



WHITE PAPER

Are You Ready to Manage Risk at Social Media Speed?

April 2023

By Ingmar Broemstrup, Alice Cho, Roy Choudhury, Martha Cummings, Brian Hughes, Brian O'Malley, Bashir Today and David Wood

The recent failures of two major US banks and a Global Systemically Important Bank (G-SIB) with significant US presence makes it clear that strong risk management is a competitive advantage. Depositors, investors, regulators, and employees are asking if they can trust their bank to successfully manage its risks. They are asking whether the bank can respond quickly enough to solve issues when they arise. Many banks face these questions despite having different business models than the institutions that failed.

It is more complicated than ever to manage risk well. Banks have grown more complex, adding new products, investing in technology and analytics, and increasing reliance on third and fourth parties. After a decade of relative stability, macro conditions are shifting quickly, as is the behavior of customers and counterparties, with social media driving herd behavior in areas like deposit outflows and margin calls.

Learning from approaches they have taken to manage cybersecurity events, successful banks are focused on increasing the speed of their risk identification and response capability to reduce response timelines to hours or days—instead of weeks or months. By focusing on what matters most, they manage the cost of investment and get the maximum value out of the resources they have in place. These banks also position themselves to grow stronger in times of crisis by making acquisitions at favorable valuations and gaining customers who seek stability.

To ensure they have the right focus, leading banks are engaging in targeted reviews of their capabilities to manage risk at “social media speed”.

Catch Risk Quickly

Keeping pace with today’s risk environment requires spotting risk quickly and proactively. Most banks keep lists of top and emerging risks that are fairly static. Leading banks, though, are reevaluating their lists in a rapid exercise to make sure the lists reflect the organization’s current business model, products, geographic footprint, balance sheet, and funding model. Banks are also updating these lists to reflect the current macro environment. New types of tools and approaches like reverse stress testing and balance sheet modeling and projections can identify the types of risks and risk levels that would cause major difficulties. Banks are applying these tools to new risks, such as short sellers or loss of major and highly connected customers. These tools can also help capture the full impacts of a risk, including liquidity difficulties causing solvency issues and vice versa.

To sustain high-quality risk identification, some banks have built risk lighthouse functions that pair risk leaders with business strategists. These lighthouse functions can both scan quickly and take a rigorous internal look as needed (e.g., by surveying mid-level business and functional executives on what they are seeing). They pay special attention to large-scale changes, including major product launches, technology upgrades, and changes to the balance sheet. Externally, these lighthouse functions use news and social media scanning tools and incident databases like ORX (the Operational Risk Exchange) to identify potential threats and trends. They also check with external stakeholders—including key investors and influential customers—and leverage interactions with the bank’s regulators.

Ensure Trending Risks Are Understood and Managed Properly

At times, banks miss the forest for the trees when confronting emerging risks. However, leading institutions strive for a broader view by focusing on the likelihood of a risk, potential impacts, and the speed at which a risk could impact them. This often requires creating an integrated view based on a stressor (e.g., a lockup of the repo markets) and an understanding of the feedback loops the stressor could generate, including any involving third parties like vendors and counterparties.

Gaining a good assessment of a risk often involves the lighthouse function bringing the first and second lines together. The first line holds the full knowledge of how the bank works, while the second line brings an understanding of all the ways a risk can manifest. External experts can also contribute a broader view, including insights from other geographies, institutions, and even other industries. As an example, bringing business, technology, and risk leaders together with external experts can help a bank understand how to better manage the risk from generative AI. This will help the risk function understand potential use cases and the value they bring, including use cases involving third parties, as well as helping business and functional leaders recognize and mitigate potential areas of concern.

Once a risk is understood, the lighthouse function also assesses the bank's approach to managing the risk. This assessment covers the availability of data and reporting to track the risk; the number and skills of the staff managing the risk; and the broader network of resources available to help if there is an incident or crisis. The lighthouse function often has the capability to redirect staff or prioritize investments required if a risk is emerging or trending quickly, even if the investments are made outside the traditional cycle. The lighthouse function can also make investments that address multiple risk types, such as rapid scenario modeling capabilities.

All of these critical risks would have a single owner responsible for an end-to-end view of the risk and its implications. This includes responsibility for coordinating across siloes and organizational boundaries in a crisis. If there is no owner assigned yet, the lighthouse function would identify one who would build the bank's response.

Streamline Governance to Act Fast

For risks with potential for rapid impact, some banks are building a fast-track form of risk governance. This often involves granting the risk owner emergency authorities once an automatic trigger occurs, like the authority many banks grant to their treasurers in a liquidity crisis. To ensure that such an owner can be effective, the bank equips the owner to activate resources across the organization, including in areas like IR, PR, communications, and regulatory relations when required. Risk owners can often activate a pre-identified SWAT team that includes a board member on point and representatives from all relevant areas of the bank, including staff able to source the right data and reporting to enable decisions.

When the situation is ambiguous, the owner will have access to an escalation mechanism that bypasses lower-level committees to convene more senior committees out of cycle, including the Risk Committee of the board. There are pre-established thresholds for when and how the board, Enterprise Risk Management Committee (ERMC), and other key stakeholders will be informed; these thresholds are aligned to the potential impact and speed of the risk.

Finally, there is no substitute for advance preparation. For high-impact risks that could move at social media speed, leading institutions have built and tested playbooks to ensure they would work in an actual event. Cybersecurity-style tabletop exercises or war games allow banks to understand how well their playbook might work and ensure that key stakeholders are familiar with the response. Certain risks will also require outside support, such as legal counsel contributing to crisis management. Having these services pre-arranged and on call makes response timelines more efficient.

Flag Changes in Risk Quickly and Clearly

Responding well to risk issues requires a good understanding of the current state. Some banks are resetting the frequency of their reporting based on the speed of a risk, such as generating intraday reports on fast-moving risks like liquidity and fraud. Many banks are also striving for better social media and sentiment monitoring to track contagion. Rather than working with the data that is available, banks are identifying the data they need and investing in automation and analytics to get it.

Several institutions are also working to spot risks faster “on the ground.” This involves training employees on how to spot key risks (e.g., the potential instability of a major counterparty) and creating blame-free, rapid escalation protocols. Such protocols are often real-time channels linked to a risk owner’s reporting team. These institutions celebrate employees who escalate—and have consequences for those who hide issues.

Finally, banks can design low-latency reporting that is clear and summarized, highlighting what has changed in the risk environment. If needed, real-time commentary can be accompanied by notation explaining that the information has not been fully confirmed. The reports would include a clear recommendation and call to action, such as changes to credit policies to address spikes in first payment default.

Resolve Issues Quickly and Effectively

When risks are newly identified and prioritized, typically there will be several issues around how they are managed. These issues can range from poor data quality or excessive manual reporting to lack of sufficient second line oversight. Leading banks scan their own capabilities to respond and make sure all issues are logged; existing, unresolved issues related to the risk are sufficiently prioritized. The risk’s owner then takes a role in issue resolution, making sure critical issues related to the risk are properly resourced and quickly closed.

When new or potential issues arise, these are flagged to the risk owner so they can be properly prioritized. Risk owners will also periodically analyze the full set of logged, relevant issues and see if there are any underlying, unresolved root causes. This creates an ongoing view of weaknesses the bank might have if the risk were to grow more important or urgent.

All of these capabilities can help banks address risks in today’s environment, where social media and faster-paced markets have reduced the time banks have to manage crises. Most banks have some of these capabilities in place and can quickly address other foundational ones, like updating their top and emerging risk list and building tools for rapid scenario analysis.

As banks build their capabilities, it’s important to engage key stakeholders and keep them informed. For many banks, this will be a new capability in and of itself. Three things are particularly important: sharing a vision of how the bank can successfully manage risks in today’s environment; updating stakeholders on progress in a fact-based way (e.g., mentioning how they are performing reverse stress testing and acting on the results); and preparing to communicate in a crisis. This communications capability is the final key ingredient—being able to tell the story of risk management at the speed of social media.

