As technology advances, will accountability be a casualty?

As the application of technology increases, the accountability mandate must evolve to remain an essential part of the governance toolkit.

The better the question.
The better the answer.
The better the world works.

Building a better working world

As digital technologies become ever more integral to the provision of financial services, firms and regulators are having to come to grips with the way technology is changing their operations and relationships with other entities in the financial ecosystem, as well as with technology's effect on the risk environment.

Regulators and firms alike can be encouraged by the ways in which digital technologies can improve market oversight and the efficiency and effectiveness of their risk controls. But they must also be mindful of technology's potential to increase risk and rapidly propagate adverse outcomes across the entire market landscape.

Senior managers of regulated financial institutions, in particular, are examining how they should address the fast-changing risk environment so they can satisfy expanding regulatory expectations and contribute to the safety and stability of financial markets. Regulators will require them to demonstrate that the risk controls they have put in place in their own operations, as well as those performed by third-party providers, are adequate; they also must demonstrate that they can mitigate the risk of adverse outcomes as those operations become increasingly automated. In a recent speech, the UK Financial Conduct Authority (FCA) Chair, Charles Randell, issued a warning: "There's also a danger that the use of technology will degrade people's willingness to judge and intervene, because they feel that they are less personally connected to consumers and consumer outcomes — the logic of the machine has taken over from individual responsibility."[1] The increase in the application of technology, together with a reduction in human intervention, therefore only emphasizes the importance of fulfilling the accountability mandate.

In this paper, we set out to explore how the more familiar ideas of accountability that have existed and evolved in the post-crisis era are now being reassessed in the wake of technological transformation. Starting with a firm's management and control structures, we then examine the issues around innovation and deployment, and, going beyond the institution itself, in terms of relationships with vendor services and infrastructure providers.

The increase in the application of technology, together with a reduction in human intervention, therefore only emphasizes the importance of fulfilling the accountability mandate.

[1] *"How can we ensure that Big Data does not make us prisoners of technology?"* FCA, July 2018.

Accountability regimes under review

Regulators in key jurisdictions, including Australia, Hong Kong, Singapore and the US, are following the lead of the UK Senior Managers Regime and have implemented, or are developing, regimes that seek to allocate greater individual accountability for risk, compliance and governance to senior management. Such regimes naturally include technology risk, so another trend is for specific guidelines to apply, such as those of the Hong Kong Monetary Authority (HKMA)[2] and the Monetary Authority of Singapore (MAS).[3] The MAS emphasizes that the "board of directors and senior management should ensure that a sound and robust technology risk management framework is established and maintained."

Notably, the UK Prudential Regulation Authority (PRA) has defined the specific roles within regulated entities that are accountable for algorithms and specified the extent to which the boards of regulated institutions are to be held responsible for their use.[4] These responsibilities include approval, testing, deployment, documentation and audit.

It is expected that a firm's governing body or, where applicable, its risk committee should set the governance framework for the firm's use of new technologies, as well as define responsibilities for approval and oversight. In practical terms, duties may be allocated or delegated based on expertise, for example, to the IT, risk and business/product development committees, but this should always be within the parameters of the overall risk management framework established by the board. The traditional three-lines-of-defense model (3LoD) is seeing a shift of risk management toward the first line, so it is essential to include accountability for use of new technology given that applications of FinTech tend to be developed more rapidly in the revenue-generating parts of a firm.

In the 2017 edition of our annual global bank management survey, EY professionals and the Institute of International Finance (IIF) observed that, although institutions have moved significant resources to the first line to support business-leader accountability, the tougher challenge is in making the new model effective and efficient. Much of that challenge lies in the introduction of new technology and the corresponding need to develop a new control framework and communicate clearly its operation and oversight. "Regulators and boards will want strong evidence that risk management and controls remain robust … they will want to know risk management is faster and smarter, not simply cheaper."[5]

Regulators face challenges too. They are conscious of the potential gains from innovation and want to deliver a welcoming environment, such as a sandbox, while being cognizant of the potential risks. However, their closer involvement in assessing part of a firm's business model in the sandbox raises the question of the extent to which they could subsequently take supervisory or enforcement action related to activities previously tested. Holding a firm accountable could be more difficult if the feedback received in a testing environment were highly positive, akin to approval, or felt like advice or guidance from the regulator to the firm.

[2] *"General Principles for Technology Risk Management,"* HKMA Supervisory Policy Manual module TM-G-1.

[3] *"Technology Risk Management Guidelines,"* MAS, June 2013.

[4] *"Algorithmic Trading: Supervisory Statement 5/18,"* PRA, June 2018.

[5] *"Restore, rationalize and reinvent: A fundamental shift in the way banks manage risk,"* EY/IIF, October 2017.

Black box or black hole?

A robust technology risk management framework may deliver the necessary governance structure, but at the level of individual processes and applications, there are still significant challenges. The workings of the most advanced decision-making technologies are anything but transparent, and even experts are challenged to understand the logic governing some machine-generated decisions.

Regulators are now including requirements to deliver accountability in the first phase of rulemaking addressing the digital agenda. Article 22 of the EU General Data Protection Regulation (GDPR) contains a "right to an explanation" provision. This provision gives an individual, when they have been subject to fully automated decision-making (and where the outcome has a significant impact on them), the right to ask for an explanation as to how that decision was reached or to ask for a human to make the decision. This would appear to create an immediate problem for black box, artificial intelligence and machine learning technology, since transparency and explainability still remain difficult to achieve.

In its 2018 paper on machine learning models,[6] the Future of Privacy Forum explained how the 3LoD model could be applied to help address the issue of explainability, i.e., by using specialist personnel in key roles across the 3LoD to take responsibility for data, applying subject-matter expertise and, most crucially for accountability, delivering robust challenge and validation disciplines. In an environment where machines are increasingly developing themselves, the oversight challenge for management becomes exponentially more difficult; therefore, the evolution of the skill set in the 3LoD seems inevitable.

New recruits to the 3LoD:

Data owners: responsible for the data used by the models; often referred to as "database administrators," "data engineers" or "data stewards"

Data scientists: create and maintain models

Domain experts: possess subject-matter expertise about the problem the model is being used to solve; also known as "business owners"

Validators: review and approve the work created by both data owners and data scientists, with a focus on technical accuracy; oftentimes, validators are data scientists who are not associated with the specific model or project at hand

Governance personnel: review and approve the work created by both data owners and data scientists, with a focus on legal risk

From "Beyond Explainability," Future of Privacy Forum, June 2018

[6] *"Beyond Explainability: A Practical Guide to Managing Risk in Machine Learning Models,"* Future of Privacy Forum, June 2018.

In the same vein, a recent EY report suggests steps firms can take to make sure that they are accountable for, and build trust into, the AI systems they deploy.[7] Institutions should take a holistic approach to those systems by taking into consideration not just their business and technological implications, but also their broader ethical, social, environmental and regulatory impacts — and should do so across their life cycles, from design to implementation, and to continuous monitoring as the systems themselves learn and evolve. The explainability requirement is central to this approach because it requires that firms have a strong grasp of how the system functions and evolves, as well as clearly defined lines of accountability. Leading tactics that institutions are using to achieve this level of accountability for AI systems include putting in place robust policies and standards specific to AI development, using validation tools, conducting regular inventories and commissioning independent audits to confirm all AI algorithms are properly governed and perform as intended.

For financial market participants, this may be a significant step up in terms of the level of rigorous analysis being applied, especially in business areas. However, it seems necessary and even inevitable to enable proper demonstration of the key elements of accountability for technological transformation: data assessment, rigorous monitoring, sophisticated back testing, exposure of bias and evaluation of trade-offs between explainability and accuracy.

In an environment where machines are increasingly developing themselves, the oversight challenge for management becomes exponentially more difficult; therefore, the evolution of the skill set in the 3LoD seems inevitable.

[7] *"How do you teach AI the value of trust?"* EYGM Limited, September 2018.

Reassessing third-party relationships

Senior managers are reviewing their relationships with third-party providers and scouring service contracts to verify that the third party's obligations are clearly defined and that third parties demonstrate that their operations have appropriate risk controls and governance in place. In many cases, financial services institutions are requiring vendors to allow audit firms to objectively validate — via SSAE 16 audits and resulting SOC1 reports, for example — that the vendors are in compliance with their risk-control obligations. Such reviews do not shift accountability or reputational risk, which in all cases resides with the regulated entity, but they help ensure that financial firms will deploy robust due diligence, ongoing monitoring and "right of audit" over third-party activities to demonstrate adequate oversight and effective risk management.

Regulators themselves are working to gather information about the connectivity among different financial institutions, as well as about their overall exposure to specific sectors, geographies and individual institutions, and, in particular, in testing more rigorously how interconnectedness works in a crisis or addresses failure of one part of a chain. The upcoming implementation of the operational continuity in resolution (OCIR) requirements in the UK[8] marks the first delivery among global supervisors of previously issued guidance of the Financial Stability Board (FSB).[9]

For this effort to succeed in exposing and managing systemic risks, key players in the marketplace will need to invest in documenting core processes from end to end, especially when they cross institutional boundaries. Doing so will enable regulators to define accountability for specific process components and show clearly where and when the handoffs between institutions occur. Although such mapping can be an onerous task, many senior leaders have discovered the value of closely monitoring the process risks for which they or their firms are accountable and determining how information needs to be shared with other players in the process chain, as well as with regulators.

In the meantime, regulators are recognizing the need to update the existing requirements applying to regulated outsourcing institutions. In its recent report on innovation in the financial sector,[10] the US Treasury made a number of recommendations, including "... setting clear and appropriately tailored expectations for chain outsourcing ... ," while the European Banking Authority (EBA) recommendations on outsourcing to the cloud took effect on July 1, 2018.[11]

For a more detailed look at the issues arising in shared services and utilities, see the EY paper "As technology moves ahead, are utilities the upgrade you need?"

To expose and manage systemic risks, key market players will need to document core, end-to-end processes.

[8] *"Ensuring Operational Continuity in Resolution: Reporting Requirements,"* PRA, April 2017.

[9] *"Guidance on Arrangements to Support Operational Continuity in Resolution,"* FSB, August 2016.

[10] *"A Financial System That Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation,"* US Treasury, July 2018.

[11] *"Recommendations on Outsourcing to Cloud Service Providers: Final Report,"* EBA, December 2017.

New systemic risks emerge

Holding management of regulated institutions accountable for their own and their vendors' operations is not in itself a comprehensive defense against systemic risk. Consider how cloud services, in a short span of time, have become deeply embedded in the financial services infrastructure. Regulated entities may be accountable for data breaches or service outages at their cloud provider, but holding a senior manager personally accountable for the failure does little to mitigate systemic risk or financial losses.

Recognizing these challenges, regulators are looking more closely at risks across the sector. In the UK, the Bank of England (BoE), PRA and FCA are consulting on how to improve the operational resilience of firms and financial market infrastructures, including how they would respond in the event of systemically significant failures.[12] In Europe, the EBA has launched a consultation[13] seeking to update and harmonize outsourcing guidelines across the EU. The authority proposes that firms maintain a register of all outsourcing arrangements and submit to regulators more comprehensive information on the outsourcing of critical functions to identify concentrations on a market level along with an overriding obligation on the management body to establish an appropriate framework for outsourcing.

Regulators are also considering whether the scale of operations that are outsourced to the cloud and/or onward via chain outsourcing has reached the point where the zone of accountability needs to be extended to include infrastructure providers. Some market observers are asking whether regulators should require key infrastructure providers to at least disclose their business continuity plans and maintain a prescribed level of operational capital, as is the case for firms inside the regulatory perimeter. Legislation aimed at various aspects of data protection and data sharing, such as the EU GDPR and the US Clarifying Lawful Use of Overseas Data (CLOUD) Act, already impose obligations on remote computing and cloud storage services. Regulators in some jurisdictions, including the Office of the Comptroller of the Currency (OCC) in the US and the Commission de Surveillance du Secteur Financier (CSSF) in Luxembourg, have in their charters the authority to regulate non-financial infrastructure providers but to date have not exercised that authority.

Regardless of whether the regulatory perimeter is extended, however, the obligation is on senior financial services managers to demonstrate that they have comprehensive knowledge of their business processes and understand which process components with their associated risks remain directly under their control and which risks are under the day-to-day control of another organization or a decision-making algorithm.

[12] *"DP 18/4: Building the UK Financial Sector's Operational Resilience,"* BoE/PRA/FCA, July 2018.

[13] *"Consultation on Draft Guidelines on Outsourcing,"* EBA, June 2018.

Summing up

Senior managers are reviewing their relationships. The accountability obligation is "technology-neutral"; whether in the case of a dealer using the latest trading algorithm or a stockbroker stacking buy and sell orders on the desk, the obligation to achieve proper customer outcomes — such as achieving best execution or making an appropriate investment recommendation — still applies, and executives are still accountable for compliance with those requirements.

But assessing that compliance requires a new toolkit. Traditional lines of reporting, sign-off, approval committees and the like must be enhanced, and new structures are needed to deal with digital transformation. We see several key areas where accountability can be enhanced.

Governance, risk and controls: setting the framework for the use of new technologies — Risk frameworks need to go beyond governance, approval, oversight and monitoring. As machines increasingly take on decision-making roles, accountability for adverse outcomes needs to be clarified and documented. So, too, do approaches to investigating adverse events and communicating the lessons learned from them. As technology drives lightning-fast processes with errors potentially occurring at a similar rate, it is vital that the response mechanisms can keep up.

Risk transformation: making sure that accountability is embedded in risk control improvements in the 3LoD model — In last year's risk survey,[14] EY professionals and the IIF showed that the industry is on a post-crisis risk management journey and has entered a phase of rationalization leading to reinvention, where success in dealing with technological transformation will be a major goal. The survey highlighted several key areas that also make a crucial contribution to the accountability obligation:

- Embedding balanced risk-taking and risk discipline into businesses
- A digital transformation of risk management; enabling risk management through automation, machine learning and artificial intelligence
- The 3LoD model; developing its operation and roles

Enterprise protection: documenting responsibilities and implementing contingency planning across outsourced activities — Regulators are not yet inclined to be prescriptive about the specific contractual arrangements between an institution and its service providers, but that may change if problems arise from service-level agreements that are incomplete or poorly enforced, especially if such issues become systemic. Comprehensive documentation that clearly allocates responsibility is not only good practice, but essential, and the latest EBA guidelines recommend that such records be available to the regulator.[15]

Also, institutions may give extended consideration to an outsourcing but may not pay enough attention to a change or exit strategy. This must not be underestimated, given evolving outsourcing models and arising complexities involving the use of technology (cloud, analytics, data lakes, etc.).

[14] *"Restore, rationalize and reinvent: A fundamental shift in the way banks manage risk,"* EY/IIF, October 2017.

[15] *"Recommendations on Outsourcing to Cloud Service Providers: Final Report,"* EBA, December 2017.

Technology disrupters: applying technology to enhance accountability – Maybe the technology itself can help to deliver a greater level of accountability than has been embedded in systems and processes up until now. In a recent speech, the Managing Director of the MAS, Ravi Menon, acknowledged that "Cloud computing has considerably enhanced risk management. Risk assessments are now more comprehensive, more granular and more real-time."[16]

There are opportunities that could be explored, resources permitting. For example, in a recent market study, the UK FCA concluded that many "direct-to-consumer" (D2C) investment platforms lack effective best-execution monitoring and thus raise the prospect of noncompliance with basic investor protections.[17] It would seem that the integration, if possible, of enhanced monitoring capability could strengthen the integrity of the platform and help management demonstrate greater oversight of the product and how it reinforces positive outcomes for customers. In cases such as this, the tangible cost of development may well be outweighed by the less-tangible benefit of more demonstrable product accountability together with future fines for rule breaches being avoided.

Traditional lines of reporting, sign-off, approval committees and the like must be enhanced, and new structures are needed to deal with digital transformation. We see several key areas where accountability can be enhanced.

[16] *"Financial Regulation – 20 Years After the Global Financial Crisis,"* keynote address by Ravi Menon, Managing Director, MAS, at Symposium on Asian Banking and Finance, Federal Reserve Bank of San Francisco, 25 June 2018.

[17] *"Investment Platforms Market Study: Interim Report,"* FCA, July 2018.

Conclusion

The technological agenda has an unavoidable impact on the operating model and governance of the firm; the two are interconnected. Whatever response a firm makes to technological transformation, it must build in appropriate accountability, starting from the board and executive management and extending outward to:

1. Risk management and 3LoD
2. Deployment of machines, bots and black boxes
3. Relations with third-party providers
4. The cloud infrastructure
5. Customers and the public

For more information, contact the authors of this report:

Michael Parker
EY Global Regulatory Analyst
Ernst & Young LLP (UK)
+44 0 207 806 9617
mparker4@uk.ey.com

Kara Cauter
Partner, Financial Services
Ernst & Young LLP (UK)
+44 20 7197 7915
kara.cauter@uk.ey.com

Eugène Goyne
Executive Director, Financial Services, Asia-Pacific Regulatory Services
Ernst & Young LLP (HK)
+852 2849 9470
eugene.goyne@hk.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

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.

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.

Christian Lajoie
christian.lajoie@fr.ey.com
As former head of Group Prudential Affairs, BNP Paribas, Christian has broad banking experience and a deep understanding of the regulatory and supervisory impacts on bank management and strategy. In recent years, he played an active role in regulation-making, participating in many international forums, and also served as Vice Chair of the EBA Stakeholder Group.

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.

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

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/grn.

EYG no. 012562-18Gbl

ED None