Deloitte.

Financial services: Managing risk to get fit for a digital future

MAKING AN IMPACT THAT MATTERS since 1845

Introduction

Amid the humanitarian and economic shock of COVID-19, the digital forces reshaping the financial industry have gone into overdrive. Nearly overnight, firms have pivoted to digital channels, technologies, and ways of working.

All this has taken place against a backdrop of customer demands for greater choice, transparency, and frictionless delivery in the products they receive. Innovative startups and non-traditional players are responding via new modes of competition. To protect consumers and maintain orderly markets, regulators are raising the bar for compliance.

The impact is just as dramatic inside the organization. From cloud computing to artificial intelligence, advancing technology is transforming the front, middle, and back offices. Operating and talent models are bending to the demand.

These trends are shot through with a common thread: digital risk. In the discussion that follows, we'll examine digital risk along its various dimensions, then break it down by type. Before we do that, however, let's review what digital risk really means for financial services—and why it's become such an urgent topic today.

The landscape of digital risk

Regulators now expect financial institutions to withstand severe business disruptions. Examples include a global financial crisis, geopolitical event, or worldwide pandemic such as COVID-19. A key part of this operational resilience is the ability to manage risks associated with an increasing reliance on digital business practices.

Digital risks include those related to software and hardware, such as service outages or unauthorized access. But they also include risks related to the application of digital technology. Consider the following examples:

- **Retail lending.** An artificial intelligence (AI) system processes a high volume of inputs through hundreds of steps to arrive at a lending decision. But it isn't clear that the decision is fair—and between the system's complexity and its ability to learn on its own, it can be extremely difficult to understand why the system behaves as it does.
- **Derivative trading.** Two parties agree to a simple interest rate swap through a blockchain. They set up a smart contract that transfers value at the end of each settlement period based on market data from a central authority. However, the blockchain authenticating the trade potentially exposes the details of the trade to competitors.
- **Underwriting.** Facing declining margins, a life insurance company turns to emerging markets where the potential for growth is significant. However, these locations have no agent networks, making mobile technology the practical way to reach customers. The insurer partners with a fintech firm to develop an app, only to find itself disintermediated as the partner gains control of the customer relationship.

As these examples indicate, digital risk can be strategic, financial, operational, regulatory, or reputational in nature. Digital risk is also highly nuanced and subject to ongoing change as digital ecosystems, business, and service models evolve.

The examples also reveal a tension at the heart of operational resilience. On the one hand, it demands that firms mitigate the new digital risks they're exposed to. On the other hand, operational resiliency more broadly reflects the firm's ability to respond to fast-changing business conditions. Said differently, financial institutions tread a narrow path between speed and control, prompting the need for more agile risk and assurance processes. The implications include:

- New culture and skills for informed risk taking and experimentation
- New frontiers of engaging in a vast and complex global ecosystem
- New speed of execution when near-continuous change is the norm
- New accountabilities for operating in the physical and digital domains
- New ethics in the wake of opportunities and challenges that didn't exist before. If all this seems incredibly complex, you're not wrong. Fortunately, there are ways to think through the risks so that firms can identify and manage them systematically. One place to start is by exploring the dimensions of digital risk from an organizational perspective.

Findings from the Deloitte Global Digital Risk Survey

To gauge the organizational impact of disruptive technology, Deloitte UK recently surveyed 167 senior executives around the world in the financial services industry.[1] Among respondents:

- Most (69%) need more than six months to convert new ideas into live solutions
- Over a third (36%) experienced significant incidents due to disruptive technologies going wrong
- Only 7% believe the information provided to governance bodies to help them manage risks effectively is comprehensive and produced efficiently
- On a scale of 1 to 10, most (60%) rate the effectiveness of their risk management tools at 5 or less
- Fewer than one in five (19%) are fully confident their digital delivery teams have the appropriate skillset to manage risk in a digital organization

The upshot? Many of the barriers to achieving true digital transformation are no longer related to technology. Instead, they arise from gaps in the organization's ability to manage risk.

[1] Deloitte, Beyond the hype: Global Digital Risk Survey 2019, https://www2.deloitte.com/content/campaigns/uk/global-digital-risk-survey/global-digital-risk-survey/global-digital-risk-survey.html

Dimensions of digital risk

Like other types of risk, digital risk often hides in plain sight. To find it, financial executives need an idea of what they're looking for. An intuitive approach is to look across the following organizational dimensions for signs that point to risk.

New digital ecosystems, business, and service models. These use partners and suppliers in different ways. What to do now: Identify who you're doing business with, how much of your customer data they might have, and whether they're hosting your systems on the cloud.

Experiences and engagement. News about how you engage with partners, customers, employees, and regulators can travel farther and faster today. What to do now: See whether your digital investment is inclusive and achieving positive outcomes for stakeholders.

Ambitions and aspirations. It takes agility to realize strategic opportunities in a digital world. What to do now: Gauge your ability to deliver digital transformation safely and securely.

Changing external environment. The risks associated with digital transformation are leading to increased regulatory scrutiny. What to do now: Assess your relationship with global regulators.

Culture and leadership. It takes a digital-first mindset to embrace new ways of working. What to do now: Gain insight into the degree of digital sophistication at all levels of your organization.

Branding. A financial firm's brand should reflect the digital ambitions of leadership. What to do now: Investigate what your customers and employees are saying about your business (including supply chain partners).

Organization and workforce. Digital success relies on a workforce that can stay abreast of change without compromising on security. What to do now: Determine how prepared your risk and control teams are to accommodate an agile workforce.

Enterprise operations. Risk management must keep pace with a more dynamic and automated operation. What to do now: Analyze the appropriate balance between post-event assurance and pre-event monitoring.

Platform, data, and infrastructure. As you digitally evolve, legacy systems can hold you back. What to do now: Find out how much technical debt exists and whether expenditures on new technology are sufficient.

Types of digital risk

Although the digital risk profile is unique to each organization, certain types of risk are common among financial institutions. Here are some of the most significant.

Cybersecurity risk

As processes and data become more digitized and networked, cybersecurity risk goes up. Firms may exacerbate the risk by trying to protect all digital assets equally rather than shifting more protection to the "crown jewels." They may also focus on avoidance of cybersecurity incidents at the expense of mitigation strategies, and vigilance at the expense of ease of doing business.

Ecosystem risk

Business ecosystems creates more opportunities for cyber-intrusion and systemic risks. For instance, partnerships and outsourced services can boost organizational exposure to bad actors, contagion, and errors from model miscalibration. Meanwhile, systemically important technology and data providers can introduce single points of failure.

Emerging technology risk

The greatest digital risks may be from technologies that don't exist yet. Think financial exclusion as technology systems invent their own logic, unintentional collusion as institutions interact through high-speed networks, and breach of fiduciary duty as digital systems take on broader sets of customer-facing responsibilities.

Execution risk

To be successful, digital projects require fundamental, top-down shifts in how organizations execute. Without those shifts, firms may run into challenges with user adoption, institutional buy-in, and integration with legacy systems. In addition, organizational structures may hamper rather than support agile execution.

Fraud risk

Amid increasing volumes of digital transactions—especially cross-border ones—strong know your customer (KYC) and anti-money laundering (AML) processes become more important than ever. They help fight fraud associated with open banking, money transfers, new account activation, and more in an environment where it can be unclear who owns the liability of fraud.

Privacy risk

Data is proliferating—and so are laws around data privacy and transparency. Between them, these two trends raise the stakes of a data breach involving personally identifiable information. Retention of unnecessary data can add to the risk. So can a lack of clarity on data ownership, uses, and alteration.

Legal and regulatory risk

Around the world, regulators are issuing new rules addressing the increasing digitization of financial services. These regulatory regimes are in various stages of maturity and may contradict existing business practices. A rush to comply can add to the risk by creating complex, overlapping layers of compliance requirements and systems.

Brand and reputational risk

Data loss, outages, and misuse can significantly impair a financial institution's reputation. Beyond that, digital tools may introduce ethical pitfalls and biases that can reflect negatively on financial services. Examples include incomplete or unrepresentative data sets, bias in input data, and subconscious developer bias that influences the internal logic of a digital application.

Strategic risk

Strategic choices can intensify digital risk. For instance, firms may opt not to integrate their IT and business strategies. They also may opt to digitize existing processes without improving them or emphasize short-term cost savings over an upgrade of the full digital environment. Another choice might be to ignore new partners and technologies rather than embrace them.

People and culture risk

Talent to support digital transformation—examples include data scientists and developers—can be in short supply. At the same time, opportunities to upskill or cross-train staff may be limited. Some employees may resist digital transformation for fear of losing their jobs, while long-term trends may prompt financial institutions to accommodate more flexible ways of working.

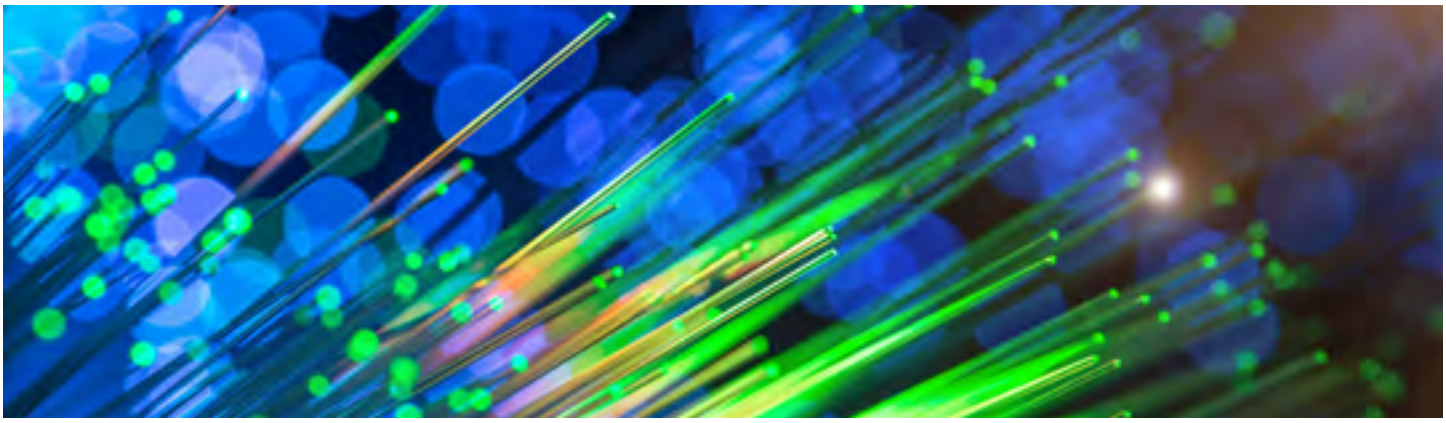
Turn digital risk into digital advantage

Financial firms are in the midst of significant digital disruption. This disruption is changing the nature of risk as well as introducing new risks that might not have existed in the recent past. At the same time, digital technologies and processes offer financial institutions the opportunity to redefine business models and transform customer interactions.

So where can boards take it from here? Consider any of the following actions as a starting point:

01. Form a board-level committee to promote understanding of digital risk
02. Add a board director with strong digital management skills and leadership experience
03. Call for internal audit to report on digital risk via the audit committee
04. Encourage management to enhance the quality of reporting on digital transformation
05. Define thresholds for digital risk situations that merit board-level attention
06. Make room on the board meeting agenda for a discussion around digital risk
07. Require management to give a plain English update of digital risks, programs, and issues
08. Bring in guest speakers to provide independent views of the digital risk landscape
09. Stress-test the organization's capabilities to respond to a major event

In a world dominated by financial and regulatory risk, it's easy to overlook the risk that arises from digital transformation. The good news is that digital risk can be easier to understand than it seems; common sense is a reliable guide. And by getting a handle on digital risk, board members have a chance to deliver a better customer experience, get their firms fit for the future, and do their part to create a more resilient financial services ecosystem.



Global contacts

J.H. Caldwell
Global Risk Advisory Leader,
Financial Services Industry
United States
jacaldwell@deloitte.com

Stephen Ley
Global Lead Partner,
Technology and Digital Risk
United Kingdom
sley@deloitte.co.uk

Tom Bigham
UK Lead Partner,
Digital Risk
United Kingdom
tbigham@deloitte.co.uk

David Wu
Deloitte China Vice Chairman
Financial Services Industry Leader
Tel: +86 10 8512 5999
Email: davidwjwu@deloitte.com.cn

Fang Ye
FSI Risk Advisory Leader, Mainland China
Deloitte China
Tel: +86 21 6141 1569
Email: yefang@deloitte.com.cn

Harry Zhang
Partner, FSI Risk Advisory
Deloitte China
Tel: +86 10 8512 5658
Email: harryzhang@deloitte.com.cn

Deloitte.

Designed by CoRe Creative Services. RITM0480751