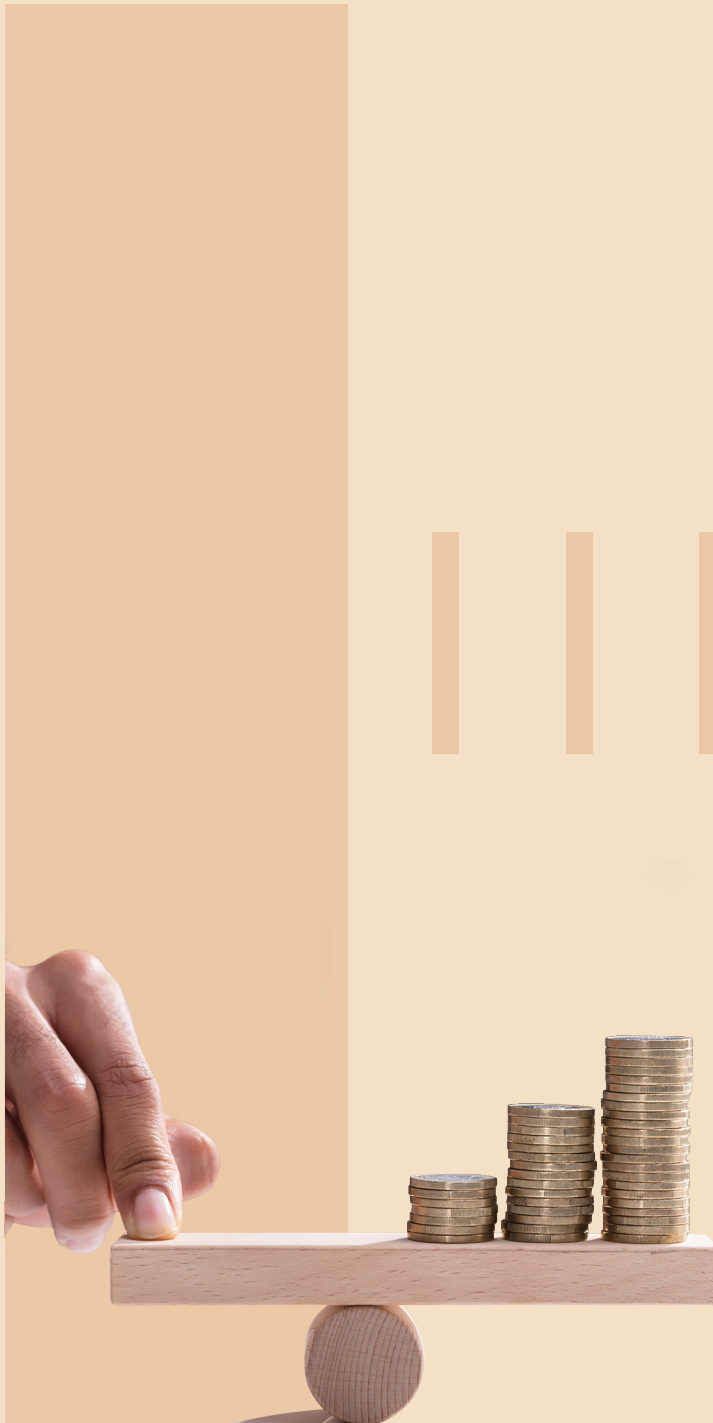


BALANCING OPERATIONAL RISK AND PRODUCT INNOVATION AFTER COVID-19

Losses from operational risk have been rising, and will become worse due to COVID-19. But few banks have adequate controls in place. New data-centric platforms that combine a wider set of metrics and enable real-time scoring are needed.



Ten years on from the subprime debacle, banks are still struggling to manage risk.

Huge levels of market volatility have exposed gaps in their practices. Many have defaulted on loan repayments, folded or gone bankrupt. American International Group, the large U.S. insurer, has been cut in half over the years. The firm incurred about \$25 billion in losses since 2008 through insuring risky credit default swaps.¹ Others have fared even worse. The closure of First NBC Bank in 2017 was the fourth bank failure in the U.S. that year. Two years after it disclosed problems with its internal controls and accounting practices, federal and state regulators seized the institution, claiming that the bank relied too heavily on volatile funding sources and illiquid assets.² And the pains go beyond credit and market risk. In the decade after the financial crisis, losses from nonfinancial (or operational) risk alone amounted to over \$300 billion, stemming from a wide range of breaches in controls, conduct and security.³

According to the Financial Times, only three of the 30 “global systemically important banks” were compliant with the Basel accord by 2017, even though the legislation came out in 2013. Many cited that new standards were too specific, or that old IT systems made it difficult to integrate information while the pace of technological innovation had left them behind.⁴ What is more worrying is that, by 2020, banks still have not achieved significant improvement in their processes to define what constitutes different types of risk, and how they should be combined when new products hit the market.

And now, with COVID-19 shaking markets, banks have no secure benchmark against which to measure their exposure to different types of risk,

and decisions based on past pricing models may not hold true any longer.

Banks must act quickly, understand what types of risks they are exposed to, monitor them effectively and put in place a risk mitigation strategy that bakes these risks into the valuation of the products themselves. Doing so will ensure they don’t run afoul of regulators, all while doing much to shore up customer confidence and safeguard their businesses from malpractice.

Measuring risk slows innovation

Basel data standards are for the most part quite basic. They say that big banks should always be able to paint an up-to-date, comprehensive picture of the risks they face.⁵ Once the risks are known, banks should develop a mitigation framework.

Operational risks are losses from failed internal processes, people and systems

But there is a problem. While banks are generally quite good at measuring their credit exposure and the downside effects of market risk, little proactive thinking has gone into determining “operational” risks. These are losses from failed internal processes, people and systems.⁶ Real-world examples include losses when an important trading partner goes bust or an unforeseen event occurs, such as when a natural disaster strikes or when an ATM network goes down. Employee malpractice or human error is also an oft-cited reason for operational jeopardy, especially when IT disruption or data compromise is involved (see Figure 1). Legacy IT

systems are especially fraught with operational risk, and have a heavy impact on future financial health. The challenge is that these risks are wide ranging, are often nebulous and are difficult to predict and protect against. And having more money in the bank doesn’t easily rectify the situation.

The LIBOR rate-setting scandal, which came to light in 2012, is a good example. Here, bankers at many well-fed financial institutions manipulated the exchange rate to benefit their derivatives traders. As LIBOR is an indicator of financial health, these traders were able to make the bank appear stronger by reporting fictitious rates, substantially increasing the riskiness of financial products being traded. This problem went undetected for almost 10 years.⁷ Once the scandal became known, regulators in both the U.S. and Britain meted out \$9 billion in fines as well as a slew of criminal charges. The banks involved also suffered bad press and ill favor with corporations that were affected by the rate-fixing. That such a debacle could have happened in the first place, without any oversight or controls in place, is indicative of a landscape where many corporations don’t know what operational risks they are exposed to, let alone have methods for quantifying them.

Figure 1. Operational risks cover a wide and diverse range of events

Top 10 operational risks in 2020			
	2020	2019	Change
IT disruption	1	2	↑
Data compromise	2	1	↓
Theft and fraud	3	5	↑
Outsourcing and third-party risk	4	6	↓
Resilience risk	5	–	
Organizational change	6	4	↓
Conduct risk	7	10	↑
Regulatory risk	8	7	↓
Talent risk	9	–	
Geopolitical risk	10	–	

Source: Risk.net

Even if these risks are known, there is the added hurdle of pricing them into financial instruments, which are often based on algorithms that might also be exposed to further operational risk. While market risk is about the known (based on available pricing information), operational risk is about the unknown (trying to predict the future). Not getting a handle on both forms of risk is a considerable reason for today's financial woes.

Another problem is how to estimate expected as well as unexpected losses from operational risk. These losses have an impact on the capital structure of the bank, and let the regulators know how much buffer capital a bank should hold in the event of a crisis such as COVID-19. Some methods use probability distribution functions. They run an algorithm for each business line within the bank, for different risk types, all on internal data. However, getting this data is difficult, and the data often cuts across business units. The models themselves are complicated by the

fact that they use extrapolation to measure the tail of the loss distribution (the unexpected losses), which can lead to errors.⁸ Further, the metadata hierarchies vary between institutions, so there is no standard way of comparing losses.

Finally, measuring and mitigating risks slows things down. Many financial products are very complex, and quantifying underlying risk from products such as credit default swaps or derivatives takes time, effort and good data from across the enterprise. However, risk officers must work in tandem with business owners in new product strategy and placement. This product innovation is important to keep in step with nimble disruptors in fintech. Banks know this, which is why compliance with ever-tightening regulations is so restrictive. As a case in point, in early 2018, Wells Fargo, America's fourth-largest bank by assets, was penalized for putting sales quotas ahead of risk controls. The U.S. Federal Reserve halted the bank's

growth until its risk management capabilities caught up with its risk appetite.⁹

A bank must balance product innovation and speed to market while managing operational and financial risk

The question is this: How does a bank balance product innovation and speed to market of fancy new products (what traders want) while managing operational and financial risk (what risk officers want)? A more dynamic approach to risk management is needed, one where the firm behaves like an organism that "feels, thinks and acts based on intelligent information at the point of insight," what Infosys calls a "live enterprise."¹⁰

Front-loading risk management

To sense, feel and react quickly to new forms of operational risk, better, more modernized and more sophisticated data is needed. This will tell risk officers very quickly whether computer systems are a liability, or whether there is a high risk of bad behavior on the trading floor. This means having one central repository for all internal data held by a bank, along with safety measures in place to protect it from internal and external bad practice, including insider trading and cybercrime. In the case of the payment protection insurance scandal that recently transpired in British banks,¹¹ this sort of data and the insights it generates would have flagged that a highly profitable insurance product was being sold to customers who didn't actually need it, or to those customers that weren't even eligible for insurance premiums.

Also, sophisticated financial products need to be priced properly in real time, based on the exposure the business has to different types of risk. This means tying together credit risk with the operational procedures that sometimes amplify the risks in the credit decision-making process. For instance, unless certain operational procedures demand that at least two people are involved in making certain advances, there is a high probability of error entering into the decision-making process. For some teams, this will mean building an embedded operational risk awareness culture, with consistent messaging across the organization.

A data platform that ingests data in real time can be used to perform advanced analysis of operational risk

Technology can help in both these cases. A “big data” platform can be built that ingests data in real time and performs advanced analysis to measure the risk of certain trades and operational processes. This will enable traders to build safer, more innovative products, using a wider set of operational metrics, including a bank’s business strategy and exposure to other vulnerable entities. For instance, when Lehman Brothers ran into trouble in 2008, global markets ground to a halt as banks determined their relative exposures to the failing bank. Since the platform would ingest data in real time, scoring products would be quicker and innovation would increase, supplementing performance in scoring credit and market risk too. This platform would also benefit from oversight by both the first and second lines of defense within the bank and enable higher levels of security than does traditional infrastructure, which is often siloed in disparate business lines.

Additionally, operational risk should be baked into the bank’s products from the start. Rather than dealing with problems after they occur and then seeking the root cause, this approach starts with the intrinsic risks stemming from product design, target market definition and distribution strategy.¹² Not only does this go a long way to “front load” risk management, but it also ensures regulatory concerns are dealt with upfront. For instance, the Australian Royal Commission and its equivalents in Europe and the U.S. state that banks are held liable for any omission of risk in their products. They also state that risks must be transparent to customers, be well understood and be communicated in a timely fashion to all key stakeholders. This is only possible if the product itself contains information about its operational risk exposure.

A helicopter-level view in real time

With a data-centric platform and operational risk baked into products, risk officers can approve or reject risk in real time and have an overview of the entire asset portfolio. They can use the platform to take alternative perspectives on a product through clever simulations, and also review the operational risk around trader behavior and cybercrime. It is also a great first step to ensure compliance with the Basel accord and increased supervisory standards on individual accountability such as the UK senior managers’ regime.

With correct processes built on a real-time, data-centric nervous system, pricing models will have robust reference markets, take underlying cash flows into account and give risk officers a helicopter-level view of the entire product portfolio just when they need it. And by baking in legitimate business practices into the risk-rating

of a product, credit, market and operational risks will be more closely linked, and banks will be better able to handle unexpected loss events when they occur. It will also mean that customers are front and center in strategic decisions, since the bank cannot simply drift where profit would otherwise drive it. In today’s market, such good-play will ensure operations are fail-safe, while doing a lot to win new friends in high places.

References

1. [Falling Giant: A Case Study of AIG](#), Gregory Gethard, March 30, 2020, Investopedia
2. [The decline and fall of First NBC Bank: What happened?](#), Richard Thompson, May 6, 2017, Nola.com
3. [Too important to ignore: how banks can get a grip on operational risk](#), Dr. Tom Huertas, EY
4. [Banks' approach to risk data is deeply inadequate](#), Charles Taylor, July 15, 2018, FT
5. [Basel III](#), Andrew Bloomenthal, April 17, 2020, Investopedia
6. [Operational risk](#), October 2007, Wikipedia
7. [The LIBOR Scandal](#), Julia Kagan, May 29, 2020, Investopedia
8. [Measuring operational risk in financial institutions](#), John Evans & Amandha Ganegoda, 2008, FINSIA
9. [Banks have learnt their lesson on risk management](#), Alexander Dill, Dec. 16, 2019, FT
10. [Infosys Live Enterprise — A Continuously Evolving and Learning Organization](#), M.R. Tarafdar, Jeff Kavanaugh & Harry Keir Hughes, July 2019, Infosys Knowledge Institute
11. [PPI scandal hits £50bn after claims rise at Lloyds and Barclays](#), Nicholas Megaw & Adam Samson, Sept. 9, 2019, FT
12. See reference 3

Authors

Dr. Ashok Hegde

Vice President – Infosys
ashok_h@infosys.com

Harry Keir Hughes

Senior Consultant – Infosys Knowledge Institute
harrykeir.hughes@infosys.com

About Infosys Knowledge Institute

The Infosys Knowledge Institute helps industry leaders develop a deeper understanding of business and technology trends through compelling thought leadership. Our researchers and subject matter experts provide a fact base that aids decision making on critical business and technology issues.

To view our research, visit Infosys Knowledge Institute at infosys.com/IKI

For more information, contact askus@infosys.com



© 2020 Infosys Limited, Bengaluru, India. All Rights Reserved. Infosys believes the information in this document is accurate as of its publication date; such information is subject to change without notice. Infosys acknowledges the proprietary rights of other companies to the trademarks, product names and such other intellectual property rights mentioned in this document. Except as expressly permitted, neither this documentation nor any part of it may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, printing, photocopying, recording or otherwise, without the prior permission of Infosys Limited and/ or any named intellectual property rights holders under this document.