financial regulation. Alex was a senior supervisor for the U.S. operations of two large and systemically important Foreign Banking Organizations and was involved in many of the Federal Reserve's financial crisis management efforts.

EY Global Regulatory Network executive team previous appointments (continued)

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 changes 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.

About the EY Global Regulatory Network

The EY 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 the 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/bank-risk-regulation

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. For more information about our organization, please visit ey.com.

The views of third parties set out in this publication are not necessarily the views of the global EY organization or its member firms. Moreover, they should be seen in the context of the time they were made.

©2019 EYGM Limited. All Rights Reserved.

EYG no. 000082-19GbI

ED None

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.

