Risk convergence creates outsized risks for banks and financial institutions

Break apart risk silos to manage and counter magnified risks

IBM

Highlights

1. Situation: the risk convergency phenomena that creates outsized risk

Financial institutions and national economies struggle with a variety of crises that cause considerable negative impacts on bank balance sheets, shareholder value and even sovereign solvency. These crises can involve complex factors such as criminal attacks, military actions, financial sector developments, natural disasters, and political and social changes. Examining such financial events reveals a pattern called risk convergence. Risk convergence is the phenomenon of outsized risk that occurs when one risk overlaps with another, and then even transforms into yet another risk.

Policymakers are well aware of this phenomenon—as one type of risk develops and grows in one silo, the risk is transforming into something much grander in scale in another silo. Historically, such convergences of risk typically involve market risk converging with credit risk. In all cases, one risk remains largely unobserved and ultimately overtakes the other in the form of a financial crisis.

Convergence of AML and prudential risk may be the most pressing regulatory issue of the moment, and certainly illustrates the power of risk convergence and impact it can bring to financial services. This convergence can be seen as three legs of the stool among conduct, prudential and efficiency. Institutions can struggle to keep up with the growing body of regulatory demands, while in parallel keeping pace with the large volume of alerts requiring review, many of which are often false positives. This drives costly compliance measures and analytical and investigative work, and labor hours.

This is why new ways of working, such as AI-assisted triage, allows human beings to keep up with the flood of signals they need to pay attention to each day. This paper discusses the challenges of managing these converging risks, and detecting the magnified threat that they represent to financial institutions.

We also review the benefits of breaking apart the risk silos that make it difficult to observe risk convergence, and some mechanisms and tools that can be used to discern risk convergence. Strategies and new technologies are available today for banks and financial institutions to identify, mitigate and protect against these risks.

The IBM® point of view is that risk convergence, complex as it is, can be managed so that the risks can be better quantified and minimized. Emerging requirements can be met by adopting new efficiencies supported by technologies like AI and machine learning.

2. Examples of convergence of risk

Each of the following examples highlights a different convergence risk, including conduct risk and prudential risk convergence, conduct risk and systemic risk convergence, and market risk and credit risk convergence. The impact of each risk convergence risk event varies, and is arranged below in descending order of impact from international market dislocation, sovereign insolvency, and institutional insolvency to major market losses.

Long Term Capital Management – The market events at Long Term Capital Management **(LTCM)** created a risk convergence situation that affected many organizations. Long Term Capital Management ran a hedge fund which had major collapses in 1998. These failures prompted the Federal Reserve Bank of New York to arrange a rescue.[1] They demanded a collective investment by each institution in LTCM to recapitalize the balance sheet and avert significant balance sheet impairment. Fourteen banks invested $3.625 billion. The goal was to help LTCM put in place an orderly wind-down, rather than allow a market rout wiping out balance sheets.

How did the LTCM crisis come to pass? Founded in 1994, LTCM followed an unusual combination of strategies. Investors analyzed the market risk implications of the LTCM strategies, and invested heavily in it. In the first few years returns were strong but after the 1997 Asian and 1998 Russian financial crises, LTCM lost $4.6 billion.

The convergence of risk happened when market volatility occurred, leading to the emergence of the correlation risk that had been created with the banks' own investment strategies. This created outsized market risk for the banks. LTCM had been analyzed as a credit risk to the banks, and not a market risk by the banks. When markets moved, the correlation risk was realized producing exponential risk for the banks. As market risk analysis and credit risk analysis were siloed, the effects of the correlation risk that LTCM ultimately created were masked.

The Sumitomo Copper Affair – The 1999 Sumitomo Copper event is in some ways is the flip side of the LTCM coin—it is a convergence of market risk and credit risk. This event, characterized by huge trading losses incurred by Sumitomo Copper trader Yasuo Hamanaka, occurred with several institutions including JP Morgan Chase and Merrill Lynch. The Sumitomo trader took positions to buy copper on the London Metal Exchange (LME). He set up deep in the money swap derivative contracts with JP Morgan resulting in an $80 million USD upfront payment. The trade was analyzed as a market risk due to the derivative contract, but not as a credit risk. Sumitomo claimed Hamanaka was a rogue trader – that he had entered into unauthorized trade arrangements with the banks. Sumitomo Copper lost at least $2.6 billion. The banks suffered trade losses, fines and legal judgements.

Such risk would have been identified had the banks analyzed the trader relationship under stricter credit risk protocols. In effect, the trader received loans from the banks that were structured as derivative contracts, and which were viewed only in terms of the market risk silo.

> "Prosecuting fraud is not a priority for law enforcement, so it's better for us to interdict than it is to pursue investigations and recoveries. Law enforcement usually only catches the mules, not the real operators."
>
> **Head of global fraud management for U.S.-based money center bank**

3. Money laundering risk convergence

AML risk, supervision, and enforcement are not new. The Bank Secrecy Act was enacted in 1970, the Financial Crimes Enforcement Network ("FinCEN") was created in 1990, and the world began to appreciate the complete impact of money laundering and terrorist financing after the September 11 attacks in 2001. Just one month later, the U.S.A. PATRIOT ACT was signed into law (on October 26) and the modern AML era had begun. Financial institutions have made enormous investments in AML compliance programs and a number of institutions have paid significant fines before making such investments for violations of law and failures to detect, monitor and manage money laundering risks.

In today's banking climate, where digitization of banking is opening new channels of exposure for banks and their clients. This is creating a convergence of risk involving money laundering risk and other types of risk, like cyber risk, conduct risk, and fraud risk. Today, we can see signs that money laundering risk is converging from a conduct risk to a prudential risk.

With the deluge of events, news, and changes the potential for "alert fatigue" is palpable. Without proper triage, decision makers will begin to ignore alerts as the majority of them will not apply to an individual organization. For example, the Thomson Reuters 2019 study, "Cost of Compliance 2019: 10 years of regulatory change" cites that the number of alerts went from 8,704 in 2008 to 57,364 in 2018.

Financial institutions and regulators the world over are facing a major crisis with money laundering, due to the growing sophistication of financial criminals in evading sanctions and moving illicit money. Efforts by financial criminals are significant, and do not reflect isolated occurrences, but rather systematic attempts to seek out weak links in the chain. And, this systematic approach to financial crime brings with it complex issues for the global financial system. The systematic methods and techniques abound in non-traditional formats and ways. Circumvention techniques are proliferating and are being used to evade, or by-pass, the controls and processes currently in place in monitoring systems and embargoes.
Let's consider two circumvention examples:

Russian money laundering business model – In this financial crime model, money launderers use real estate loans as mechanisms to place and layer illicit funds. On the surface, the loan appears to be standard and legitimate. As the loan is cash collateralized with deposits in a high net worth individual's account, it does not attract any risk weighted asset rating, nor does it raise credit considerations as the deposits are sufficient to repay the loan. The loan is approved, payments are made each month, and the mortgage appears to be a healthy, performing loan.

However, closer review of the customer's intent will raise a question about the legitimacy of the loan. For instance, the loan may be taken by a non-resident alien for property in a third country. The loan rates might be high, with monthly interest payments simply representing the cost of placing the money. We must conduct a business model review. Through this lens, it is much easier to see that there is no legitimate purpose for the loan. Additional types of fraudulent businesses and transactions may be involved. The Troika Laundromat[2] is a variation of this model.

Troika Laundromat example – The $8.8 billion Troika Laundromat included real estate purchases in and outside of Russia, as well as fake trade deals, reinsurance fraud, a fuel pricing fraud scheme at Sheremetyevo Airport and much more. Between 2006 and 2013 perhaps twenty banks were involved – and many of the counterparties had compliance programs in place. Troika fraud occurred in multiple channels and across domains, with thousands of transactions. How did the fraudulent activity go undetected for so long?

Part of the problem is static or passive anti-fraud methodology. Ineffective compliance and risk management functions are another factor. Outmoded technology is another. The lesson is that AML today involves multiple types of fraud, tax evasion, illegal trades and other crimes in a type of interdisciplinary approach. For Troika, the tools to gather all the data were not available to support a holistic, self-learning approach. As is often the case, decisions were based on siloed and incomplete data.

Banks need more dynamic approaches to help them separate suspicious activity from low risk transactions. They also need new tools to understand whether their customers and counterparties are using them to facilitate criminal acts. Several other incidents involving cyber-breaches, fraudulent conduct, and governance and compliance gaps are summarized in Figure 1.

Figure 1: Additional examples

	Summary	Perpetrators
Bangladesh Bank theft (2016)	– US$951 million stolen, initially seen in SWIFT transactions – Approximately one-fifth of losses recovered	Suspected: North Korea, Lazarus Group
Australian banking Royal Commission inquiry (2017)	– Estimated taxpayer cost of inquiry US$51 million – Bank tax levies estimated at US$4.6 billion	Four major Australian banks
Capital One data breach (2019)	– 106 million customer credit card applications and accounts hacked	Hacker; former vendor: Paige Thompson

Figure 1 – Cyber-breaches, fraudulent conduct, and governance and compliance gaps

Notwithstanding this investment and focus, the sophistication of money laundering has made prevention and detection even more difficult. And with newfound prudential implications, we are witnessing the confluence of a number of different risk types. To untangle them, we must stop analyzing risk in the typical, siloed manner to which we are accustomed, with distinct frameworks for credit, market, liquidity, compliance, conduct and other risks. Instead we must obtain and analyze data that crosses these silos to detect the convergence of risk the way it occurs now.

Typically considered a conduct risk, AML risks now bring reputational and prudential impacts. Current events leave no doubt that the results of AML risk have reached new heights. Examples of banks that suffered severe consequences as recently as 2018 include ABLV Bank, Pilatus Bank and Versobank.

Bank (Region)	Risk situations	Consequence
ABLV Bank (Latvia)	– The U.S. Treasury calls money laundering a "pillar" of the bank's business, and designate it an "institution of money laundering concern." – The European Central Bank (ECB) cuts off access to the bank's funding mechanisms by determining it is an "institution failing or about to fail."	ABLV Bank enters into a voluntary liquidation.
Pilatus Bank (Malta)	– Pilatus Bank's chairman-owner is arrested in the U.S. on charges of money laundering and sanctions. – Maltese authorities seize control of the bank's operations, leading to discovery of money laundering inside the institution.	The ECB revokes the bank's license.
Versobank (Estonia)	– Estonian banking regulators find grave deficiencies in the bank's anti-money laundering compliance system. – Bank fails to remedy systemic breaches in its AML control framework after repeated warnings.	The ECB revokes the bank's license.

We must stop analyzing risk in distinct frameworks for credit, market, liquidity, compliance, conduct and other risks. Instead we must analyze data across these silos to detect the convergence of risk the way it occurs now.

The challenges are not limited to small institutions and peripheral jurisdictions. Money laundering through Danske Bank led to the forced resignation of a number of its senior managers and a drop in share price of more than 25%. Similarly, money laundering deficiencies cited by regulators and law enforcement at ING, Deutsche Bank and others has been followed by billions in fines, resignations of senior management and de-risking of some of the institutions' businesses (e.g., correspondent banking).

These events not only increase risk to banks, but more broadly, to the full financial sector. In fact, there are correlations between the strengthening of a country's anti-money laundering framework and its overall financial health:

- Fitch placed Swedbank's rating on rating watch negative, following the identification of money laundering scandal.
- S&P lowered Malta's Banking Industry Risk assessment's score.
- In Cyprus, the implementation of a new AML framework for Cypriot financial institutions formed part of the country's bail-out terms, following its 2012/2013 crisis.

This linkage has now been clearly recognized by global financial supervisors. In 2018 for example, Valdis Dombrobskis, the current Executive Vice President of the European Commission stated, "What we see is that there's clear interaction between prudential supervision and anti-money laundering issues — we have seen how quickly money laundering can turn into financial issues . . . we now need to draw lessons from those cases."[3]

4. Benefits of breaking down risk silos

In today's business environment, defined by sustained market volatility and ever-increasing regulations, organizations need the ability to integrate enterprise-wide risk management processes and multiple regulations. There are significant opportunities offered by embracing holistic advanced analytics capabilities and AI to formulate better cross-risk business decisions.

The prudential reasons to acknowledge risk convergence and building an enterprise view of risk are indisputable. But banks can gain in several other areas by approaching risk management in new ways. Clearly, better risk management helps institutions (and the financial sector) as a whole prepare for and prevent the unexpected, but analyzing across risk types can also bring the following benefits:

- **Board friendly** – Providing a single view of risk, consolidated within comprehensive reports and using consistent measures allows for a single view of risk, rather than relying on multiple reports. All of this brings greater shareholder value and transparency for the organization.
- **Consistency** – Consistent and common approach to risk identification, mitigation, and reporting across the organization allows for the breaking down of silos and allowing for aggregating of risk indicators across risk types.
- **Efficiencies and cost control** – With greater insight into risk across risk stripes, institutions can focus investment and resourcing in the highest risk areas and demonstrate appropriate coverage without overspending in lower risk areas.

5. Platform strategy for automated, proactive monitoring

Banks need a holistic view of risk including first line of defense, in an intuitive, manageable platform. The goal is an integrated governance, risk and compliance (GRC) portfolio. This provides a centralized repository which automates the process of identifying, analyzing and managing new policies.

- A key capability of a GRC portfolio is the regulatory compliance management module, which helps firms manage new and changing regulations with cognitive, artificial intelligence (AI), workflow and automation capabilities. Such regulatory compliance management gives financial firms complete visibility into regulatory changes, their obligations, and associated internal business controls. Financial organizations can use the platform capabilities to successfully understand and manage risk across data held in disparate institutional, departmental and geographic silos.

- This holistic approach is well-suited for hybrid multicloud environments that demand mission-critical performance, security and governance — in public clouds, in private clouds, on-premises and on the desktop. To help counter converged risk, such a portfolio delivers a holistic, advanced approach to AML, KYC, regulatory compliance, data analytics and artificial intelligence (AI).

- Regulators have signaled support for institutions applying new technologies, particularly AI. In December of 2018, five US government agencies, including the Financial Crimes Enforcement Network (FinCEN) and Office of the Comptroller of the Currency (OCC) issued a joint statement on innovative AML and anti-terrorist financing efforts. The document encourages banks to implement innovative approaches, specifically referencing AI.[4]

- AI, advanced analytics, automation are applied to increase efficiency and effectiveness across AML compliance, KYC, fraud prevention and employee conduct surveillance. Consolidating data across dimensions, solutions are designed to augment human performance in combating financial crime and fraud. This alleviates the time-consuming, labor-intensive and often inaccurate processes of financial crime prevention operations.

- Machine learning is an AI-driven service with features for building, custom training and deploying machine learning models and neural networks. Tools fully automate the training process for rapid prototyping, allowing complete control to create a custom model that matches business needs.

- Organizations can maintain regulatory compliance by tracing and explaining AI decisions across workflows, and intelligently detect and correct bias to improve outcomes. A best-in-class platform makes it possible by tracking and measuring outcomes from AI across its lifecycle. It adapts and governs AI to changing business situations — for models built and running anywhere.

– Data lakes are next-generation hybrid data management solutions that can meet big data challenges and drive new levels of real-time analytics. Data in the lake might include everything from highly structured files to completely unstructured data such as videos, emails and images. Users can tap into the tremendous potential of previously unanalyzed data and make smarter, more agile, data-driven decisions.

– Financial organizations and banks need enterprise-grade solutions to help build a data lake and then manage, govern, access and explore big data. Best-in-class solutions combine cost-effective, open source technology with real-time analytic capabilities. Governance features ensure data is relevant and trustworthy.

– Predictive models and extra contextual data help correlate multiple sources of intelligence to spotlight high-dollar organized activity while reducing false positives. These capabilities allow better detection and faster response by the special investigative units (SIUs) and financial insights that enable proactive and anticipatory decision investigative units (FIUs).

– Investigative teams can leverage rich functionality for KYC, list screening, AML and various types of fraud alerts and cases. Alert and case management systems built on a common baseline of financial crime data allows different alert and case types to coexist on a shared infrastructure. The established governance process validates new rules, models, and watch lists that are crucial to the feedback loop in the management lifecycle, helping to address dynamic changes in fraud and AML.

– Enterprises also need an integrated environment with intuitive graphical tools designed to make it easy to develop, train, manage models and deploy AI-powered applications. Authoring and creation capabilities empower organizations to more easily tap into data assets and inject predictions into business processes and modern applications. Individuals can generate charts and visualizations and refine data in a powerful, intuitive environment.

6. Next steps: five action items

While the excitement and opportunity of AI leads many to start with the results, the fundamental ingredient is AI is high quality data, which all organizations struggle to achieve. Without this foundation, AI can result in inaccurate decisions which would negate any benefits.

IBM has created a structured adoption methodology that defines five steps to AI readiness and ultimately AI success. These incremental rungs on the "AI ladder" helps clients not only maximize the benefits of their current AI project, but also build a structure for yet-to-be-considered initiatives. These are the five steps to ensuring AI success:

1. Collect: All organizations have data, but often the process to gather that information is inconsistent and ad hoc. By creating consistency in how data is collected, simplifying it and ensuring it is easily accessible, AI can make better decisions based on all data, not just available data.

2. Organize: Once data has been collected, it needs to be structured in a way that makes it ready to be utilized for the type of analysis that will take place. Normalizing this information and making it accessible ensures it will fit the current purpose as well as future use cases.

3. Analyze: After the data architecture has laid out a solid foundation, based on uniform collection and organization, organizations can analyze that data in a way that is consistent and delivers insights at scale. In addition, creating a data lineage that can unearth which sets of information led to which insights helps provide both trust and transparency that the technology is delivering unbiased, information-based decisions.

4. Infuse: When most organizations think of the benefits of AI, they immediately jump to how it can be incorporated into their business. But even within this step of the AI Ladder, there are levels of maturity and complexity that shape the impact of AI on the business.

- Learn: Initially, organizations experiment with new AI approaches and uncover value to prove the business case. This can be a valuable first step, as it showcases potential.

- Augment: As part of the second phase, organizations look to enhance the operation of existing systems with AI for greater efficiency and to reduce costs. Often, this can be achieved quickly and helps free up funding to continue investment in the later phases.

- Transform: While many existing systems can be enhanced, others will be replaced with more modern solutions. This is not a traditional one-to-one replacement of an old system with one that achieves the same results, but instead a reinvention of the current capabilities using AI to improve the results and reduce the burden of operation.

- Optimize: As a last phase of this step, organizations will move beyond more limited use cases to utilize insights and information across channels and the enterprise. This will create a more agile organization, linking traditionally siloed groups from marketing and sales to risk management and compliance. It helps improve the customer experience by understanding context and anticipating their needs.

5. Modernize: The ultimate goal of AI is not technology for its own sake, but instead to improve how quickly and effectively the organization can adapt to changes. By removing the traditional barriers of how and where information is located, organizations can unlock greater value of data for an AI and multi-cloud world.

About IBM RegTech

IBM offers a unique combination of financial services, technology, and regulatory expertise. We help banks and financial institutions make more timely and risk-aware decisions by applying the latest advancements in artificial intelligence, machine learning and automation to the risk and compliance process. To learn more, visit ibm.com/RegTech.

Authors

Michael Curry, Vice President IBM Regtech, IBM Cloud and Cognitive Software

James Ray Jr,. Principal at Promontory Financial Group, an IBM Company

Footnotes

1. Stephen Slivinski, "Too Interconnected to Fail? The rescue of Long-Term Capital Management," Economic History, Summer 2009. https://www.richmondfed.org/-/media/richmondfedorg/publications/research/econ_focus/2009/summer/pdf/economic_history.pdf
2. https://www.occrp.org/en/troikalaundromat/
3. https://www.politico.eu/article/commission-calls-for-eu-crackdown-on-money-laundering/
4. "Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing." Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Financial Crimes Enforcement Network, National Credit Union Administration, and Office of the Comptroller of the Currency, December 3, 2018. https:// www.fincen.gov/sites/default/ files/2018-12/Joint%20Statement%20 on%20Innovation%20Statement%20%28Final%2011-30-18%29_508.pdf

IBM Corporation Route 100
Somers, NY 10589

Produced in the United States of America, January 2020

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access.

IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.