EY
Building a better working world

Moving from analog to digital

A new paradigm for risk management

The world has moved from analog to digital. Risk management must do the same.

Demographic change, geopolitical turbulence and macreconomic uncertainty. Disruptive technologies and exploding data volumes. Shifting regulatory requirements. An increasingly complex matrix of competitors, partners and vendors.

The financial services industry faces an unprecedented quantum of change — one that will only expand and accelerate.

Major global trends and client demand for seamless digital delivery of products and services are forcing firms to fundamentally change how they design, build and deliver their offerings to consumer and corporate clients alike. Convergence across — not just within — sectors is forcing firms to adopt new business and operating models. Even the new industry players that have gained traction must focus on staying relevant.

Debates about robotic automation, machine learning, artificial intelligence (AI) and supercomputing have quickly moved from the esoteric and hypothetical to the practical and logistical. It's a matter of when, not if, for these technologies.

Profitability has never been harder to maintain, especially given the intensity of competition and the need to address the often competing demands of shareholders, regulators and governments. Social media makes it more difficult to manage company reputations; damaging news travels far and fast — almost instantaneously.

These megatrends mean risk management needs a new approach. Tried-and-tested methods that were effective in navigating yesterday's challenges will not work today. Adaptive digital risk management — which addresses the risks associated with digital transformation across the business and aims to digitize the practice of risk management — holds the key.

All of this will fundamentally affect risk management. Boards, senior management, the chief risk officer and other key executives will have to address four key risk imperatives:

1. Leveraging risk management to enable business transformation and sustained growth
2. Adapting to a risk environment and risk profile that is changing faster and more intensively than ever
3. Delivering risk management effectively and efficiently
4. Managing through and recovering from disruptions

Risk management will have to move from analog to digital — if it hasn't already. It will have to both manage the downside risk of ill-informed risk decisions and enable the firm to capture upside potential from measured risk-taking.[1] Risk management has contributed directly to restoring and protecting the franchise over the past decade. Now, in addition, it needs to earn a seat at the table in driving transformation. Risk management will need to inform evolving strategies; business and operating models; and new digital products and services. New capabilities will be required in areas such as smart and nimble controls, especially around the enablement of the customer experience and journey. Data analysis and reporting will have to change considerably to properly identify and capture new opportunities, as well as better manage downside risk. Delivery capabilities will need to be more resilient and secure.

[1]To better understand the three types of risks — upside, downside and outside risks — refer to the EY article: "How can you turn digital risk into a source of competitive advantage?" https://www.ey.com/en_gl/digital/how-can-you-turn-digital-risk-into-a-source-of-competitive-advan

Four risk imperatives: maintaining focus on what matters

Financial services are evolving quickly, and the manner in which firms manage risk has to keep up, evolving at a commensurate scale and pace.

1 Leveraging risk management to enable business transformation and sustained growth

Risk management professionals have to work with the business in managing through a digital transformation to properly address new risks and identify and grasp growth opportunities presented by industry change. This will require the risk group and its processes to change so that, collectively, risk management accelerates risk decisions.

Ultimately, risks and controls need to be owned by the first line, right up to the business unit leaders. Just because risk and compliance professionals sit alongside the first line, and work with their colleagues in the second line, does not mean first-line risk-takers can set aside their responsibility to own and manage the risks they create. Regulators concluded that that was a major failing in the run-up to the last financial crisis. First-line accountability had been heavily diluted.

A strong, two-way collaboration is required.

First-line revenue generators have to willingly and actively work with risk and compliance professionals in the first and second lines so that those professionals can inform business unit strategies, new product design, credit and pricing decisions, and so on. Risk, compliance, controls, security, privacy and other considerations have to be integrated into first-line innovation, process and product transformation and be firmly embedded in the customer experience and platforms. Risk management has to validate that risk is always considered and push the businesses to optimize the use of the firm's risk capacity. Risk management is not simply about risk avoidance — it is about enabling the firm strategically in taking risk-informed decisions to grow and prosper.

Knowing your lines of defense[2]

First line of defense comprises the risk-takers and enablers that generate revenue and risk-enabling activities. It encompasses business lines, day-to-day operations, technology groups, customer relationship management, marketing and human resources.

Second line is made up of the risk monitors. They develop the risk management framework and provide guidance to the front lines to maintain an independent, aggregate view of risk.

Third line includes the risk assurance group. They independently assess the risk governance framework and provide a view beyond control adequacy.

Given the expected magnitude and speed of change to firms' risk profiles as they transform digitally, second-line risk management has to reimagine how it will achieve its objectives and meet its mandate to the fullest extent possible. The trick will be balancing the need to remain independent from the first line, challenging line of business managers' decisions and validating their operating model within the board-approved risk appetite and risk policy constraints, with the need to contribute to sustained firm growth, profitability and safety and soundness.

[2]For more information concerning lines of defense, refer to the EY Financial Services webcast: "Cybersecurity: three lines of defense," 12 January 2017; replay available here: https://www.ey.com/gl/en/issues/webcast_2017-01-12-1100_cybersecurity-three-lines-of-defense

2 Adapting to a risk environment and risk profile that is changing faster and more intensively than ever

Risk management has to stay in the moment, keeping a keen eye for immediate changes in market or firm conditions, and focus to the future to spot emerging or long-term risks and opportunities. It has to stay sensitive to financial and nonfinancial risks that are here today or that might emerge tomorrow.

The paramount importance of maintaining confidence in financial institutions and the pace at which market and counterparty conditions can change almost instantly (and nowadays, arguably faster than ever, given high-velocity and machine-based trading) mean short-term risks need to be proactively monitored carefully so that speedy, informed decisions can be made on how to adapt to new conditions.

At the same time, a focus on emerging risks is equally important. Such risks may be known but increasing, new or, until now, immaterial, and need more analysis and consideration. Today, such risks include cybersecurity threats; rising interest rates; use of technology; impact of FinTech; heightened reputational and privacy risks; industry disintermediation and ever-more growth in the dependency on third and fourth parties; and the evolving regulatory environment.[3]

Few of these are unknown, but their relevance and impact could change materially over the coming months or years. Risk management has to remain nimble and constantly aware to help the organization consider how strategies, business plans, suites of products and services, technology investments, financial resources, and controls need to adapt in light of these emerging risks.

Beyond the next three to five years, it is important to consider how risks will evolve over 20- to 30-year time horizons.[4] After all, many financial services firms are investing or providing insurance over such time frames. Risk management is perhaps the only part of the firm that has the time or resources to properly consider these broader changes and their impacts on economies, clients, customers, sectors and, most importantly, the firm itself. Changes that may be considered medium-term emerging risks include the potential long-term impact on customer demand for financial services products and services from the impact of climate change, sensor technology and the connected Internet of Things, urbanization, population growth and mass migration, and broad-scale use of AI and virtual reality and workforce patterns. The long-term impacts could be profound, and short-term solutions that ignore these megatrends will likely create significant problems for those not taking the long view.

3 Delivering risk management effectively and efficiently

In the last 10 years, the focus on strengthening risk management in the first and second lines has been on effectiveness. Do firms have the appropriate resources to identify, manage, monitor and mitigate risks? Oftentimes, near-term risks — notably, regulatory and reputational — preoccupied firms. Boards and regulators have had a laser focus on implementing and maintaining a robust set of controls that keep residual risk within the bounds of the agreed-upon risk appetite.

However, risk management is not, and should not, be immune from working efficiently. It has to seek out and continually find ways to conduct its work efficiently, working in partnership with other control functions that are also going through substantial change, such as compliance and internal audit. Risk management has to deploy new technologies in its own activities, which will inevitably necessitate new operating and talent models. The pace of change in digital risk management innovation is quite remarkable and ongoing; we are seeing significantly more use of automation and data analytics — and the establishment of new industry consortia and utilities — in areas such as know-your-customer and other aspects of financial crime, as well as third-party risk management.

[3]To learn more about emerging, risks refer to the EY article: "How can regulation keep up as technological innovation races ahead?" https://go.ey.com/2CKIUmn

[4]To learn more about the evolution of risks, refer to the EY article: "Risk. Innovation. Can your business strategy tell the difference?" https://www.ey.com/en_gl/digital/risk--innovation--can-your-business-strategy-tell-the-difference

Very quickly, the same will be true in other areas, such as cybersecurity and fraud, credit analysis, and regulatory reporting and compliance.

In the end, risk management is a balancing act between effectiveness and efficiency. Emphasizing one over the other carries its own risks. Newly digitized processes such as automated underwriting and credit approvals may speed and improve decision-making, but regulatory and supervisory requirements and ever-changing and challenging customer expectations for transparency and fairness still need to be met.

4 Managing through and recovering from disruptions

Risk management has a central role to play not only in helping navigate the evolving risk profile but also in preparing for, managing through and recovering from disruptions.[5]

Such disruptions appear to be becoming more commonplace, making senior executives increasingly concerned about their firm's true resiliency capabilities. Cyber attacks are driving some of these concerns, as is an elevated focus on fragile information technology and more frequent and pronounced weather-related disasters. Dependency on third- and fourth-party providers, industry consortia and new partners — e.g., FinTech firms — is accentuating the focus on resiliency because dependencies and concentration risks in the ecosystem are being created or amplified.

Increasingly, firms have recognized that their continuity activities are disparate and unconnected. They often have countless activities across business continuity, disaster recovery, cyber-incident response and crisis management (and for large banks, the integration with recovery and resolution planning). Often, myriad crisis and contingency plans exist across lines of business, technology, human resources and other areas. Few plans are connected or consistently applied; few have common or consistent triggers for escalation and decision-making; and few have properly prepared their senior executives and/or boards for actual crises. The result is often ineffective or slow decision-making in times of stress.

Regulators have witnessed the same shortcomings. They are increasingly focusing on business-model, operational, technological and financial resiliency, and believe these issues should be managed in a connected manner, with a strong focus on differentially protecting the most critical business processes and assets. They expect first- and second-line risk management to influence resiliency strategies and link them to the overall enterprise-wide risk management framework; to validate that risks are being considered and decisions to accept more risk during a crisis event are well-informed, challenged and documented; and to make sure that the firm returns to business as usual as soon as possible post-crisis. Risk management should challenge everyone to learn from past events and remediate issues so the firm is better prepared next time in addition to being prepared for new and unforeseen issues.

Risk management can help accelerate efforts to simulate crises to build muscle memory across the organization, especially at senior management and board levels. Testing contingency and crisis-management processes is important, but even more so is getting senior leaders used to making decisions in crisis situations, no matter what type of event. It has to feel natural.

[5]To learn more about emerging continuity factors refer to the EY article: "Managing through crises: preparation is key." https://www.ey.com/Publication/vwLUAssets/ey-managing-through-crises/$File/ey-managing-through-crises.pdf

Converting from analog to digital risk

Executives have long spoken of S-curves — the evolutionary journey that industries go through from one stable era to the next. Disruption marks the transition between eras.

The reality this time may be that the next S-curve itself will likely be an era of constant disruption. Unlike prior eras, when stability returned after a period of transition and firms could fall back into three- to five-year planning cycles, we are now looking at change being a constant — ongoing innovation and reinvention. Firms will prosper only if they can build change into their DNA and recruit and retain talent who can thrive and prosper in such an environment.

Firms can't simply pull out old risk management playbooks, dust them off and sprinkle in references to digital. That's wholly inadequate and unrealistic. A new paradigm is required.

[6]To learn more about digital transformation and trends, refer to the EY-commissioned financial services study conducted by Forrester Consulting: "Digital enterprise transformation: winning themes of financial services leaders." https://www.ey.com/Publication/vwLUAssets/ey-digital-enterprise-transformation/%24File/ey-digital-enterprise-transformation.pdf

[7]To learn more about skills required by a new generation of risk professionals, refer to the EY article: "Do you have the right talent to take the right risks" https://www.ey.com/en_gl/digital/do-you-have-the-right-talent-to-take-the-right-risks

A new risk management philosophy: nimble and integrated

It starts with a different philosophy. Digital is a culture, a new way of thinking and behaving. Being digital is about transforming one's business at its core, including risk management processes, people, technology and firm operations. Companies have to reinvent their operating model and extended ecosystem; this is not simply investing in new technology.[6]

Inevitably, risk management processes and operations need to be nimble, evolving and able to turn elevated amounts of data into actionable risk intelligence. For many organizations, risk and compliance operations are unable to keep up with the pace of change because of the manual, inefficient and typically siloed operations and are unable to leverage the data available across the organization, resulting in an inability to fluidly capture and manage risks effectively. Thoughtful streamlining of operations and broad-based use of technology will enable risk management to be more responsive to the ever-evolving business environment.

A new set of integrated capabilities

Five core areas comprise digital risk management:

1 Adaptive digital risk governance

Risk management of the future will need to be more adaptive to new and emerging risks and build adaptiveness into core risk management disciplines, such as risk strategy, risk identification and assessments, risk appetite and limits management, and the firm's overall risk operating model and culture. A strong three-lines-of-defense model will remain a core foundation to strong risk management in a digital world. Accountability must be palpable, from the board level, through management, down to every employee.

Adaptation has to focus on three core design elements: the risk management organization structure, the location strategy (the firm's and that of the risk management function) and the talent strategy. These elements will change materially in coming years, especially talent. A people model based mainly on subject-matter professionals will not suffice — new skills will be required, notably linked to data analytics, technology, product design and agile development. Soft skills such as communication and negotiation skills, diversity and inclusiveness, and active teaming across lines of business, functions and geographies will become paramount.[7] Those who can combine business and technical acumen — and knowledge of customers and products — will move forward faster, gain competitive advantage and excel in a changing world.

2 Product and services management

Properly governing, as well as integrating risk management processes and controls into the design and implementation of new products, services and business processes, is an essential part of implementing digital risk management. It enables faster innovation and mitigation of risk through the establishment, or use of, new platforms — that is, new data capabilities and different technical environments (e.g., cloud or distributed ledger) and the use of AI in decision-making, surveillance and processing.

3 Resiliency and trust

None of the above means anything if firms aren't dependable — customers want reliability, access and protection. Too often, with a rush to get innovations to market, firms give such issues short shrift, with the expectation, after launch, that controls can be retrofitted. With proper digital risk management, issues are factored into the initial consideration around the business case, so the full cost of delivery and the impact on the firm's risk profile are considered at that point, not later, when products and services have been greenlighted and designed. Data privacy and security are prime examples — core concepts need to be designed at the outset and drive how firms collect, use, secure and, when appropriate, destroy data, and design principles need to be flexible enough to adapt to changing regulation and customer expectations on what's appropriate.[8]

Digital risk management requires firms to infuse resiliency, cybersecurity and privacy into the design of platforms and products, as well as into the extended enterprise through third- and fourth-party vendors. This will call for a transformation of how third-party risk management conducts its full life cycle of activities, from pre-onboarding due diligence, through to monitoring onboarded vendors, to offboarding. The management of critical vendors — those that support crucial business processes or whose disruption would have system-wide impacts — will need to change the most.

Preparedness will be essential. Firms should conduct simulations against a range of scenarios, from cybersecurity breaches, to technology or third-party outages, to operational or location failures. Worst-case cybersecurity scenarios (e.g., the corruption of production and backup data) ought to be considered.[9]

[8]To learn more about the EU's General Data Protection Regulation (GDPR), data privacy and security, refer to the EY article: "GDPR: demanding new privacy rights and obligations." https://www.ey.com/Publication/vwLUAssets/ey-gdpr-demanding-new-privacy-rights-and-obligations/$FILE/ey-gdpr-demanding-new-privacy-rights-and-obligations.pdf

[9]To learn more about digital risk resiliency, refer to the EY article: "Governing cyber risk in financial services." https://www.ey.com/Publication/vwLUAssetsPI/EY-governing-cyber-risks-in-financial-services/$FILE/EY-governing-cyber-risks-in-financial-services.pdf

4 Platform, data and infrastructure

Getting technology and data foundations right is key. In many cases, financial services firms are still grappling with legacy systems that inhibit digital transformation, but replacing core legacy systems is a major change — it's costly, brings with it major execution risks and can take years. Yet, transformation is essential.

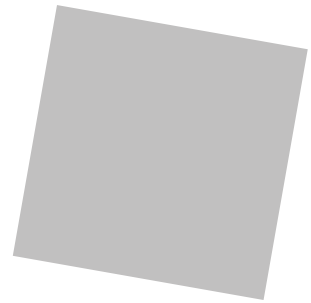
Core, central capabilities provided by a platform and connected data sources (e.g., so-called "data lakes") allow for quicker integration of customer, transaction and risk management data into decision-making processes. Together, this will uncover new opportunities to meet evolving customer expectations and drive value, as well as enable better risk management through improved data-driven insights. Controlled, secure cloud-based architectures are required to enable risk management and regulatory compliance.

5 Agile decisions

The lifeblood of effective risk management is insight based on accurate, timely data. Most firms have myriad management information systems and analytical tools and capabilities; most are siloed and inefficient. It is challenging to mine connected data quickly to provide decision-makers with the requisite intelligence, whether they be front-line customer-facing teams or senior management and the board of directors. In a digital risk management environment, core capabilities allow for end-to-end management of the firm's risk portfolio using data and analytics to provide accelerated identification, measurement and monitoring of customer and portfolio-risk signals in support of customer and product strategy and alignment with the board-approved risk appetite. Risk, compliance and control intelligence requirements need to be built in at the design stage so that necessary data is captured from the outset to aid risk monitoring and analysis. Such an approach allows for more real-time risk detection, more informed and granular risk and reward optimization, and better and more aggregated reporting up the entire organization.

Embedding risk management activities into the design and execution of the customer journey and related business processes will allow risk management professionals to validate that the right controls and risks are being considered, as well help them identify how the digital engagement of customers could enable faster and more effective risk decision-making.

Nimble and smart controls within digitized processes and transformation programs have to be responsive to evolving risks and environmental factors, and self-adapt to learn and improve. The firmwide control strategy will have to be fundamentally redesigned across the three lines of defense, particularly as it relates to first-line risk management. Automated — and, where possible, continuous — controls monitoring should be implemented within the context of an automated monitoring and surveillance framework appropriate for a digital world.



Transforming to a digital future to address risk imperatives

The financial services industry is undergoing a massive transformation, and risk management runs the risk of falling behind and staying focused on only downside risk.

Over the past decade, risk management has helped restore and protect franchises and the industry at large. That role remains critical. However, risk management will now have to undertake a transformation that feels even more substantial. It has to build on solid foundations and its strong stature across the firm to be a leader in enabling business transformation, adapting to a fast-changing risk environment and helping the firm manage through and recover from disruptions. It has to do so in an extremely effective and efficient manner.

Only time will tell which firms make the changes properly and in time. Some will get lost in the day-to-day, while others will get distracted by shiny new technologies. Others will be paralyzed by continued uncertainty. The winners will be those that have the forward-leading courage to embrace business transformations and reinvent their processes and technologies while continuing to focus on long-term firm performance, safety and soundness.

The time for risk management to act is now. Products and services — and the manner in which customers are being engaged and served — are already changing materially. Without risk management being deeply involved in such change, firms run the risk of mispricing or understating risk, or inadvertently creating future misconduct-risk challenges. Very soon that risk will be dwarfed by the potential failure of risk management to inform and guide material changes to business and operating models — and the very role of existing players in the industry's value chain.

Risk management has to have a seat at the table, and to be credible it needs to be very much part of the overall digital transformation discussion, from strategy to implementation. Being an interested spectator is not an option.

Ernst & Young LLP

Authors

Cindy Doe
Principal
cynthia.doe@ey.com
+1 617 375 4558

Amy Brachio
Partner
amy.brachio@ey.com
+1 612 371 8537

Amy E. Gennarini
Principal
amy.gennarini@ey.com
+1 212 773 2696

Marc R. Saidenberg
Principal
marc.saidenberg@ey.com
+1 212 773 9361

Adam C. Girling
Principal
adam.girling@ey.com
+1 212 773 9514

Thomas Campanile
Partner
thomas.campanile@ey.com
+1 212 773 8461

Samir Nangea
Principal
samir.nangea@ey.com
+1 212 773 6742

Mark Watson
Executive Director
mark.watson@ey.com
+1 617 305 2217

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.

EY is a leader in serving the global financial services marketplace
Nearly 51,000 EY financial services professionals around the world provide integrated assurance, tax, transaction and advisory services to our asset management, banking, capital markets and insurance clients. In the Americas, EY is the only public accounting organization with a separate business unit dedicated to the financial services marketplace. Created in 2000, the Americas Financial Services Organization today includes more than 11,000 professionals at member firms in over 50 locations throughout the US, the Caribbean and Latin America.

EY professionals in our financial services practices worldwide align with key global industry groups, including EY's Global Wealth & Asset Management Center, Global Banking & Capital Markets Center, Global Insurance Center and Global Private Equity Center, which act as hubs for sharing industry-focused knowledge on current and emerging trends and regulations in order to help our clients address key issues. Our practitioners span many disciplines and provide a well-rounded understanding of business issues and challenges, as well as integrated services to our clients.

With a global presence and industry-focused advice, EY's financial services professionals provide high-quality assurance, tax, transaction and advisory services, including operations, process improvement, risk and technology, to financial services companies worldwide.

US SCORE no. 04391-181US
1809-2863640 (BDFSO)
ED None

ey.com