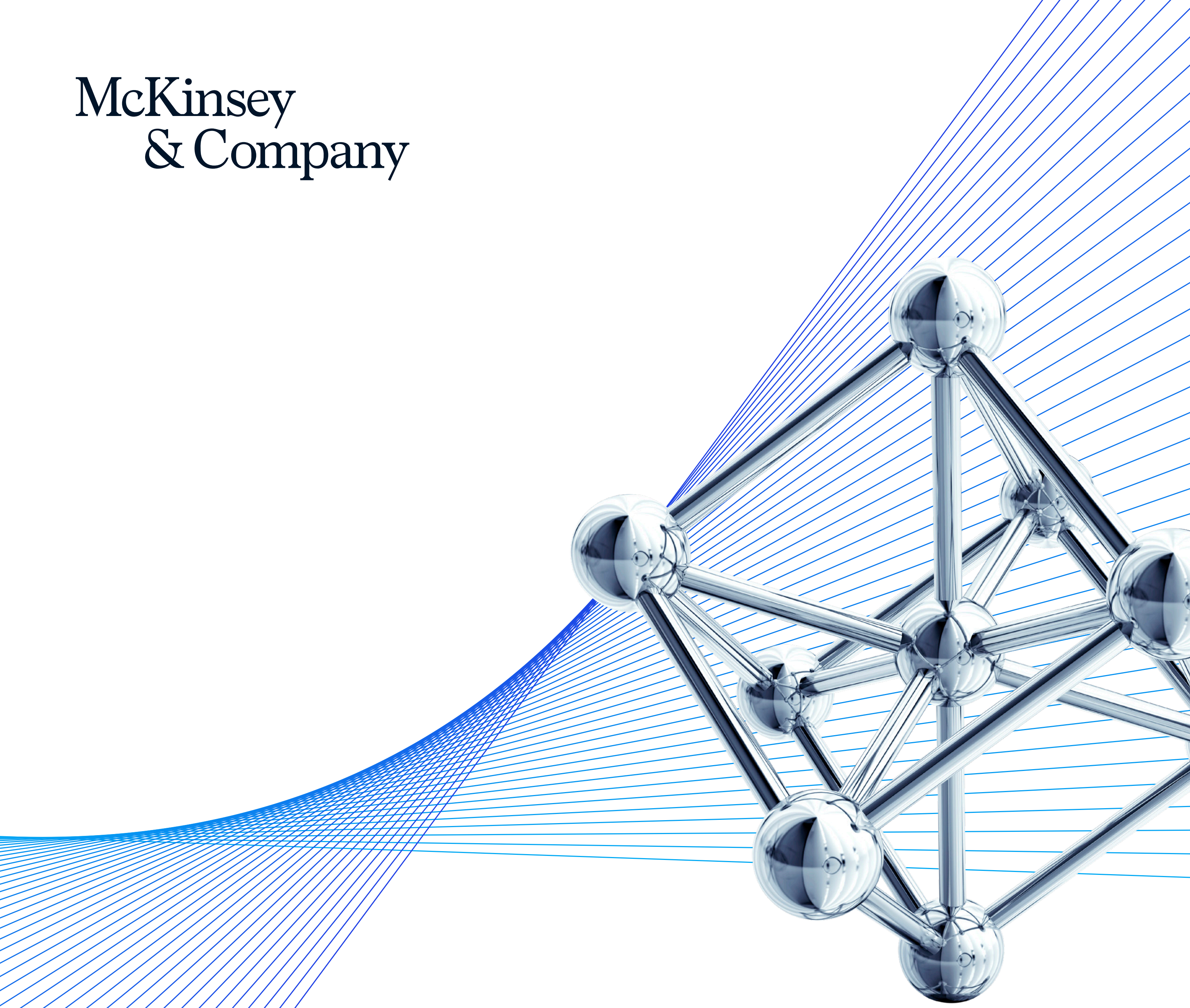
McKinsey & Company



Creating the bank enterprise risk management function of the future

March 2020

Creating the bank enterprise risk management function of the future

March 2020

Authors

Hans Helbekkmo, Cindy Levy. Olivia White

Originally published in the Journal of Risk Management in Financial Institutions, Volume 12, Number 4, Autumn/Fall 2019, Henry Stewart Publications, https://www.henrystewartpublications.com/jrm

Abstract

Banks today face an unprecedented pace of change and high uncertainty, dealing with significant threats ranging from bad employee behaviours to sophisticated cybercrime, trade wars and climate change.

These trends severely challenge the formulaic approaches to enterprise risk management (ERM) in place at many banks today. Our work supporting leading global banks convinces us that ERM functions must transform themselves, so they can guide their institutions through threats and opportunities while simultaneously meeting the expectations of all stakeholders. This paper discusses the abilities that the ERM function of the future will need, across three dimensions:

1. Delimiting the bank's appetite for risk taking: supporting banks to set limits on risk taking dynamically, accounting for the institution's values, strategy, skills, and competition.
2. Detecting new risks and weaknesses in controls: working with businesses and functions in an agile way to understand new threats and changes to existing ones.
3. Deciding on the risk management approach: implementing more agile governance processes and approaches to risk mitigation and controls.

Enhancing these abilities requires ERM to take four steps:

1. Define its own vision and mandate for creating value for the bank.
2. Shift its ways of working in core areas, with an agile approach that applies cross-functional teams and rapid decision making.
3. Set its responsibilities beyond the core in areas of risk management that benefit from transparency and coordination with businesses and functions.
4. Ensure the right ERM talent, with new capabilities and knowledge, including a better understanding of the business, digital innovations, and agile management.

Introduction

The unprecedented pace of change and high degree of uncertainty in the world today severely challenge more formulaic and stationary approaches to risk management. For banks and other financial institutions, significant threats have emerged from inside, outside and the world at large. These range from inappropriate or illegal employee behaviours to sophisticated cybercrime, trade wars and climate change. There is no reason to believe that these trends will abate.

As a result, risk functions must become more dynamic and flexible. They must help guide their organisations through a complex and volatile landscape of opportunities and threats, simultaneously meeting the evolving expectations of key stakeholders—regulators, legislators, shareholders, customers and the community at large.

We believe a cross-cutting enterprise risk management (ERM) function is central to accomplishing the needed change, complementing and working with groups focused on specific risk types and business groups. An ERM function can lead a bank in developing new and more proactive capabilities across traditional risk management activities, including delimiting the appetite for risk taking, detecting new risks and potential control weaknesses and dynamically deciding how to adjust the risk management approach.

This represents a fundamental shift in ERM as a discipline, which only a few years ago seemed to have reached maturity, based on concepts laid out in regulatory guidelines such as 'Heightened Standards'[1] and 'Enhanced Prudential Standards'.[2] ERM had its initial roots in the mid-1990s, when it operated as a catch-all category for a vague array of nonfinancial risks that were left uncovered by more established risk disciplines, including market, credit and interest rate risk. In 2004, the Basel II Accord introduced more analytical rigor to nonfinancial risk, linking statistical analysis of past losses to bank capital requirements. Nonetheless, ERM remained fundamentally backwards looking. It finally became a risk management discipline in its own right following the crisis of 2008. Since that time, ERM has been defined by enterprise-wide risk programmes such as risk appetite and risk identification, all subject to clear guidance and enforcement by regulators, but all still typically static and mechanical.

We believe ERM functions should take four steps to position themselves—and broader risk management—for future success. These include defining a vision and mandate for ERM as a discipline and as a function, building more agile approaches for risk management across the bank, setting the full scope of responsibilities owned by the ERM function and ensuring that ERM has the right internal talent.

The shifting landscape of opportunities and threats

The world is changing in fundamental ways, leading to dramatic change in the landscape of both opportunities and risks. We see three interrelated changes as particularly fundamental for banks. First, the digital revolution is drastically increasing the availability and use of data and the speed at which decisions are made.[3] Secondly, technological innovation is accelerating changes in the competitive and customer landscapes in which banks operate. Finally, hyperconnectivity is escalating the pace of information flow and reshaping how people think and act, affecting the nature of a bank's relationship with its customers and other stakeholders.[4]

These changes certainly present new opportunities for banks. For example, McKinsey Global Institute research suggests that, together, artificial intelligence (AI) and advanced analytics (AA) in banking could generate as much as US$1 trillion globally in annual economic value. AI and AA enable better, personalised understanding of customer needs and rapid ways to proactively meet these needs through targeted marketing and more effective customer interfaces.[5] Examples of opportunities linked to risk management include improvements in underwriting, fraud detection and trade surveillance. For example, more detailed underwriting models could allow banks to underwrite new types of customers, reaching people who are unbanked or only semi-banked today. They could also help bankers design optimal deal structures, including product offers and line assignment. Process automation offers the potential for dramatically faster and less error-prone processes. For instance, natural language processing can help automate labour-intensive tasks like reviewing customer complaints, legal contracts and suspicious activity reports.

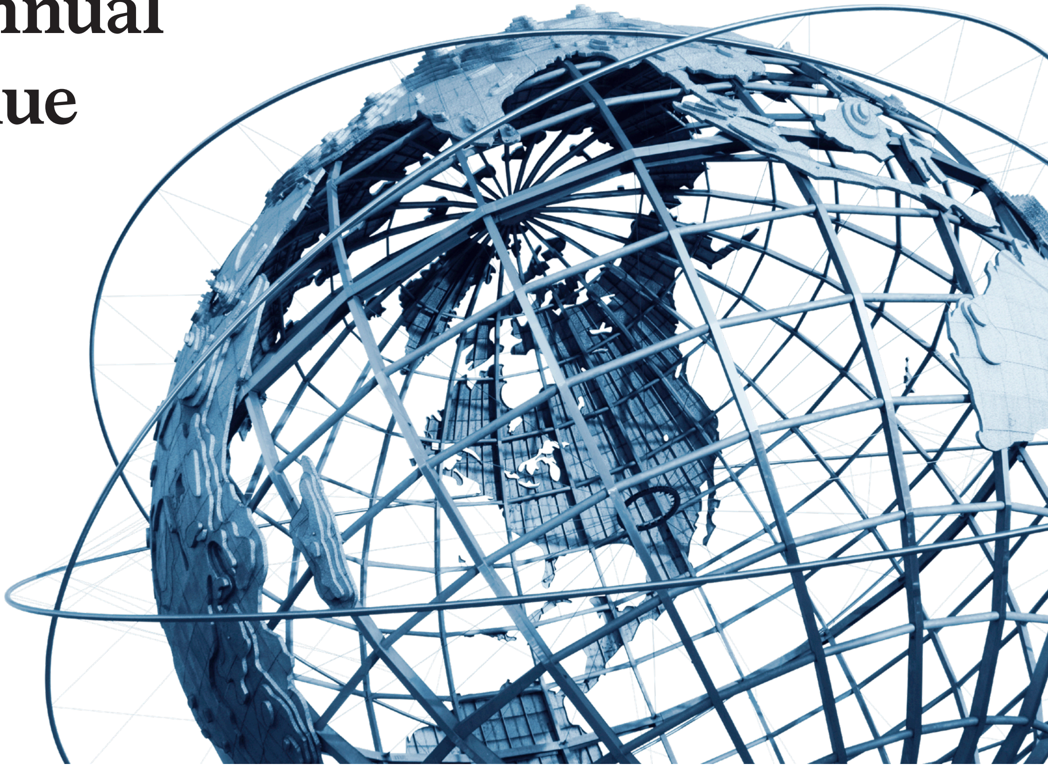
The fundamental changes we are seeing, however, also drive increased uncertainty and threats. For instance, AI and AA can trigger a host of unwanted, and sometimes serious, consequences including, privacy violations, erratic automated processes and discriminatory model outcomes. For banks, these challenges are new and are made even more difficult by the increased complexity of outsourced services and other third-party relationships. Because AI-fuelled analytics are a relatively new force in the digital universe, the full scope, nature and magnitude of their risks remain only partially understood.[6]

More broadly, society's increased use of data, reliance on technology and hyperconnectivity are changing the profile of nonfinancial risks that banks face. Banks have always had to deal with the potential for rare, severe events like a rogue trader or natural disaster. Today, while automation has markedly reduced cases of human error, technological advances have increased the pain that some isolated events can inflict. Examples of this include infrastructure failures (eg data centre incidents) model risk (eg trading decisions relying on flawed analytics[7]), financial crimes (eg synthetic identity fraud[8]) and data privacy violations (eg cyberattacks on insufficiently secured data[9]). Traditional, historically based loss analysis is insufficient for predicting or understanding such unlikely occurrences, which may have never happened before.

At the same time, the new normal of risk threats includes fundamental and irreversible change to banks' operating environment. Examples of potential shifts include FinTech (financial technology) disintermediation that reduces the value of customer relationships; new competitors that affect customer selection in ways that disrupt risk models or changing customer preferences that shorten deposit durations, affecting bank liquidity and rate sensitivity. Beyond technological change, the world's changing climate also presents a structural shift to banks' risk profile, increasing credit, market and operational risks[10]. It has irrevocably altered the considerations in underwriting certain risks—for example, financing of electric utilities, heavy producers or consumers of aluminium or real estate finance in coastal zones.

Another product of all this change is that when risk events occur, they can evolve and escalate rapidly. Expanded visibility for and evolving expectations of stakeholders amplify reputational risk impacts, whether due to standalone incidents, such as a rogue trader, or pervasive issues, such as a culture enabling sexual harassment or discrimination. As has been seen repeatedly and increasingly over the past decade, a sudden crisis can turn into a truly existential threat. Between 2010 and 2017, headlines with the word 'crisis' and the name of one of the top 100 companies as listed by Forbes appeared 80 per cent more often than in the previous decade.[11] The consequences are severe, including lost trust from poor interaction with customers and shareholders. The increased velocity of business decisions, reliance on complex analytics and heightened visibility to the public all contribute to an increased likelihood of crisis. Traditional, regimented and committee-based decision making can be unequal to keeping up with fast-changing risk events.

Banking could generate as much as US$1 trillion globally in annual economic value



Risk management's new capabilities

In the face of these threats, we believe that banks will need to develop new risk management capabilities of three sorts. They will need to significantly enhance their ability to delimit appetite for risk taking, detect both new potential risks and weaknesses in controls and decide on the appropriate action steps.

The ERM function's job can include defining the vision and support execution for doing so in a unified way across businesses and functions for all risk types. At institutions that already have ERM groups, this will be a natural extension of the group's traditional responsibilities, which include running enterprise programmes for risk identification and risk appetite and, typically, maintaining the enterprise inventory of risks and controls. Those institutions that traditionally have not had an ERM function should look to centralise the way they define their approaches for delimiting, detecting and deciding on the risk. This ERM group can help provide a unified and coordinated approach across the enterprise—in contrast to the more disjointed and regulatory-focused setup that some institutions still use to run enterprise risk programmes. In either case, the work will involve taking a fresh look at the bank's established programmes including those for risk identification, risk appetite and risk-based decision processes and exploring what gaps need to be filled to make sure the enterprise can manage risks with the appropriate oversight, speed and decisiveness.

Delimiting risk appetite

This encompasses setting limits on risk taking in a way that accounts for the bank's values, strategy, risk management capabilities and competitive environment. Today, most banks maintain relatively static, formal statements of risk appetite. These typically consist of aggregate metrics delimiting risk taking by risk type and business and sometimes also include qualitative statements.

The ERM function of the future will need to support banks to delimit risk taking dynamically, directly translating principles and metrics into a concrete view of what the bank will and will not do at any given time. The ERM function is uniquely positioned to do this in light of its comprehensive overview of risks across the enterprise and the understanding of which risks represent true constraints on risk taking, whether driven by financial capacity (constraints on capital and liquidity) or strategy (restrictions on customer segments and products). Furthermore, the ERM function's cross-cutting view of risk will enable it to make sure limits are set in a way that are inherently consistent across risk types (eg understanding how a strategic expansion into new market segments could require tighter limits on both credit and operational risks). Banks will need to be able to answer the following three questions:

Should we avoid any risks entirely?
Risk appetite statements of the past were frequently littered with lofty declarations about zero tolerance for certain types of risk—for example, legal and compliance-related risks. In the future, banks will need a much more realistic and definitive perspective on avoiding risks, based on a strong, objective fact base. For example, will risk drivers like climate change render risks in certain businesses fully untenable, such as real estate finance in certain coastal regions?[12] Or should the reputational risk of being caught on the wrong side of environmental and social responsibility drive the bank out of certain business segments altogether—for example, in the way some institutions have exited the business of financing weapons manufacturers?[13]

If this is a risk we are comfortable taking, how much should we take?
Historically, risk profiles of banks have tended to evolve organically, based on relatively static views of comparative advantage and comfort with predictable results. In the new world, rapidly changing customer behaviours, digital capabilities,

The work will involve taking a fresh look at the bank’s established programmes including those for risk identification, risk appetite and risk-based decision processes

competitive landscapes and broader global trends can quickly uproot established views on risk appetite. For example, many banks that categorically refused to use the cloud five years ago are migrating to cloud-based storage and software solutions today, driven by improved technology and security. Changing energy regulations could significantly increase the cost of energy production, reducing the value of reserves that collateralises bank loans.[14] As a more tangible example, lending secured by taxi medallions in New York was long considered a bullet-proof business model—until ride-sharing companies came along.[15]

Does our risk appetite adequately reflect our control effectiveness?
The increased threat of severe nonfinancial risks challenges the status quo of risk/return trade-offs. For example, advances in competitiveness and profitability of consumer businesses have relied on significant automation to speed up processes and reduce costs. At the same time, the risk of fraudulent attacks or violations of data privacy have increased dramatically. Thus, banks will need to rethink investments in control capabilities and adjust their risk appetite for businesses to reflect these evolving control requirements and their costs.

Detecting risks and control weaknesses

This encompasses the abilities to anticipate, predict and observe threats based on disparate internal and external data points as well as the ability to assess the magnitude of the risk and the duration of its impact. Banks need to detect new threats, of course. But they also must detect changes in existing threats due to shifts in underlying risk drivers or in internal control effectiveness. At most banks, these abilities have evolved over the past five years, driven by Comprehensive Capital Analysis and Review (CCAR) mandated 'risk identification' programmes. For the most part, however, banks have settled on a relatively static process to maintain and periodically update a risk inventory, which is primarily used to inform adverse scenarios used in stress testing.[16]

In the face of uncertainty and volatility, the ERM function of the future will require a much more agile and dynamic approach to risk detection, directly linked to business decision making and incident response. As the keeper of risk inventories and control assessments, ERM should have a good starting point understanding of pain points and weaknesses. ERM will need to build on this to make sure the bank can respond rapidly and systematically to new sources of risk and uncertainty. For example, ERM can take the lead in engaging with business and support functions to identify lessons learnt from past issues and control failures and leveraging this knowledge to anticipate how controls need to be updated to address new risks. Importantly, the ERM function possesses the requisite cross-cutting view of risks to ensure effective and comprehensive risk detection. For example, a bank that embarks on an aggressive growth strategy in consumer lending is potentially exposed to new sources of credit risk, driven by differences in the level of indebtedness and financial health of the new target customer segments compared to the current portfolio. At the same time, the expansion could increase the exposure to other risks such as synthetic identify fraud or reputational risk associated with increased risk of missteps in how new customer segments are handled (eg inadvertent discrimination in underwriting decisions). If the role of detecting these risks were handled in traditional risk silos, the bank might very well miss some of these cross-cutting effects. To adequately detect diverse and emerging risks and control weaknesses, we believe banks will need to be able to answer the following three questions:

What will happen in the future?
Institutions will need to cast a net wide enough to detect potential risks that have not yet occurred. Traditional risk taxonomies based on historically

observed losses are not going to be sufficient. For example, most institutions will not have historical losses linked to climate change, and many will not have encountered significant reputational blowback from being on the wrong side of a social issue. But such risks will certainly play an increasingly important role in the future. As a result, banks will need to develop a forwards-looking, comprehensive taxonomy of fundamental risk drivers. To make sure they shine lights in all the right corners, as well as around them, institutions will require a real-time view of these drivers based on internal performance metrics and external indicators, as well as an up-to-date view of what business leaders see in their day-to-day work.

What is the magnitude of the risk?
Banks need to think of magnitude not just in terms of direct financial impact but also incorporate reputational, regulatory and legal implications. The assessment should also consider how large the risk would become under a stress scenario or other changing conditions. For example, many banks have built in systematic assessment of nonfinancial risk associated with new products and new business initiatives. Importantly, a bank's judgment on the size of any particular risk should incorporate a realistic view of internal risk management capabilities, accounting for controls, tools and processes and the skills and knowledge the risk organisation can deploy.

How will the risk play out over time?
Some risks are slow moving, while others can change and escalate rapidly. Independent of speed, risks can be either cyclical and mean-reverting or structural and permanent. Historically, most banks have focused on managing cyclical, mean-reverting risks, such as credit risk. While losses have ebbed and flowed, the fundamental long-term economics of business lines have held firm, requiring only minor tweaks in underwriting policies through the cycle. The sorts of structural change present today require different approaches. For example, as FinTech innovators nibble away at banks' value chains, commercial lending might no longer be able to depend on fee income that brings a sufficient return on capital for the business. The right risk management approach will depend strongly on the time course of a risk.

Deciding on the risk management approach

This includes the ability to quickly decide what response a risk requires—whether immediate or more prolonged—to design and undertake that response or to mitigate it and to institute a feedback loop to track effectiveness. At many banks today, such decisions invariably run through linear committee-based governance processes and are rooted in policies and procedures, limiting the ability to respond immediately. In light of how quickly the world can change, banks need a greater ability to make decisions rapidly and assertively when they detect emerging risks or control weaknesses.

The ERM function of the future should help implement more agile governance processes and approaches to risk mitigation and controls. ERM can build upon a cross-cutting view of existing risk-based decision processes and ongoing engagement with key front-line stakeholders that occurs as part of risk detection and delimiting. The function should actively engage leaders from across the organisation to understand what mitigation and response efforts have worked well in the past—and which have not—so that it can evolve to manage risks in today's world. This involves answering three questions:

If we decide to take a risk, what mitigation should we have in place?
Historically, many institutions have relied heavily on manual controls as well as on judgmental assessment of control effectiveness, particularly for nonfinancial risks. This approach can simultaneously generate excess costly layers of controls in some areas, while leaving gaps or insufficient controls in

others. Today, the art of the possible in defending against adverse outcomes is rapidly evolving. This includes automated control systems that are built into processes and detect anomalies in real-time, behavioural 'nudges' to influence people to act in the right ways and controls guided by AA to simultaneously guard against risks while minimising false positives. For example, deep learning models and natural language processing have revolutionised the detection of fraud and money laundering and allow for highly nuanced credit risk assessment, credit line management and collections.[17]

If a risk event or control breakdown occurs, what immediate response is required?

Institutions need to be able to switch quickly to crisis response mode, guided by an established playbook of actions. Most institutions have historically done little to deliberately and holistically prepare for crises, taking an attitude of 'this will not happen to me'. In the evolving world, banks will need to build their crisis-preparedness muscle systematically. Leading institutions will maintain a well-rehearsed approach to manage through a crisis, whether it results from external or internal events and whether from the emergence of new risks or the dramatic escalation of known ones. Preparation should involve identification of possible negative scenarios unique to the organisation and mitigating strategies to adopt before a crisis hits, including periodic simulations involving both senior management and the board. Banks should maintain and periodically update a detailed crisis playbook, including when and how to escalate issues, pre-selected crisis leadership, resource plans and a road map for communications and broader stakeholder stabilisation.[18]

How should we integrate what we learn into risk decisions, detection and delimitation?

Information gained from ongoing risk mitigation, together with actual risk events and control breakdowns, can guide bank decisions to further hone risk processes and controls. At the same time, updates to processes and controls can impact materiality of risks and willingness to take them. Some stand-out institutions have undertaken systematic root cause analysis, but even these have typically done so in a relatively static way, through committee-based processes. Yet more rare is the bank that comprehensively monitors, analyses and learns from its ongoing successful risk mitigation. In the future, banks will need a dynamic feedback loop to continuously improve processes and controls. Such dynamic updates help catch control gaps while also avoiding overly tight controls. For example, AA models for credit underwriting or for identifying 'high risk' accounts as a part of know-your-customer can continuously improve with use, including to incorporate any shifts in the customer populations they analyse.[19] As they change their processes and controls, banks should also contemplate the potential impact of these enhanced capabilities on their risk appetite and on the magnitude of risk they are taking. For example, when first developing a new AA decision model with greater discriminatory power, a bank might run its traditional processes in parallel, until it has gained full comfort with the new approach.

Establishing the enterprise risk management function of the future

The ERM function of the future will need to enable banks to effectively delimit risk appetite, rapidly and accurately detect risks and control weaknesses and dynamically decide on the right risk management approach. Today, however, many banks approach delimiting, detection and decision either in silos (single risk types or isolated businesses) or in static and rigid ways across the enterprise, rooted in regulatory-driven programmes run by an ERM function or by a handful of risk and, sometimes, finance executives.

In the future, ERM functions should play a central role in driving a more dynamic approach, both setting clear standards for the full organisation while also making direct changes to how it operates. This sort of dynamic approach requires coordinated action, stemming from understanding of risk decision processes and risk governance enterprise wide; connectivity to senior stakeholders across businesses and support functions and strong understanding of the requirements and expectations of external stakeholders, notably regulators and rating agencies. Such expertise and centralised connectivity fit naturally under an ERM function.

We believe that ERM should take four steps to position itself, and broader risk management, for future success. These include defining its vision and mandate, shifting ways of working in its core areas of responsibility, setting the full scope of responsibilities beyond the core and ensuring the right internal talent within ERM.

1. Vision and mandate: Take the lead in reaffirming the role of the risk function and set an enterprise risk management–specific vision for value creation

The ERM function can help risk functions reclaim the territory of charting the risk management course for the organisation. Simply put, everything risk functions do should be designed to help banks make better risk-based decisions. This is a cornerstone of risk management but has, to some extent, gone missing in the risk programmes of regulatory design.

Existing regulatory-driven programmes must evolve to meet the new needs for risk management that arise from the changing landscape of threats and opportunities in banking. Many banks have treated the risk function as just another stakeholder in business decisions, not as a full partner, thereby distancing the function from the front line. When risk does not have a full voice in decision forums, it is reduced to acting in the background through passive policies and procedures, establishing a vicious cycle: the more the risk function exercises authority by pointing to policy, the less likely it is to have the true seat at the business decision–making table that it needs in today's word.

The ERM function can take the lead in reaffirming the role of the risk function as a business partner while also setting its own ERM-specific vision for value creation. ERM can help the risk function set a high aspiration for value creation in executing this work. This should include a clear definition of objectives, such as ensuring that efforts are focused on the risks that matter most, providing clarity about risk levels and risk appetite in a way that facilitates effective business decisions and making sure that the organisation is prepared to manage risks and adverse events. Heads of ERM should work together with the Chief Risk Officer (CRO) to identify those senior leaders whose input and support is necessary to articulate their vision and then to put it into action.

In practice, ERM should engage in a productive dialogue with business leaders to both gain an in-depth understanding of how the business thinks about risk in its day-to-day decision processes and share what risk capabilities ERM can bring to bear to help the business make better risk-based decisions. Typically, businesses approach decisions with the right risk versus return mindset but often lack key information to do this effectively. For example, business units often do not have a full systematic understanding of the full range of risk drivers affecting customers, together with a clear view of how a stressed environment could lead to losses. More broadly, businesses typically also lack a portfolio view, such as a full understanding of the cross-cutting effects of risk drivers on different products, or of the organisation's marginal capacity for risk taking. These are all critical aspects of risk-based decisions where the ERM function can help provide much needed clarity.

To create direct value itself, ERM must be able to understand the bank's business needs and help articulate the risk management activities necessary for those businesses to thrive. By developing the ability to clearly delimit risks, effectively detect risks and swiftly decide how to manage them, ERM will be in a much better position to partner with the front line, providing real-time knowledge and guidance rather than getting bogged down by ineffectual processes. In addition to defining objectives in a qualitative way, ERM should pursue a deliberate approach to measure how the function helps the bank mitigate risk, increase operational resiliency and reduce costs as well as how it supports business units in achieving their strategic objectives. To do this, ERM should keep track of risk mitigation performance. This has traditionally been done, for example, through monitoring the risk reduction achieved by control frameworks. Banks looked at the residual risks after controls, and contrasted them with the inherent risks that they had faced. There is an opportunity to keep track of the performance of potentially more impactful risk mitigation efforts as a direct result of ERM's actions. Example include monitoring how inner limit 'tripwires' for risk appetite have allowed the enterprise to get a leg up on mitigating risks and assessing the effectiveness of addressing actual risk appetite breaches through corrective action plans. In addition to helping to substantiate the value ERM brings to the table, this will also help provide an important feedback loop to shed light on whether risk limits are set at the right level. ERM can also keep track of how effectively it detects new and emerging risks and how this allows the bank to reduce or avoid losses.

2. Ways of working: Develop an agile approach to delimiting risk appetite, detecting risk and control weaknesses and deciding on the risk management approach

The ERM function should play a leading role in building more agile risk management. ERM is well positioned to do this, given its central risk coordination role, its comprehensive overview of risks and controls and its connectivity to risk stakeholders across business and support functions. In light of the increasingly volatile, uncertain and dynamic risk environment, we expect successful banks to increasingly adopt agile ways of working, convening cross-functional teams in real time and authorising them to make rapid decisions—in running the business, innovating and managing risk.

Today's outmoded, static risk management models must grow more flexible in the way they delimit risk appetite, detect risks and decide on how to manage risk. Led by their ERM functions, most banks run periodic, committee-dependent processes to establish and update formal risk appetite statements, identify risks that inform annual or biannual stress resting and to escalate and respond to risk events or control breakdowns. These processes typically do not accommodate rapid, real-time updates in response to changing circumstances and events. Furthermore, formal committee structures can inhibit quick formation of cross-functional teams with the tailored expertise and authority to make decisions and execute quickly. When risk management is ponderous and process bound, immediate events can outpace a bank's ability to respond, and in the longer term, businesses grow less likely to proactively involve the risk function as a thought partner in the face of time pressure or uncertainty.

The ERM function can reimagine the approach to delimiting, detecting and deciding, all areas for which hallmarks of agility—including collaboration, prioritisation and speed—are growing increasingly essential. We believe ERM should take steps to promote five agile ways of working:

Working in cross-functional teams
A more collaborative approach entails building teams and decision bodies with cross-functional membership. ERM can help put in place processes that ensure an appropriately comprehensive response by including people from across the bank, in a dynamic way based on the nature of the issue. For example, in response to a breach of a credit risk appetite limit, a bank would want to understand the full implications. Does the breach trigger any regulatory compliance concerns or questions of capital adequacy? What are the legal implications of a proposed mitigation response? Might reputational issues arise either from the breach or mitigation—for example, if the client is involved in lending in a sensitive industry? As a result, in addition to a direct risk owner in the front line and someone from credit risk, the team might include personnel from finance, legal, compliance, regulatory relations and reputational risk. For example, one bank defined the establishment of a cross-functional working team as a key step to address risk appetite breaches. The bank had struggled with achieving effective risk mitigation and corrective action, effectively

operating above its limits as a status quo. In reality, the business lacked the risk capabilities to drive sufficiently effective mitigation actions, while the risk function was viewed as too academic and removed from the daily business realities to help solve the problem. By convening a dedicated cross-functional team, the bank managed to bring together the right business and risk and finance understanding under the umbrella of a shared objective with a clearly defined goal and timeline.

Understanding the basics first
To ensure the level and speed of attention needed, the bank needs to quickly understand the nature of the issue at hand—its significance and how quickly it may play out. ERM can design mechanisms to quickly convene the right subject matter experts, in case of any uncertainty. Is an immediate decision needed about whether to withdraw from a business line or client relationship? Has a new, ill-understood risk emerged? Might a control breakdown merit shifting into crisis response mode? This allows for immediate prioritisation and triage. For example, one FinTech company runs daily 'customer huddles' with business and risk leaders. Executives review funnel metrics for the day side by side with customer complaints, to triage complaints accordingly.

Tailoring the approach
Decisions should receive appropriate transparency and scrutiny but not more, to avoid getting bogged down in excessive bureaucracy. ERM should lay out the decision points associated with each of delimiting, detecting and deciding and then sort them according to a hierarchy of decision 'archetypes', based on factors including significance, urgency, required expertise and degree of current understanding. This will involve formulating a clear view of what sorts of decisions require committee review versus execution by single responsible parties or teams, which layers of committee review are needed and what level of information and documentation is required to support decisions.

Empowering decision making
Previously unforeseen issues and risks that have the potential to evolve rapidly may require special fast-track decision-making mechanisms. ERM should design a process which first convenes the right subject matter experts and stakeholders to quickly understand and then design an approach to react to the issue at hand. Teams operating in such circumstances will need to make decisions quickly and be empowered to take ownership and move to these special mechanisms when needed. For example, one organisation does regular crisis preparedness exercises and has developed a playbook for how to respond to various types of crises, including who to go to for what in a potential crisis situation. The playbook makes clear who has decision-making power depending on the type of issue. This has proven to be critical in moments of potential crisis, including unexpected changes in the executive team, regulatory uncertainty and potential conduct issues. Another bank brings together risk, business and stakeholder engagement leaders weekly to perform scenario planning and understand what issues may emerge. Depending on the type of issue, the team is empowered to make decisions—whether it is to communicate messages internally and externally or to escalate to more senior leaders within the business or risk.

Digitising where possible
Effectively managing the evolving landscape of risks requires the ability to quickly obtain information about risks and control issues and to design a tailored approach to their management and mitigation. To do so, ERM has an opportunity to leverage new advances in process digitisation and AA. For example, to enhance early identification of new risks and control weaknesses, ERM functions can build a real-time digital dashboard of internal and market intelligence. By analysing the underlying drivers of risks, such dashboards can help reveal warning flags, whether through internal performance metrics or external indicators.

3. Defining full scope: Delineate enterprise risk management scope unambiguously in those areas of risk management that benefit from cross-cutting transparency and coordination

The role of ERM continues to evolve against a backdrop of a changing risk landscape and changing stakeholder expectations. The ERM function of the future should play a central role in coordinating the bank's approach to those components of risk management that require a cross-bank view, drawing on its connections to stakeholders across risk, business and support functions and on its comprehensive view of risks. ERM should ensure that a clear, single owner does exist, and if ERM is not that owner, it should carefully delineate its responsibilities and working model versus those of the group that is. We believe five areas benefiting from cross-cutting transparency and coordination deserve particular consideration.

Managing new and emerging risk types

As part of its risk detection, ERM should always maintain a point of view on emerging risk areas—such as climate risk—as well as on rapidly evolving risks—like reputational risk. ERM will have the most comprehensive view on how risks could affect different parts of the enterprise and a good perspective on how new and emerging risks have played out in the past, including an assessment of when things have worked well and when there have been gaps and vulnerabilities.

When ERM identifies such an area, it should either run it internally or partner to build the right capabilities elsewhere in the organisation. For example, some ERM functions are considering establishing dedicated teams tasked with assessing climate risk impact and defining how climate risk should affect business decision processes, including limit frameworks and policies. In some institutions, ERM functions are also developing specific capabilities to manage reputation risk, the nature of which has rapidly evolved with the spread of social media and heightened societal sensitivity. Actions include systematically embedding consideration of reputational impact in decision making, as well as forming reputation-focused committees. Learning from other industries, some banks are also starting to undertake sentiment analysis on customer complaints to identify emerging risks stemming from public perception.

Embracing the digital revolution

To embrace the digital revolution, risk functions should assign single-point responsibility for charting the bank's path on digital risk management and for guiding coherent, consistent execution. Such responsibility may sit with an ERM function. If responsibility lies elsewhere, such as with a Risk Chief Operating Officer (COO) or in a dedicated group, the ERM function will need to help set core requirements associated with delimiting, detecting and deciding.

One such area for clear delineation of responsibilities is in leveraging AA techniques as part of the risk detection process. For example, some banks are using natural language processing to support more effective risk detection including in customer complaints, employee allegations, internal communications or in suspicious activity reports.[20]

Optimising risk function organisation

ERM should take responsibility for ensuring that the enterprise is organised the right way to address the rapidly evolving complexion of risk in today's world.

ERM is uniquely positioned to play this role, because its management of enterprise risk programmes gives it a view across the enterprise—spanning both all businesses and all risk types. Its role in risk detection also helps it look ahead to assess what capabilities will be needed in the future, to meet emerging risks.

This responsibility takes two forms: the first is ensuring there is a consistent definition and corresponding operationalisation of lines of defence across the bank. Without this, the bank will not be able to manage risk effectively, and any attempts to increase agility will likely inject further confusion. The second is to assert what types of activities belong in the ERM function itself. These will typically comprise enterprise-wide activities that require the enterprise perspective to ensure highest value (as with centralised testing utilities, for example). By taking a systematic lens to the evolving risk types and organisational capabilities, ERM should help ensure that the enterprise has the right organisational setup and clear roles and responsibilities across the first and second line.

Ensuring the right talent

For effective risk management, institutions must maintain an up-to-date, comprehensive view of talent requirements, monitor and assess existing talent against that target and hire and train people to fill gaps. While many of these elements are owned by human resources (HR), the identification of risk management talent requirements should be strongly supported by risk, as it holds subject matter expertise on the type of skills that are required. This engagement can be coordinated by a central point within risk—perhaps a Risk COO or ERM. Central coordination is critical, as too often individual risk functions can duplicate skills across the organisation (eg risk reporting roles) or make assumptions that another part of the risk organisation is covering a particular skill area, which leads to gaps in risk coverage (eg who is undertaking independent testing).

Regardless of whether it leads to coordination, ERM should give significant input, based on its uniquely cross-cutting view of risk and risk management, spanning both risk types and businesses and functions. In particular, ERM can highlight new or increasingly important necessary risk management skill sets. For example, banks will increasingly need both model developers and model validators with an understanding of machine learning, including on unstructured datasets.

Shaping the risk culture

True ownership and responsibility for risk culture should sit with the front line. To be truly lived, culture must be linked with day-to-day business activities and outcomes of an institution. To support this, however, banks must assign ownership for coordinating the definition, measurement, reporting and reinforcement of risk culture. These responsibilities should sit centrally—either within ERM, a risk COO, an enterprise COO or within HR. It is helpful to have a central point, as too often, varying language is used to discuss culture within a bank. Without an enterprise-wide view and vocabulary, it is not possible to effect true, coordinated cultural change.

Regardless of where the central point sits, ERM in particular should contribute in three primary ways. First, it can identify cultural characteristics needed to support emerging priority areas in risk management, such as the sharing information across siloes essential to effective digital and cyber risk management or the individual accountability that helps guard against conduct risk. Secondly, ERM can incorporate a view of risk culture into aggregated reporting to senior management and the board. Thirdly, ERM can use each its multiple touch points across the bank—within the risk function, with businesses, with all functions—to further reinforce risk culture, including embedding the spirit of transparency, challenge and escalation.

4. Talent: Develop new capabilities and expanded domain knowledge to support the future-looking enterprise risk management vision, scope and ways of working

If the ERM function is to play the roles outlined here, its members need to develop new capabilities and expanded domain knowledge—this should cover a better understanding of the banking business from the perspective of the front line, familiarity with digital innovations and agile management capabilities.

The business of banking
As ERM moves to a more dynamic operating model, it needs to engage more effectively with the front line—not just to understand the landscape of risk better and become an effective second line of defence, but also to act as an effective counsellor and partner as the bank navigates the risk landscape. Therefore, ERM needs a strong understanding of how the business operates. For example, some banks are starting to make this happen by increasing rotation programmes between front-line and second-line functions.

Digital innovation
With data, analytics and technology driving shifts in how banks operate and much of the changing risk landscape, risk managers need a strong understanding of these domains. This is true both in terms of how data and digital interfaces are affecting bank processes and how banks are employing AI to support day-to-day decisions.

Agile management
Rather than organising their problem solving in a process-centric, committee-driven chain, risk managers will need to develop agile capabilities and mindsets, allowing them to identify opportunities to rapidly convene stakeholders and contributors across functions and drive to quick solutions. Similarly, ERM will need to develop strong abilities to work with other units and plug into processes without being a bottleneck—for example, by working effectively alongside the technology group as part of broader digital development efforts in the bank.

All these skills are highly specialised, and as ERM teams help develop them, leading banks will tap into these people in real time. For example, a large financing deal could have potential social, environmental, reputational and regulatory implications, all of which need to be evaluated. The recent example of the Dakota Access Pipeline can be illustrative of the need to understand wide-reaching consequences—in this case, fundamental concerns about the environment and native peoples' rights rapidly escalated from grassroots protest through social media and eventually made its way into congressional hearings focusing on bank's roles in financing the project. Banks will do well to understand the skills and knowledge required to manage the full spectrum of risks involved as they make decisions. As ERM becomes a centre of this critically important knowledge, the function will increasingly have a seat at the table during front-line decision making.

Conclusion

The ERM function is facing rapid change, with rising internal and external risks as well as increased expectations from customers, regulators, legislators, shareholders and the broader community. As these changes accelerate, functions will need to find ways to keep up. We believe successful banks will deploy highly skilled, diverse and agile risk organisations, allowing them to develop a strong and dynamic understanding of risks and much-improved organisational mechanisms for managing them.

About the Authors

Hans Helbekkmo is a partner in McKinsey's San Francisco office, where Olivia White is a partner. Cindy Levy is a senior partner in the London office and leader of the firm's global risk practice.

References and notes

[1] Office of the Comptroller of the Currency Rule 12 CFR Parts 20 and 170 (2014), available at: https://www.occ.treas.gov/topics/laws-regulations/occ-regulations/index-occ-regulations.html (accessed 24th June, 2019).

[2] Federal Reserve Board rule 12 CFR Part 252 (2014), available at: https://www.occ.treas.gov/topics/laws-regulations/occ-regulations/index-occ-regulations.html (accessed 24th June, 2019).

[3] For example, IDC predicts that the global data sphere will grow from 33 zettabytes (ZB) in 2018 to 175 ZB by 2025. See 'The data age 2025: The digitization of the world, from edge to core' (November 2019), Seagate Technology LLC, available at: https://www.seagate.com/our-story/data-age-2025/ (accessed 24th June, 2019).

[4] The pace of information flow overall and cross-border is growing rapidly. For example, annual global IP traffic is projected to reach 4.8 ZB per year by 2022 from 1.5 ZB in 2017. See 'Cisco visual networking index: Forecast and trends, 2017–2022 White Paper' (27th February, 2019), Cisco Systems Inc., available at: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html (accessed 24th June, 2019). The amount of cross-border bandwidth used has grown by a factor of 45 from 2005 to 2016. See Manyika, J., Lund, S., Bughin, J., Woetzel, J., Stamenov, K. and Dhingra, D., 'Digital globalization: The new era of global flows' (February 2016), McKinsey & Company, available at: https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows (accessed 24th June, 2019).

[5] See, for example, Dash, R., Kremer, A., Nario, L. and Waldron, D., 'Risk analytics enters its prime' (June 2017), McKinsey & Company, available at: https://www.mckinsey.com/business-functions/risk/our-insights/risk-analytics-enters-its-prime (accessed 24th June, 2019).

[6] See, for example, Cheatham, B., Javanmardian, K. and Samandari, H., 'Confronting the risks of artificial intelligence' (April 2018), McKinsey Quarterly, available at: https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/confronting-the-risks-of-artificial-intelligence (accessed 24th June, 2019).

[7] Philips, M., 'Knight shows how to lose $440 in 30 minutes' (2nd August, 2012), Bloomberg News, available at: https://www.bloomberg.com/news/articles/2012-08-02/knight-shows-how-to-lose-440-million-in-30-minutes, (accessed 24th June, 2019).

[8] Beyoud, L., 'Banks, credit companies to get new anti-fraud tool' (7th June, 2019), Bloomberg News, available at: https://news.bloomberglaw.com/banking-law/banks-credit-companies-to-get-new-federal-anti-fraud-tool (accessed 24th June, 2019). See, for example, Richardson, B., Waldron, D., 'Fighting back against synthetic identity fraud' (January 2019), McKinsey on Risk, available at: https://www.mckinsey.com/business-functions/risk/our-insights/fighting-back-against-synthetic-identity-fraud (accessed 24th June, 2019)

[9] 'Better identity in America: A blueprint for policymakers' (July 2018), The Better Identity Coalition, available at: https://static1.squarespace.com/static/5a7b7a8490bade8a77c07789/t/5b4fe83b1ae6cfa99e58a05d/1531963453495/Better_Identity_Coalition+Blueprint+-+July+2018.pdf (accessed 24th June, 2019); Sobers, R., 'The world in data breaches' (16th July), Inside out Security Blog, available at: https://blogvaronis2.wpengine.com/the-world-in-data-breaches/ (accessed 24th June, 2019).

[10] 'Transition in thinking: The impact of climate change on the UK banking sector' (26th September, 2018), Bank of England Prudential Regulation Authority, available at: https://www.bankofengland.co.uk/prudential-regulation/publication/2018/transition-in-thinking-the-impact-of-climate-change-on-the-uk-banking-sector, (accessed 24th June, 2019).

[11] See, for example, Kalavar, S. Mysore, M., 'Are you prepared for a corporate crisis?' (April 2017), McKinsey on Risk, available at: https://www.mckinsey.com/business-functions/risk/our-insights/are-you-prepared-for-a-corporate-crisis (accessed 24th June, 2019).

[12] Ortega F., Taspinar S., 'Rising sea levels and sinking property values: Hurricane Sandy and New York's housing market', *Journal of Urban Economics* (2018), Elsevier, Vol. 106, pp. 81–100.

[13] Hsu, T., 'Bank of America to stop financing makers of military style guns' (10th April 2018), *New York Times*, available at: https://www.nytimes.com/2018/04/10/business/bank-of-america-guns.html (accessed 24th June, 2019).

[14] Comfort, N. '“Bank tech shift biggest challenge since crisis”, Bundesbank says' (21st May, 2019), *Bloomberg News*, available at: https://www.bloomberg.com/news/articles/2019-05-21/bank-tech-shift-biggest-challenge-since-crisis-bundesbank-says (accessed 24th June, 2019).

15 Rosenthal, B. 'How we investigated the NY taxi medallion bubble' (22nd May, 2019), available at: https://www.nytimes.com/2019/05/22/reader-center/taxi-medallion-investigation.html (accessed 24th June, 2019).

16 See, for example, Hughes, M., Serino, L., Steinert, M., Walsh, J. and White, O., 'Perspectives on CCAR: Preparing for 2019 Amid Expectations for Regulatory Relief' (December 2018), McKinsey on Risk, available at: https://www.mckinsey.com/business-functions/risk/our-insights/perspectives-on-ccar-preparing-for-2019-amid-expectations-of-regulatory-relief (accessed 24th June, 2019). Also see 'Comprehensive capital analysis and review 2018: assessment framework and results' (June 2018), Board of Governors of the Federal Reserve System, available at: https://www.federalreserve.gov/publications/files/2018-ccar-assessment-framework-results-20180628.pdf (accessed 24th June, 2019). In this report, the Federal Reserve Board noted (emphasis ours): 'In particular, most firms' revenue and loss estimation approaches have matured and generally result in credible estimates that inform capital adequacy assessments. These advances have resulted from those firms improving the methods they use to identify their unique risks, using sound practices for identifying and addressing model deficiencies, and appropriately relying upon the results of capital stress testing to evaluate their capital positions on a forward-looking basis.'

17 See, for example, Breslow, S., Hagstroem, M., Mikkelson, D. and Robu, K., 'The new frontier in anti-money laundering' (November 2017), McKinsey on Risk, available at: https://www.mckinsey.com/business-functions/risk/our-insights/the-new-frontier-in-anti-money-laundering (accessed 24th June, 2019).

18 Kalavar and Mysore, ref. 11 above

19 Breslow, Hagstroem, Mikkelson and Robu, ref. 17 above

20 See, for example, Baquero, J., Eceiza, J., Krivin, D. and Venkatesh, C. 'The advanced analytics solution for monitoring conduct risk' (November 2018), McKinsey on Risk, available at: https://www.mckinsey.com/business-functions/risk/our-insights/the-advanced-analytics-solution-for-monitoring-conduct-risk (accessed 24th June, 2019).

Designed by US Design Center

www.mckinsey.com

@McKinsey
@McKinsey