kyndryl

The power of effective IT risk management

Regulation, risk, and the call for an integrated digital operating model in banking.

Contents

2 Executive summary

3 Introduction

4 Risk in information technology

5 The research

5 Organization and management profile

5 Technology profile

6 Regulatory profile

6 Conclusion: The future of bank risk management

8 Acknowledgments

8 About the research

“Looking at the effects of regulation, the global market, IT security threats, financial budgets, and talent pools, IT risk management is becoming increasingly interconnected.”

Executive summary

Amid all of today’s banking risks and challenges, IT can have a difficult standing. When perceived to solely enable operations and system availability or to prevent cyberattacks, technology’s inherent complexity—and moreover, its value to the business—is profoundly underrated.

A global peer group study of 20 Kyndryl Vice Presidents and their teams examining financial services customer accounts explores the state of today’s IT infrastructure currency, the impact of supervisory changes on decision-making, and prevalent IT risk management approaches.

Looking at the effects of regulation, the global market, IT security threats, financial budgets, and talent pools, IT risk management is becoming increasingly interconnected. It requires intelligent IT governance models that capture intrinsic and extrinsic complexities, a more secure infrastructure and related investments, and an overall stronger risk management and governance function. Given the magnitude of these and other influences, most risk functions in financial institutions are still in the midst of transformations that respond to these increased demands.

Introduction

Risk management in financial institutions has changed substantially over the past two decades. The regulations introduced after the global financial crisis—and the considerable fines that were imposed in its wake—triggered change in banks' risk functions. These changes included stronger requirements for liquidity, market, and capital risks; a higher transparency towards the public and the regulator; and higher standards for risk reporting. Stress testing has become increasingly important as a major supervisory tool and as an answer to growing expectations towards banks' risk-appetite statements. With tightening standards for compliance and conduct, managing non-financial risk has gained substantial importance, which has continued in recent years where the extent and speed of technological advancements have spurred threats to data, systems, and services.

The rapid increase of technology risks within banks' operational risk posture presents a number of challenges. The management of technology risks highlights factors such as:

- Availability of services and their underlying systems
- Age of systems and the increasing threat that legacy systems pose over time
- Criticality of applications and databases for delivering continued services to the banks' customers
- Minimization of outages for customer-facing services
- Management of increased demand for technology skillsets within a generally aging workforce
- Pace of technological change

These factors all signify an overall weaker technology risk prevalence and ask for continual monitoring and adaption.

Technology risk holds strategic, financial, operational, regulatory, and reputational implications. Addressing the emergence of these technology risks, their evolving nature, and the increase of cybersecurity and internal model risk points to an attentive risk management system that uses real-time data insights for decision-making and accounts for the interconnectedness of technology risks.

In the midst of these changes, we have come to witness a diversified status quo among financial institutions. While some excel, others find it significantly harder to adapt to these changes. Tapping into this challenge, we asked 20 Kyndryl Vice Presidents and their teams working with our financial shared services customers about their views on today's risk management practices and board's IT risk affinity, as well as the prevalent technological challenges in a regulatory environment. Our research points to three recommendations for banks and financial service companies addressing technology risk and resilience.

Risk in information technology

Technology is one of the greatest enablers in our day and age, but also presents potentially high-impact risks. With impending regulatory changes for financial institutions, inflation confronting financial markets, and the ever-evolving field of information technology, risks in financial institutions have evolved in recent years.

Some of the most significant trends include:

1. **Absence of technology investment threatens service quality and regulatory requirements.** With hardware, middleware, and software providers continuing to improve their products, IT maintenance and management of legacy technology has become an increasingly important operational and cost management task. When banks' IT and business strategies are misaligned, balancing technology expenditures becomes a struggle. Moving on to newer technologies, phasing out or decommissioning outmoded technologies and accounting for other parameters such as age, availability of resources, and criticality of applications or databases all become part of a proactive view on risk transformation. These factors are not only mandatory for supervisory compliance but will, in turn, be critical for upholding service and security promises to banks' customers.

2. **Cybersecurity and the emergence of new risks signify unknown complexity.** The heightened probability of cyber incidents increases the need for a vigilant cybersecurity approach and measures, which are especially important as new risks emerge and demonstrate new risk complexities.

3. **The disconnect of IT services, business, and the broader operating model presents new challenges.** Banks require a more comprehensive IT transformation approach that factors in legacy applications and the adoption of new technology in an attempt to balance costs, availability, and security requirements. For most banks, this move to a hybrid cloud model requires new skillsets, key performance indicators (KPIs), and risk measures that connect supporting functions to the front of the bank in one holistic, digital IT operating model. An effective, practical, and consistent operating model across all IT domains also aims to identify, manage, and address risks. Such a taxonomy ensures incorporating the many risk sources and their interdependencies in one model that produces real-time recommendations to banks, including ease of change or transformation, necessities for investments, and more.

> “Technology is one of the greatest enablers in our day and age, but also presents potentially high-impact risks.”

The research

In our managed services practice, we turned to 20 of our global Vice Presidents who look after 20 of our financial shared services customers and their technological scope under Kyndryl management. These 20 customer institutions encompass a total of USD $3.5 trillion in assets under management, a total revenue of USD $294 billion, and an average market capitalization of $101 billion. Our survey data followed a combined approach of qualitative interviews and standardized quantitative data sampling for each of the respondents.

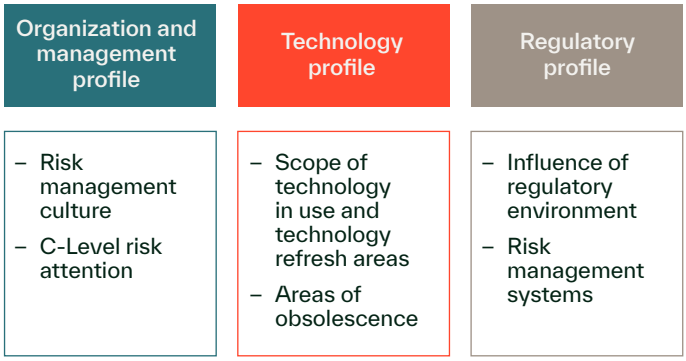


Figure 1. Overview of the six trends and results within three distinct profiles

Organization and management profile

The future of risk: The rise of end-to-end risk responsibility

In our sample of financial shared services customer organizations, a shift in risk management distribution is prevailing. Five years ago, financial and market risks were among the most important risk management areas. 18 out of 20 financial shared services respondents state that technology risks now account for at least 50% of the overall risk picture. In addition to market movement, technology is now recognized as a source of company changing events, holding reputational, financial, and existential power. Accounting for the increase in complexity and criticality of risk (for example, cybersecurity and business continuity), 40% financial shared services accounts have started to establish a stronger end-to-end responsibility where the business owns the upkeep (budget, costs, upgrades, maintenance, and more) of the apps, systems, and programs in use.

Attention to IT risk from C-level executives drives stronger risk governance systems

63% of respondents state that in the last five years, the discussion of technology risk at the highest level of the company (CEO and/or CIO) has increased. Age of the system, the critically of apps, the age of technology workforce skillsets, and the necessity and impact of technological investments are all factors board members are increasingly involved in. An involved and technology risk–attentive C-level executives have an effect on other factors, too. In accounts where C-level members are highly involved in IT risk management, stronger internal risk governance structures and heightened IT investments can be observed.

Technology profile

Age of hardware associates risks of outages and incidents

50% of interviewed financial shared services organizations point to the age of the underlying hardware and its impact on major outages and incidents as one of the most pressing technology refresh topics. 11% of respondents see aging software and the associated risk as less critical than aging hardware. These respondents were following an understandable line of reasoning informed by their experiences: incidents that happen in connection to hardware lead to long outages, while software incidents tend to result in shorter outages. As a result, these respondents are highly alert toward timely hardware refresh.

Launching technology transformation programs with a focus on stability and resilience

50% of respondents reported the launch of a major technology transformation program in the past five years. In these cases, the programs were launched after one or more major outages with large reputational and/or financial losses for the financial institutions. While the operationalization of these programs varies between interviewees, all of them are linked to optimizing obsolescence, operational stability, and resiliency. Many of these accounts reported that the outages served as a lever for finding financial resources to fund the transformation programs. A pivotal momentum was necessary to streamline political forces and funnel financial investments for necessary—and, in some cases, overdue—technological transformations.

Regulatory profile

Vehemence of regulator actions drives risk appetite, service quality, and technology investments

95% of respondents implemented a positive business case for technological investments. Driven by a regulator that imposes severe punitive measures on willfully accepted business risk, 50% of these companies adopted a rigid risk governance structure. The regulator's intent to drive good business behavior translates to higher rates of C-level attention to risk, lower overall risk appetite, higher investments in hardware refresh, and overall constant technology refresh. These respondents were also more advanced in moving towards hybrid cloud models for both cloud strategy and implementation.

Total cost of obsolescence versus individual risk: The emergence of cumulative risk management

The traditional view toward capital risk management in financial shared services does not account for the multi-layered effects of complex IT dependencies. 85% of financial shared services respondents recognize the need for a more robust risk management system that accounts for interrelated risk aggregation. With the introduction of DORA and BASEL III and IV, the positive impact of stable, reliable IT operations and infrastructure on overall ROI are much more accentuated. Any business disruption or system failure needs to be accounted for in banks' internal loss multiplier (ILM) calculations (BASEL III) or will lead to additional regulatory fines and findings (DORA).

In our sample, banking account customers with a higher affinity for following regulations, higher pace of technology investments, more technological currency, and higher attention of board members toward technological risks and necessary changes had the most evolved target operating models. These respondents tended to intelligently anchor decision-making and responsibility in their organizations and structurally necessitate IT investments (in spending as much as the actual migration work) between the front and back of the bank.

Conclusion: The future of bank risk management

We've come to understand that future bank risk management is a significant departure from today's practices in multiple areas. Banks face the multifaceted challenge of increasing efficiency and effectiveness not only when identifying and mitigating risks but also when supporting business and customer needs. They need to become better in supporting decision-making across the entire bank, think about technology and IT modernization in a more holistic way, and prepare to incorporate tighter regulatory expectations.

We've identified three recommendations to support banks in addressing these challenges:

1. Empower risk function and evoke positive risk culture

With shifts in regulation, technology, and the market, risk management functions are likely to focus on growing analytical and consultative services throughout organizational relationships. By using big data (for example, through modeling scenario planning and automation) financial services institutions can reduce bias in IT risk decsion-making while also reducing non-financial risk. Using data and technology and integrating business and IT functions provokes a stronger overall risk model. With increasing financial and reputational threats to risk posture, financial institutions may want to rethink existing governance of decision-making, budgeting, and ownership. Separating the latter enables more purposeful IT spending actions and decision-making.

Some practical implications include overseeing the IT risk governance and ownership model, recurring IT risk awareness campaigns and trainings, the initiation of a risk committee that includes board members, and making IT risk and its facets—top IT risks, past critical IT incidents, IT investments, risk management culture, vendor risk, and more—a regular board meeting agenda item.

2. Advance IT operations model

Technology in financial services institutions is a complex undertaking and its assessment, maintenance, and transformation requires a comprehensive IT transformation plan. While the transformation can come in varying forms and shapes—be it the move to a hybrid cloud model, new technological skillsets, updated KPIs and risk measurements where the back of the bank connects to the front of the bank, or infrastructure updates—they must all integrate into one overarching belief: the integration of IT foundational services and the line of business in a broader operating model.

Technology risk is, in its nature, less prevalent than credit and market risks, and traditional risk management models and traditional non-IT risk maintenance cycles are hardly applicable. With the acceleration of technology and the challenge it poses for the maintenance of an entire technological estate, new risks like cybersecurity and financial model risk are on the rise.

For practical purposes, the required IT operating model links IT business drivers (growth, costs, risks) and connects them to required operating model components (governance, management processes, tolls, technology) to enable IT risk management across the organization and link them back to the institution's IT management areas (service continuity, vendor management, IT strategy). While the names or configuration of these areas may vary from company to company, they are typical of the activities required to implement IT capabilities in a financial organization. Risks may still occur in such a model due to unsound management or delivery of any of the components, but the inherent design of accountability and comprehensiveness reduces the likelihood.

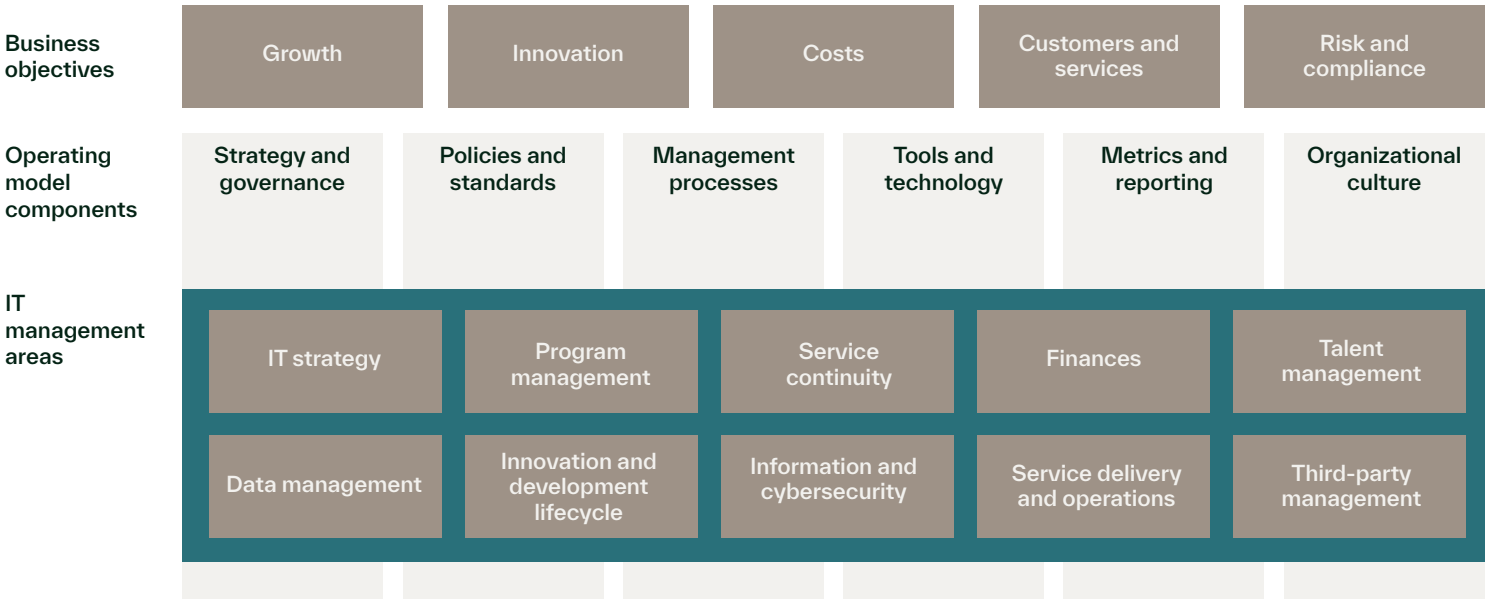


Figure 2. Integrated IT operations and risk management framework

3. Embrace new technology and tackle legacy technology

With the substantiated importance of technology risks, taking risk-based approaches becomes an important element for financial institutions' continuous success. In this effort, IT risk management is stronger when combined with a proactive view on IT risk prevention and transformation. It's vital to actively account for and manage the age of IT infrastructure elements (hardware, software, middleware, networks), the availability, criticality, and stability of its components (apps, servers, databases), and the IT security framework throughout the organization. A taxonomy around all these elements ideally ensures the identification of blind spots and produces real-time recommendations for prioritized actions.

Financial institutions recognize the increased importance of obsolescence, availability of skillsets, outages and incidents, and the pace of technology change itself on their overall wellbeing. Delaying the refresh of obsolescent technology components poses not only further risks, but also impacts the entire technology transformation with interdependent elements. Mitigation strategies range from amplified outsourcing practices, spurring multiple vendor and vendor risk management scenarios with the need for alignment on cost and length, to stalling tactics like reducing movement in present and planned transformation activities, triggered by a sunk-cost effect of elapsed time and resources.

The transformation of legacy technology is no simple endeavor, but it ultimately cannot be avoided. Bygone time and institute-specific characteristics determine the outcome of these transformation efforts.

Throughout the years, financial institutions have always faced challenging demands, profound changes, and growing complexity. Today's environment is no different in this regard. But technology, its threats, and their magnitude—be it security, obsolescent IT estates, unfit strategies and transformation roadmaps, or dated governance models—are a differentiating factor among financial institutions. How these organizations chose to react and structure the resulting complexities will determine their success.

Acknowledgments

The authors wish to thank their many colleagues in the global banking and risk practice—including Ajay Sethi, Andrew Alberti, Andrew King, Andrew McDougall, Andy Hughes, Anton Wilsen, Antonio Raposo De Lima, Arto Sorvoja, Brian Medeiros, Bruce Herholdt, Dan Himmerich, David Gajdoš, David King, Davide Veronese, Edward Gähwiler, Harish Ramamoorthy, Isidro Carrasco Jativa, John Graham, Jose de Vera, Katsuhiro Kojima, Kinichi Iida, Kiyotaka Kagawa, Luca Chiarito, Masayoshi Shino, Matthew Kea, Pablo Berges Galvan, Rajat Rao, Ravikiran Gullapalli, Regina Urquhart, Sharon Sauve, Sonia Basser, Tim Coates, Tim Hands, Wojciech Kisiel, Yoshitaka Seki, and many more—for their contributions to this report.

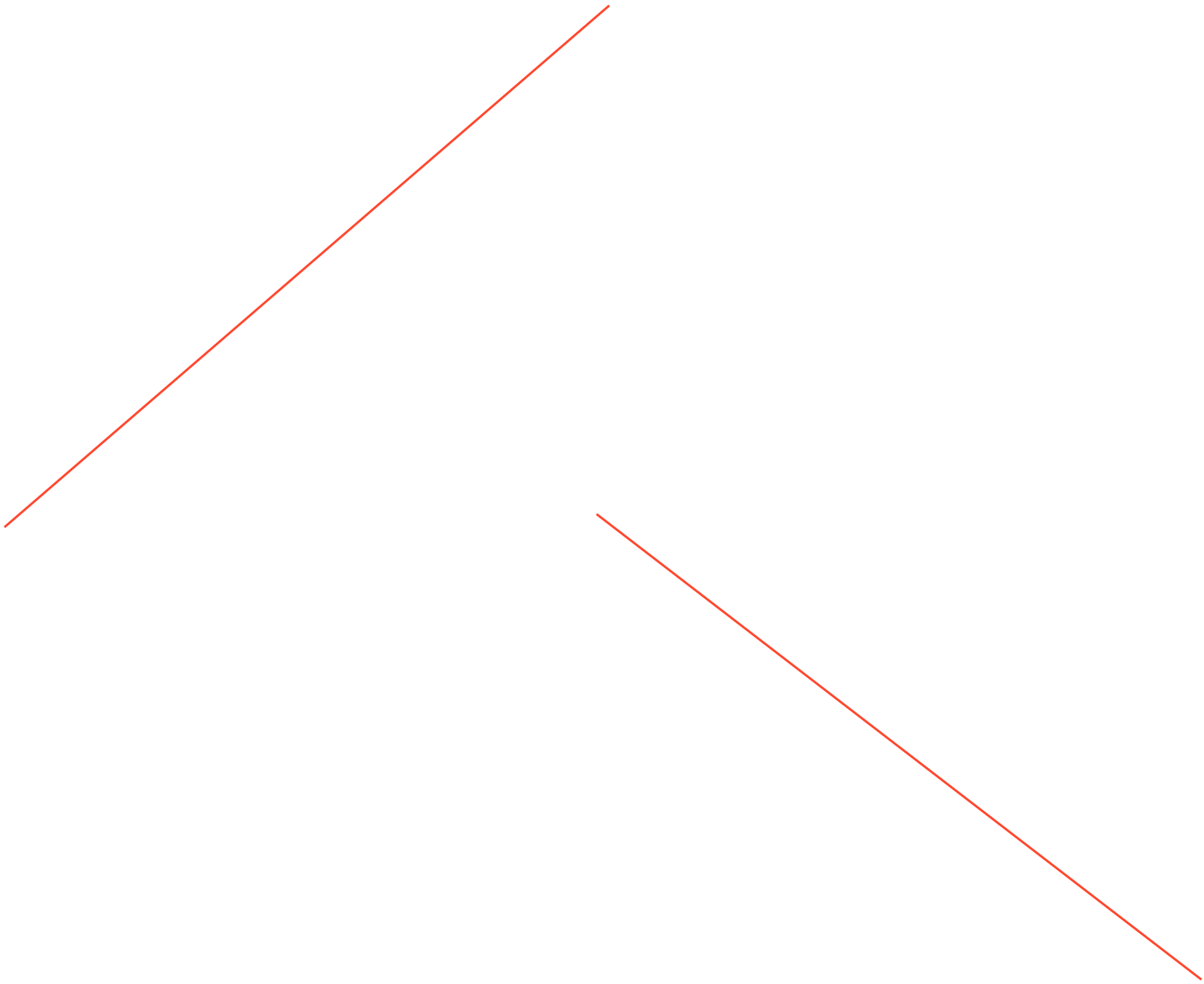
The authors also wish to thank the many CIOs, CROs, and senior risk managers with whom they discussed this research. These individuals provided invaluable insight into industry challenges. Finally, they wish to thank Rebecca Hardy, Toni Chester, Rachel Small, Zoe Katz, Laura Dragonu, Prashant Kaushal, and the entire Kyndryl Content House for their editorial support.

Carina Himstedt is a Senior IT Consultant at Kyndryl's Frankfurt office.

Merlin Jung is Managing Partner & Global Banking Community Leader located at Kyndryl's Berlin office.

About the research

This paper draws on extensive quantitative and qualitative research amongst 20 Kyndryl financial shared services customer account teams in North America, Europe, and Asia during Summer 2023.



kyndryl