INTELLIGENT RISK

knowledge for the PRMIA community

May 2025

PRMIA
Professional Risk Managers'
International Association

PROFESSIONAL RISK MANAGERS' INTERNATIONAL ASSOCIATION

CONTENT EDITORS

Carl Densem

Risk Manager, Financial Markets, Rabobank

Steve Lindo

Principal, SRL Advisory Services and Co-Principal, Intelligent Risk Management

SPONSORSHIP

PRMIA's Intelligent Risk is distributed to more than 40,000 risk professionals worldwide. If you would like information about the various sponsorship opportunities available, contact sponsorship@prmia.org.

FIND US ON

prmia.org/irisk @prmia

INSIDE THIS ISSUE

editor introduction

Carl Densem
Editor, PRMIA

Steve Lindo
Editor, PRMIA

Our May capstone explores the behavioral risk causes of bad outcomes that risk managers care about. It expands on the risk culture lens by looking at patterns in human behavior and connecting them to risk drivers. The co-authors, Wieke Scholten and Alexandra Chesterfield, provide case studies to discuss the biases which work against the use of behavioral risk analysis and how to overcome them.

We recorded a short interview with Wieke and Alexandra about their article, which you can watch on our public LinkedIn group.

Understandably, our writers focused more on geopolitics in the May issue, with others writing about people risks, fraud, regulatory and cyber risks:

- In "Rising Powers and the coming multi-polar World: What does it mean?" Merlin Linehan looks at the rise of the BRICS+ countries and ensures risk practitioners are able to spot the signs of this global shift in power.
- Alan Franklin & Mohammad Asif write about the employee productivity decline and unveil a risk-based approach to KPIs and recognition that can address this issue.
- In "Shadow Banking: Where Demand Breeds Risk," Stella Grossu looks at the causes for the shadow banking sector, defines legal and illegal forms, and then describes how the separation of regulators, banks and law enforcement could curb shadow banking.

We also highlight the United Arab Emirates chapter in this issue.

Several writers participated in webinars and chapter events this quarter. Two recent authors joined Carl in our quarterly "Intelligent Risk presents" webinar on geopolitics. You can find the recording, slides and Q&A in PRMIA's Webinar Library. Look out for the next one in July. Also in April, Andrea Calef and Chandrakant Maheshwari took part in a panel event with the Kingdom of Saudi Arabia chapter.

If you're interested in sharing your thoughts in a future Intelligent Risk or providing feedback on something you read in this issue, we welcome your emails to iriskeditors@prmia.org.

CAPSTONE ARTICLE

Synopsis

All company failure situations have, at least partly, a behavioral risk root cause. Looking beyond the scope of risk culture, leading organizations are now using behavioral science research and techniques to address specific patterns of human behavior that may lead to negative outcomes. In this article, the authors describe and give examples of behavioral risk and recommend behavioral risk management practices which can be adopted by organizations to strengthen their resilience.

strengthening resilience through behavioral risk management

by **Alexandra** Chesterfield & **Wieke** Scholten

introduction

On a chilly January morning, a routine Alaska Airlines flight turned into a nightmare scenario: mid-air, a door panel wrenched free, vanishing into the blue. The subsequent National Transportation Safety Board investigation[1] revealed four bolts that should have secured the door panel were unaccounted for. This wasn't merely a mechanical failure but a symptom of deeper systemic issues at Boeing.

When whistleblowers surfaced with alarming stories of compromised quality, ignored warnings, and retaliation for speaking up, it became clear that on the factory floor, production speed had overshadowed safety protocols. Success meant prioritizing speed over safety. The repercussions for Boeing's long-standing misdemeanors include the tragic deaths of 346 people from the 2018 and 2019 crashes[2], multibillion dollar fines, and nearly $100 billion in direct and indirect costs[3].

Boeing's string of crises follows in the footsteps of other high-profile failures: the collapse of Silicon Valley Bank, the fall of Credit Suisse, and the Volkswagen emissions scandal. Could these have been prevented? We argue yes, through organizations adopting Behavioral Risk Management.

Although corporate failures vary widely in nature and context, their underlying causes often trace back to similar roots: human behavior. This includes both the cause—normalized cutting corner behavior for example—and the reasons problems weren't prevented, such as silencing dissenting voices[4]. Put differently: all problems that occur have, at least partly, a behavioral root cause.

Behavioral Risk Management is about pre-empting future problems and identifying blind spots that risk organizational sustainability. It has the potential to transform risk and audit from rear-view to forward-looking functions. Behavioral risk mitigation involving improvements in work contexts and organisational culture also contributes to greater resilience, reduce uncertainty, and generate better outcomes for all stakeholders. We believe that current geopolitical developments and associated changes intensify the need for behavioral risk management as a stabilising forward-looking approach.

what is behavioral risk?

Behavioral risk refers to the risk of poor outcomes driven by behavioral patterns and their underlying factors[5]. In financial services, assessing and mitigating behavioral risk aims to prevent poor outcomes for the organization, customers, employees, shareholders, and society—including poor customer outcomes, talent loss, impaired innovation, decreased market share, and market instability.

While risk culture focuses on an institution's norms related to risk awareness and management, behavioral risk takes a more holistic view. It addresses specific patterns of human behavior that may lead to negative outcomes, encompassing decision-making errors, communication breakdowns, unethical actions, inadequate collaboration, and problematic customer behaviors.

From a risk taxonomy perspective, behavioral risk underlies all types of risk, including financial and non-financial risks, from financial crime to credit decisions.

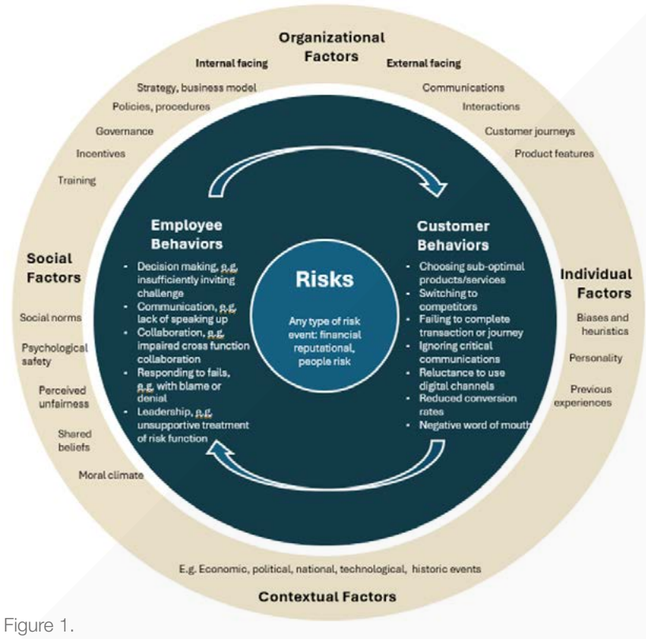


Figure 1.

Our behavioral risk model is depicted in Figure 1.

What makes our model unique is its comprehensive approach combining both internal behaviors (employees) and external behaviors (customers).

Employee behaviors that – often unintentionally – may drive poor outcomes include patterns in:

- Decision making (insufficient challenge)
- Communication (emphasizing successes over failures)
- Collaboration (inadequate cross-functional work)
- Responding to mistakes (blame leading to cover-ups)
- Leadership behaviors (unfair treatment)

Customer behaviors that may harm customers or the organization include:

- Choosing sub-optimal services (not getting value for money or paying too much)
- Struggling to complete processes
- Ignoring critical communications
- Switching to competitors
- Negative word-of-mouth
- Withholding information
- Missing payments (incurring financial harm)

These behavioral patterns emerge wherever people work together. Groups develop behavioral patterns (or "the way we do things here") that both help and hinder their performance and goal attainment. Most people genuinely want to do good work and make the right choices. However, factors in their daily professional contexts can make this challenging.

Four categories of driving factors influence these behaviors:

1. Organizational factors, or "anything on paper that may drive behavior": internal (strategy, procedures, incentives) and external (customer communications, product design).
2. Social factors, or "anything between people that may drive behavior": for example, social norms, shared beliefs, psychological safety and moral climate.
3. Individual factors, or "anything within people that may drive behavior": for example, cognitive biases, capability, previous experiences and personality.
4. Contextual factors, or "anything outside of the organisation that can drive behavior": for example, external conditions like interest rates, market developments and regulatory agendas.

The links between these driving factors, behavioral patterns, and risks are substantiated by research from cognitive science, organizational psychology, and behavioral economics. While we present a somewhat simplified model for clarity, we acknowledge the complex, interrelated nature of these elements in reality.

behavioral risk management process – three steps

Having understood what behavioral risk is, how do we manage it? Behavioral Risk Management (BRM) follows three key steps:

1. Identify: Determine hotspots for behavioral risk using existing data or advanced analytics combining behavioral science and AI to predict where staff face challenges or customer vulnerabilities exist.
2. Assess: Conduct deep-dive reviews of specific areas using qualitative and quantitative data collection. For employee reviews, gather information through confidential conversations, focus groups, observations, document review, and surveys. For customer reviews, analyze transaction data, marketing responses, and feedback.
3. Mitigate: Address identified risk factors through targeted, behaviorally-informed interventions, ideally testing their effectiveness through experimental designs like randomized controlled trials.

To bring these concepts to life, let's examine two case studies that demonstrate BRM's practical application in financial institutions.

case study 1 – mitigating technology risk by changing behaviours

A first case study concerns a financial services firm with a digital focused strategy and highly technology-driven solutions and products. BRM was successfully deployed to strengthen technology resilience and mitigate the risk of technology issues. First, a behavioral risk review was conducted within the technology division, focusing on employee behavior, to identify those aspects of "the way things were done and why" (patterns and driving factors) that could lead to technology disruptions. For example, staff skipping steps in update processes that recently had been made more complex and time consuming. Meanwhile, there was a strong push for delivery from leadership without contextualisation of the process changes. The granular insights into what behavioral patterns and driving factors within the technology division were driving technology risk allowed the firm to address these aspects in a targeted manner. Behaviorally-informed interventions were designed and implemented. Effect measurement showed a significant behavioral change, mitigating technology risk.

case study 2 – COVID 19 "bounce back" loans: spotting a hidden credit risk

At the height of the pandemic the UK Government launched the Bounce Back Loan Scheme (BBLS), allowing SMEs to borrow up to £50,000 with a 100% government guarantee to the lender. Crucially, the guarantee protected the bank, not the borrower.

Given the government link, we suspected many business owners would incorrectly perceive the guarantee as meaning the loan was “free money”, increasing the probability of later default. The behavioral assessment of this risk involved a “pub quiz” style survey sent to 1,000 business banking customers. Multiple choice questions tested understanding of key features of the loan, including who ultimately repays the loan and the consequences of non payment. The findings supported the hypothesis, with 51% of customers believing the Government, not the business, would repay the debt. Subsequently, the business attracted the highest severity/impact risk rating, given its priority to remediate.

Both case studies illustrate how BRM delivers insights about behavioral risk factors that, when addressed, can strengthen resilience and prevent future risk events that might harm institutions, customers, and society. It's no surprise that financial institutions are increasingly investing in these capabilities.

behavioral risk management in practice

Financial institutions globally have established behavioral risk management capability in various defense lines. Teams typically range from two to twelve people with multidisciplinary skills from behavioral sciences, audit, and risk. Examples of global institutions that have built such behavioral risk teams in the 3rd, 2nd and 1st Line are Citi (US), NatWest (UK), HSBC (APAC) and ING (Europe).

Regulators are increasingly encouraging this approach, with for example the Office of the Superintendent of Financial Institutions (Canada) expecting continuous evaluation of behavioral risks, the Monetary Authority of Singapore hiring behavioral risk experts in their supervisory teams and the European Central Bank recognizing BRM's crucial role in understanding bank risk management in their published guidance.

As the first teams were established around 2011, the financial industry now has over a decade of experience in managing behavioral risk. As the industry evolves further, new developments are expanding BRM's potential impact as alluded to next.

future developments

Two significant trends seem to be shaping the future of Behavioral Risk Management.

Digital footprints for measuring organizational culture

Traditional methods like employee surveys can mask issues due to response bias and normalization of problematic cultures. In other words: more surveys will not provide insight into “how things are done” in operational reality. Instead, researchers at the London School of Economics[6] are using natural language processing to analyze unstructured data from sources like staff feedback, customer comments, and incident reports—establishing links between cultural indicators and future outcomes. We see these methods of creating digital footprints adding great value to available behavioral data.

Ethical AI assistants

AI assistants designed with ethical frameworks could become impartial advisors enhancing transparency and fairness in decision processes. For example, an ethical AI in hiring could analyze applications based on qualifications while alerting HR managers to unconscious biases like hiring people similar to us. These ethical AI assistants could be deployed to improve decision-making behavior and mitigate behavioral risk.

recommended actions for risk managers

In financial services, behavioral risk management has delivered positive impact and contributed to forward-looking risk management. Next to financial services, industries such as mining and pharmaceuticals are managing behavioral risk explicitly. If your organization hasn't yet added this perspective to your risk management and resilience enhancing approach, now may be the time.

To start, you may have to overcome the following implicit beliefs preventing senior leadership from initiating BRM:

- The first concerns a degree of overconfidence that operational reality is well understood and that, for example, conducting an employee engagement survey is sufficient to substantiate that understanding.
- The second concerns a certain wilful blindness about behavioral risk factors. We shape work environments with the best intentions. It can therefore be tempting to rely on these intentions and challenging to take an honest look at daily practices.
- The third is a belief that behaviors are too difficult to change; that it will take heaps of time to shift “how things are done” and organizational culture.

Learning from experience in BRM in financial services, we can offer the following strategies to overcome these barriers.

1. Adopt curiosity: Acknowledge that despite good intentions, operational realities drive outcomes. How decisions are made, customer journeys are shaped and how shortcomings are responded to: these aspects drive good and poor outcomes. The most effective BRM approaches start with a curiosity to know that operational reality.
2. Build in-house capability: Develop expertise to provide insights into daily contexts and behavioral risk factors. Behavioral science backgrounds help to adopt evidence-based review and behavioral change methodologies.
3. Start small and measure effectiveness: Demonstrate that BRM works by showcasing interventions that successfully shifted behavior at work, and shaped work contexts that encourage aspired employee and customer behaviors.

Behavioral risk management helps organizations become more resilient, more forward-looking and less reactive. As Einstein said, "Intellectuals solve problems, geniuses prevent them."

references

1. https://www.ntsb.gov/investigations/Pages/DCA24MA063.aspx
2. Although some sources estimate total fatalities of 5,779 involving the Boeing 737 since the 1970s https://en.wikipedia.org/wiki/List_of_accidents_and_incidents_involving_the_Boeing_737
3. https://en.wikipedia.org/wiki/Financial_impact_of_the_Boeing_737_MAX_groundings
4. See Hald, Reader & Gillespie (2023) in recommended reading
5. See full references to Scholten (2022); Eccles (2022); Raaijmakers et al. (2021) in recommended readings
6. See Reader & Gillespie (2023) recommended reading

recommended reading

- Dambe, K., Hunt, S., Iscenko, Z., & Brambley, W. (2013). Applying Behavioral economics at the Financial Conduct Authority. FCA Occasional paper, Vol. 1.
- Eccles, Robert (2022): How The Behavioral Risk Team Is Innovating The Internal Audit Function At NatWest. Available online at Forbes
- Engler, H. & Wood, A. (2020). How Banks are Using Behavioral Science to Prevent Scandals. Available online at: Harvard Business Review
- Hald, E. J., Gillespie, A., & Reader, T. W. (2021). Causal and corrective organisational culture: A systematic review of case studies of institutional failure. Journal of Business Ethics, Vol. 174, pp. 457-483.
- Raaijmakers, M., Isarin, N. & Compagner, A. (2021). Managing Behavioral risk: the key to sustainable organisational change. Available online at: Reuters Regulatory Intelligence
- Raaijmakers, M. (Ed.). Supervision of Behaviour and Culture: foundations and practices. De Nederlandsche Bank (2015). Springer-Verlag Berlin Heidelberg
- Reader, T. W., & Gillespie, A. (2023). Developing a battery of measures for unobtrusive indicators of organisational culture: A research note. Journal of Risk Research, Vol. 26 (1), pp. 1–18.
- Scholten, W.W. & Chesterfield, A. (2024). Dear CRO: Behavioral risk management is the new thing for you. Journal of Risk Management in Financial Institutions, Vol. 17, 4, pp. 383-394.
- Scholten, W., Vries, F. de., & Besieux, T. (2022). A better approach to avoiding misconduct: use nudges to complement traditional methods of risk management. Harvard Business Review Magazine (May-June).
- Wood, A. (2021). Behavioral science gains traction as more banks seek to mitigate employee risk. Available online at: Thomson Reuters Institute.

authors

Alexandra Chesterfield

Alexandra Chesterfield has over 15 years' experience establishing and leading Behavioral Science teams to drive better outcomes in both regulatory and commercial contexts. Most recently, she led the Behavioral Risk team at NatWest Group, the UK's largest business and commercial bank, where her team's innovative work was featured in Forbes (Eccles, 2022). Previously she was the principal psychologist at the UK financial regulator (the FCA). Alex holds an MSc in Cognitive and Decision Science from University College London (UCL) and is the best-selling co-author of Poles Apart (Penguin Random House, 2021), which she also teaches as part of a course at The Intellectual Forum, Jesus College, Cambridge University. Now based in the U.S., Alex consults globally while pursuing a PhD at the London School of Economics (LSE), in their Corporate Culture and Risk Unit, where her research integrates psychological science with advances in AI and digital data to understand and assess institutional failure.

Wieke Scholten

Wieke Scholten is a social and organisational psychologist with over 22 years of experience in behavioral analysis and change in organisations, including 14 years in financial services. As a former Head of Behavioral Risk at NatWest Group Internal Audit, (Co-)Lead Partner of Behavioral Risk at &samhoud consultancy and Senior Supervisor of Behavior & Culture at the Dutch Central Bank (DNB), she pioneered strategies for identifying and managing behavioral risk. Wieke obtained her PhD in social psychology on preventing conduct issues in trading and sales businesses in banking organisations. She lectures at the Institute of Banking and Institute of Directors in Ireland and has published papers in leading journals, including the Journal of Financial Regulation and Compliance and the Harvard Business Review, on how organisations deploy behavioral science to obtain better outcomes. Wieke is founder of BR Insights, a globally operating behavioral risk management practice based in the Netherlands and the UK.

peer-reviewed by

Steve Lindo

Synopsis

This article explores how data and analytics are revolutionizing enterprise fraud management by enhancing detection, prevention, and response functions. It delves into the architecture and mechanisms financial institutions use to combat increasingly sophisticated fraud incidents. Risk managers can uncover new techniques and technologies that effectively address evolving fraud threats.

building an enterprise fraud management value chain powered by data and analytics

by **Sanjukta** Dhar

introduction

Traditionally, financial fraud can take various shapes and forms, more so in this digital era. The use of sophisticated digital banking and payment channels such as Zelle, Billpay, and Venmo is giving rise to novel fraud incidents which are harder to detect and prevent due to their complex structure, continuously evolving nature, superfast velocity and mostly irreversible transaction types. Some recent numbers help justify this. According to a study by Javelin Strategy & Research and AARP, account takeover fraud resulted in nearly $13 billion in losses in 2023[1]. Businesses are losing more than $100 billion from chargeback frauds, specifically first-party frauds, according to identity verification platform Socure[2].

Following the complex nature of fraud incidents, many enterprise fraud risk management functions within the financial institution are reorganising themselves into well-defined detection, prevention and response functions. In this article, we will take a detailed look at how fraud analytics is helping to strengthen these functions and also supporting decision analytics for downline operations such as operational risk or finance. Albeit a little technical, we explore the key building blocks that comprise the target enterprise fraud management architecture built to strengthen the organization combatting financial fraud.

enterprise fraud management: one mission, many ways

Nowadays, it is not uncommon to see the fraud management teams of large financial institutions building multiple mechanisms to fight fraudulent attack from all possible angles. These different mechanisms are highlighted in Table 1 and discussed on the next page.

Mechanism	Description	Examples
Prevent	Create a comprehensive repository of historical fraudulent patterns to flag and block such transactions proactively.	Mimicking scenarios like 'check kiting' or forged check transactions, where the system flags such transactions based on known patterns.
Detect	Detect and flag transactions not in the historical repository but suspicious in nature, requiring real-time monitoring and intervention.	Identifying account takeover fraud through IP address tracking or suspicious credentials and flagging transactions for additional authentication in near-real time.
Respond & Recover	Minimize the impact of fraudulent transactions that could not be blocked by responding to them post-facto and recovering the losses or managing disputes effectively.	Posting unrecovered fraudulent transactions to a suspense GL account for operational management until recovery or resolving disputes with customers.
Continuous Improvement	Utilize fraud data and analytics to enhance the system, improve decision-making, and provide actionable insights to business leaders with a balanced scorecard of metrics.	Monitoring metrics like Net Fraud Loss, Fraud Detection Rate, or YTD/MTD fraud complaints to measure operational performance and optimize fraud management strategies.

Table 1. Fraud Fighting Mechanisms

Typically, each mechanism comprises of these essential building blocks depicted in Figure 1.

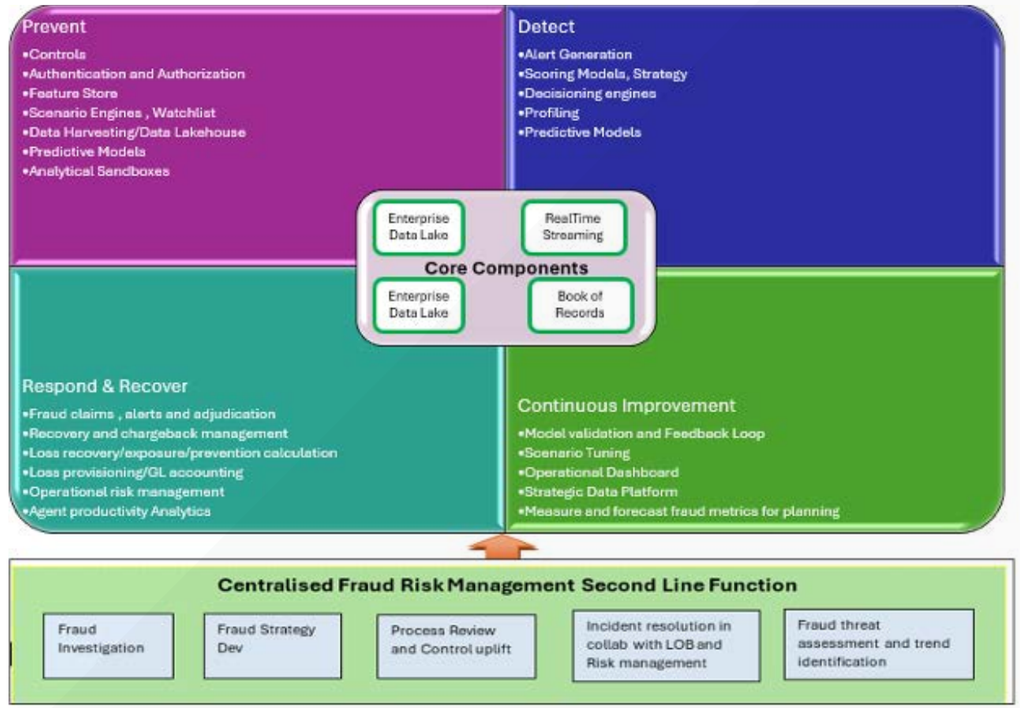


Figure 1. Enterprise Fraud Management - Target State - Essential Building Blocks Fighting Mechanisms

As a rule of thumb, preventative mechanisms are used by fraud management teams to deter bad actors by installing preventative controls or pre-facto filtering them out by studying and detecting patterns from fraud history.

Detection mechanisms are used for identifying and flagging fraudulent transactions that managed to pass through the preventative layer.

Fraud response mechanisms are by definition post-facto, to ensure that the impact on affected customer experience is minimal, accounting systems are able to capture the monetary impact accurately and the agent workflow navigating from alert generation via case management to suspicious activity report (SAR) filing is seamless.

There is a continuous improvement layer which binds the critical components of all these otherwise disjointed frameworks together by introducing common functional components. For example, a common model validation layer which works with the detection as well as prevention models. Or an analytical sandbox which runs business intelligence (BI) rules or analytical strategies on both alert data and customer profile data.

There are a few essential technical components which are central hubs to these frameworks, such as a centralised data lake supporting data in both structured and unstructured form and also supporting multiple ingestion modes such as streaming, batch, API, event, etc. This component is potentially capable of storing and processing both raw and processed data coming from external watchlists, handwritten notes, check images, voice and video surveillance, databases, end-user files and digital certificates. This is critical information related to the customer profile and their transaction behaviour, past fraudulent history and patterns, ongoing disputes handled and flagged by agents, metrics/dashboards prepared by fraud analytics teams, and therefore supports critical decision-making.

value creation for the enterprise

We mentioned before that the primary aim of the future state fraud management ecosystem is to strengthen the organization in its pursuit to combat financial fraud. However, the system can generate holistic value for the organization in various other ways such as:

1. Identify and block anomalous behaviour on real-time or near real-time (Fraud Technology)
2. Identify pattern and pre-facto fraudulent transaction alerting to stop fraud before it happens (Fraud Technology)
3. Evaluate downstream impact on operational risk management, claims and case management systems, loss recovery management processes and financial accounting systems (Operations and Processes)
4. Continuous improvement of detection logic using analytics (Analytics)
5. Provisioning a centralised data Lakehouse to build integrated data storage, curation and analytical capability for on-demand insight and analytical reporting (Data)
6. Performance monitoring dashboard for Fraud agents and fraud forecasting and planning dashboard to generate metrics for risk and finance departments (Operation and Processes)

key building blocks for fraud management framework

Spread across the 4 pillars, below are some of the essential building blocks of a comprehensive fraud management framework for the organization.

Category	Details
Prevent	A central book of record for customer, transactions, instruments (e.g., check, wires, credit card, ACH, etc.), accounts, GL, reference data, etc.
Detect	Event-driven architecture enabling real-time or near-real-time detection and decision workflow. - Real-time API orchestration to fetch case-related data elements for additional evidencing for case disposition.
	Knowledge graph or Elasticsearch-based entity resolution or case commentary generation. - Identification of fraud rings or connected cases across detection engines and customer identifiers using link analysis algorithms.
	AI/ML-based algorithms to detect known (supervised) or unforeseen (unsupervised) fraudulent patterns across various channels like digital, wires, Zelle, Easy Apply, checks, etc.
Respond & Recover	A Low-code-No-Code workflow-based solution for building post-detection response systems (e.g., case management, claim management, dispute management, chargeback management, exposure calculation, etc.).
	Convergent AML and Fraud operations, e.g., SAR filing provisions triggered by both Fraud and AML teams.
	Global case and claim search irrespective of the alert-generating unit (Fraud, AML, HR, Cyber Security, etc.).
	Straight-through no-touch SAR referral without agent intervention initiated by non-AML business functions (e.g., claims management or security and investigations).
Continuous Improvement	Generating supporting data for fraud trend analysis.
	Singular and connected view of case, claim, and investigations.
	Top-notch data governance capabilities, including data cataloging, data lineage, metadata management, data provenance, MDM, entity resolution, and data quality across enterprise data from various SoRs.
	Generating real-time metrics using an analytical sandbox to enable business units to interpret data and develop mitigation strategies for emerging fraud risks. Fraud trend metrics include:
	Detection rate - False positive/false negative rates - Gross and Net fraud loss - Fraud-to-sales ratio - Fraud typologies
	Missed fraud/customer-identified fraud - Net and projected fraud loss ($) - Authentication rate

Table 2. Enterprise Fraud Management Core Pillars and their standard building blocks

value creation for the enterprise

Due to growing threats from sophisticated fraudsters and subsequent regulatory pressure to brace up the fraud management systems, financial institutions are mandated to up the ante to build an intelligent, scalable yet robust fraud management platform or framework which supports heterogeneous sources of data and events in various frequency and velocities both pre- and post-facto. Post-facto, the system should be able to trigger the right workflows seamlessly to trigger dispute or credit chargeback or handle the claim seamlessly to minimize dissatisfaction of innocent customer but without compromising its own financial impact.

Finally, data is power. The essence of building analytics powered system is to have meaningful and quantifiable data at your fingertips. In this case, a fraud operations team needs on-demand data to build a full-fledged fraud case with detailed commentary and evidence. Regulatory compliance teams need meaningful data to build a full-proof SAR report. Fraud second line of defense teams need tons of data to build and manage fraud strategies for the enterprise or effectively resolve open incidents/investigations.

In summary, while the holy grail of fraud management framework is yet to come, data and a nimble multi-pillar fraud management system is what businesses need now, and we can expect some exciting innovations from Fintech or FinCrime consulting firms in the coming days.

references

1. https://www.fintechweekly.com/magazine/articles/hethe-growing-concern-over-account-takeovers-and-why-the-financial-industry-needs-more-tools
2. https://www.cnbc.com/2024/07/25/retailers-are-losing-100-billion-a-year-from-friendly-fraud-report-finds-.html

author

Sanjukta Dhar

Sanjukta is a senior risk advisory from the risk and regulatory compliance practice of TCS. She has recently been part of few transformative FinCrime technology projects as a data and domain specialist. She has led and participated in many critical build-the-bank risk & regulatory compliance programs such as Risk-Finance Integration, FRTB Standardized approach, VaR Back Testing framework, BCBS239 and SR11/7.

peer-reviewed by

Dami Osunro

Synopsis

Employee productivity is vital to organizational success, yet many high-performing employees experience declines over time. This raises critical questions for risk practitioners: if hiring processes are robust, what internal risks lead to decreased productivity? This paper identifies key risk factors including ineffective recognition systems, unclear or misaligned KPIs, biased promotions, and poor communication—elements critical to behavioral risk management. Through an analysis of motivation, burnout, and reward systems, we outline best practices for risk teams to mitigate operational risks tied to employee disengagement.

understanding employee productivity decline: a risk-based approach to recognition, KPIs, and organizational practices

by **Alan** Franklin & **Mohammad** Asif

introduction

Organizations invest substantial resources in recruiting skilled employees, yet productivity often declines, creating operational risks such as increased turnover and reduced efficiency. Risk practitioners must proactively address these behavioral risks to safeguard business continuity. This paper highlights primary risk factors leading to productivity declines and proposes practical strategies risk teams can integrate into their risk management frameworks.

factors contributing to employee productivity decline

Burnout and Emotional Exhaustion

Burnout significantly shifts high performers to low productivity. The World Health Organization classifies burnout as chronic workplace stress managed ineffectively, manifesting as emotional exhaustion, cynicism, and decreased efficacy (Maslach & Leiter, 2016). Burnout correlates directly with decreased employee engagement, diminished job performance, and higher turnover (Schaufeli, Bakker, & Salanova, 2009).

Risk Mitigation Strategy**: Risk teams should advocate burnout assessments, workload monitoring, and mental health programs to proactively mitigate these risks.**

Employee Disengagement

Employee engagement is the involvement and enthusiasm of employees in both their work and workplace. According to the 2023 Gallup Employment Engagement Report, in the US, 31% of employees are engaged, globally 23%, but Best Practice Organizations have 70% employee engagement. “Engaged employees have higher wellbeing, better retention, lower absenteeism and higher productivity.”

According to Gallup Workplace, people want purpose and meaning from their work. They want to be known for what makes them unique. This is what drives employee engagement.

And they want relationships, particularly with a manager who can coach them to the next level. This is who drives the employee engagement. One of Gallup's biggest discoveries: The manager or team leader alone accounts for 70% of the variance in team engagement.

Risk Mitigation Strategy: Risk teams should advocate helping employees find purpose and meaning in their work, sometimes by restructuring, and train managers to develop relationships with their employees to coach them to the next level. Understand that disengagement is not “an HR thing” but is a management issue; engagement can be measured.

Poor Communication and Lack of Clarity in Risk Policies

Clear communication is crucial for mitigating risks associated with misunderstandings and compliance failures. Unclear expectations significantly demotivate employees, impacting productivity. A Chartered Institute of Personnel and Development (CIPD) 2021 study reported 47% of employees felt demotivated due to unclear communication from management.

Risk Mitigation Strategy: Establish structured communication frameworks, including standardized policy documentation and regular risk-awareness feedback loops.

Lack of Recognition and Misaligned Rewards

Recognition sustains employee motivation. When rewards contradict stated organizational values or KPIs, employees face moral dilemmas, leading to disengagement and turnover. Gallup (2022) found structured recognition programs to increase productivity by 22% and reduce turnover by 27%.

Risk Mitigation Strategy: Ensure reward structures accurately reflect organizational values and KPIs. Implement real-time recognition tools and peer acknowledgment platforms to reinforce consistent messaging.

Unfair Promotion Structures and Unclear KPIs

Promotion biases and unclear KPIs pose significant disengagement risks. Employees perceiving favoritism or misalignment between stated values and actual evaluation criteria experience decreased morale and productivity (Heslin & Keating, 2017).

Risk Mitigation Strategy: Conduct behavioral risk audits to identify biases in promotion policies and standardize KPIs, ensuring fairness and transparency.

measuring workplace culture risk

Organizations often lack structured methods to quantify cultural risks associated with disengagement. Risk practitioners can utilize:

- Employee Net Promoter Score (eNPS)[1]: Measures employee satisfaction and advocacy.
- Burnout Index Surveys: Identifies high-risk teams. (See Gallup or tools like Glint's Burnout Survey for more)
- Promotion Fairness Index[2]: Assesses transparency and fairness in advancement.

These tools enable risk teams to detect early signs of disengagement, facilitating targeted interventions.

role of risk teams in productivity management

Risk professionals play a unique and often underutilized role in managing employee engagement and productivity decline. While human resources (HR) departments traditionally “own” processes like communication policies and reward structures, risk leaders often have access to real-time insights from the frontline—patterns of absenteeism, feedback silence, policy noncompliance, and disengagement that may not be immediately visible in HR systems.

Rather than duplicating HR’s role, risk teams must use their vantage point to advocate for leadership interventions that reflect real operational dynamics rather than idealized policy.

Here is how risk practitioners can support productivity without crossing the line into HR territory:

1. Clarify KPIs using risk intelligence

   Risk leaders often detect unintended consequences of KPIs—such as promoting speed over accuracy. They should work with performance teams to ensure KPIs are aligned with both ethical conduct and core job expectations. For example, Gallup’s Q12 study, an employee engagement survey, found that employee clarity around expectations directly correlates with productivity and performance (Gallup).

1 / https://www.hibob.com/hr-glossary/employee-net-promoter-score/

2 / https://www.greatplacetowork.ca/en/8-ways-to-have-a-fair-process-for-promotions

2. **Advocate for fair recognition structures**

   Leaders must differentiate between policy-based recognition systems and frontline realities. Risk professionals should highlight gaps where recognition inconsistently reinforces desired behaviors and push for frameworks that reflect compliance, collaboration, and client outcomes.

3. **Bridge communication gaps with ground-level data**

   While HR designs communication channels, risk teams often identify where messages fail to land. This includes lack of feedback, inconsistent interpretation of rules, or fear of speaking up. Partnering with leadership, risk practitioners can surface these failures and advocate for feedback mechanisms that genuinely protect voice and anonymity.

4. **Protect against burnout through role boundaries**

   Risk teams can highlight workload patterns and control design flaws that lead to burnout, especially in regulated environments. Burnout is not just a wellness issue—it increases exposure to operational risk. Leaders need support in navigating the emotional boundaries of coaching staff while maintaining objectivity and consistency. Training in "professional empathy," including frameworks like Gallup's Q05 ("someone at work cares about me"), supports this balance.

Ultimately, we are not asking risk leaders to become HR. We are asking them to become behavioral risk translators—converting culture, communication, and role clarity into tangible risk indicators and control recommendations.

conclusion

Addressing productivity decline is critical for mitigating operational risks. Risk practitioners must proactively integrate structured recognition programs, transparent KPI frameworks, and behavioral risk assessments. By prioritizing fairness, clarity, and alignment between rewards and organizational values, risk teams can significantly enhance employee engagement and productivity, safeguarding organizational success.

Disclaimer: ChatGPT was used as a writing assistant in drafting this article under human editorial oversight.

references

1. CIPD. (2021). Effective communication in the workplace.
2. Gallup. (2022). Employee recognition: The key to engagement and performance.
3. Gallup. What Is Employee Engagement and How Do You Improve It?
4. Gallup. State of the Global Workplace 2023 Report.
5. Heslin, P. A., & Keating, L. A. (2017). "Developmental job experiences and leader development: The moderating role of perceived organizational support." Journal of Applied Psychology, 102(6), 918–932.
6. Maslach, C., & Leiter, M. P. (2016). Burnout: The Cost of Caring. Psychology Press.
7. Schaufeli, W. B., Bakker, A. B., & Salanova, M. (2006). "The measurement of work engagement with a short questionnaire: A cross-national study." Educational and Psychological Measurement, 66(4), 701–716.

author

Alan Franklin

Alan is a renowned expert in international business risk management, serving as the Managing Director of Global Business Risk Management, with operations in Vancouver and Toronto, Canada. With a distinguished career in strategic advisory, corporate governance, legal risk, and business due diligence, Alan has worked with over 350 companies across Canada and the United States, helping organizations navigate complex regulatory environments and mitigate global business risks.

Alan holds a prestigious academic background, including an LLM from The London School of Economics and Political Science (LSE), one of the world's leading institutions in law, economics, and political science and a JD from the University of Toronto. He is also an active member of the Columbia University "Teaching Business and Human Rights Forum," contributing to cutting-edge discussions on corporate responsibility and ethical business practices.

Mohammad Asif

Mohammad is the Director of MetaNexus Business Solutions and a recognized expert in digital transformation, financial strategy, and workforce optimization, with over 20 years of executive experience in banking, risk management, and strategic consulting. He has held senior leadership roles across the financial services industry, where he advised on financial strategy, regulatory compliance, and operational transformation. His consulting work includes high-level engagements with Continental Currency Exchange, a subsidiary of DUCA Credit Union, where he helped shape risk management frameworks and compliance protocols.

He has successfully coached executives, managers, and teams to build resilient, high-performance cultures using data-backed retention models and engagement strategies tailored to the financial sector. Holding a degree in economics and an Executive MBA with a focus on leadership, risk management, and decision-making, Asif blends academic strength with real-world insight—delivering solutions that drive both profitability and lasting impact.

peer-reviewed by

Carl Densem

Synopsis

The threat posed by ransomware is rapidly increasing, underscoring the urgency for integrating ransomware risk assessments into risk management strategies. A structured evaluation of the controls at an asset level can significantly uncover 'unknowns' and enhance an organization's ability to protect its data from ransomware threats. The authors propose a structured control self-assessment (RCSA) process for managing ransomware risks. By adopting this practical template for assessing ransomware controls institutions can execute an effective risk identification and management exercise and provide assurance to their management and board on the controls to mitigate the pervasive challenge of ransomware attacks.

from threat to thwart: enhancing ransomware defences

by dr. **Martin** Leo & **Hany** Roslie

introduction

As the day begins, you open your inbox, yet a sense of caution remains at the forefront of your mind. With each word, your wariness grows. Cyberthreats, scams, phishing. Over recent years, the frequency and the sophistication of such attacks have increased drastically. With more advanced techniques used to infiltrate the systems, organisations must ensure there is a growing emphasis on combating ransomware.

Ransomware is a type of malware that encrypts a victim's data where the attacker demands for a payment to restore access. If the ransom payment is not made, the attacker threatens to leak and publish the data or blocks access to the files in perpetuity (PubPub, n.d.).

J.P. Morgan identifies five main stages of a ransomware attack (JPMorgan Chase, n.d.). The attack often begins with a compromise of the network through social engineering techniques (Delivery stage) followed by the ransomware establishing a connection to the main server (Command and control stage) while stealing credentials (credential access stage). Through lateral movement the ransomware searches for files to encrypt (canvas stage) and finally the attacker demands payment (extortion stage). Attackers typically provide the decryption key in exchange for a monetary sum, often in Bitcoin due to its anonymity and evasiveness (Kott & Arnold, 2019).

Ransomware threats continue to present significant risks globally, illustrated by several notable attacks in recent years. In 2024, Change Healthcare in the U.S. was compromised by the ALPHV/BlackCat group, with the total cost of the breach at $2.87 billion (HIPAA Journal, 2024).

The UK's NHS-affiliated Synnovis experienced a breach resulting in financial costs of £32.7 million (Digital Health, 2025). In 2021, the Colonial Pipeline attack captured headlines around the world. The company paid $4.4 million to the hacker group (Wikipedia contributors, n.d.). A 2023 attack on Clorox resulted in a $356 million financial impact (Tufin, 2023). A common threat across all incidents is inadequate cyber hygiene. Unpatched systems, weak remote access controls, supply chain vulnerabilities have proven to expose companies to ransomware attacks with significant financial impact. These incidents underline the critical need for robust cybersecurity measures and advanced threat detection systems.

This article aims to provide guidance for building a robust and structured controls assessment framework to evaluate the adequacy and effectiveness of controls required to mitigate ransomware risks.

risk assessment framework

The ransomware risk assessment process is a structured and targeted approach towards evaluating the risk exposure to ransomware threats. The key feature of the assessment is that it is done at an asset level. Each in-scope assessment is identified and the control is evaluated for each asset to then arrive at the overall adequacy and effectiveness of the controls. The controls are aligned with the NIST Cyber Security Framework (CSF).

The following are key components of the assessment template:

a) NIST CSF Category – Control Requirement – List of controls to be evaluated as part of the assessment. This can be mapped to the NIST CSF categories for better classification. Examples of the category and a description of ransomware control requirements are listed in the table below. The template would state the specific control to be evaluated e.g. Has 2FA been implemented for all privileged accounts?

Identify	
This section focuses on understanding the organization's assets and their vulnerabilities. *Key controls include:*	
Inventory Management	Ensuring all assets, including ingress and egress network points, are accounted for and scanned for vulnerabilities.
Threat Management	Establishing processes to identify vulnerability and assess ransomware risk.
Protect	
This section assesses the measures in place to safeguard the organization's assets. *Key controls include:*	
Identity and Access Management	Implementing controls to ensure only authorized and appropriate level of access is allowed.
Network & System Controls	Implementing policies to segregate, harden and secure systems, at standards commensurate with their criticality and to prevent lateral movement.
Patch Management	Ensuring all assets are patched with the latest updates and implementing any necessary mitigating measures.
Awareness	Enhance awareness for all staff (e.g. administrators).

Table 1. Key Components of Assessment Framework (continues on next page)

Detect	
This component evaluates the organization's ability to identify ransomware events promptly. Key controls include:	
Monitoring Systems	Implementing 24/7 monitoring of ingress, egress points, and key assets
Respond	
This section focuses on the organization's preparedness to respond to ransomware incidents. Key controls include:	
Incident Response Playbook	Documenting procedures for incident response, roles and responsibilities, communication protocols, measures to mitigate impact of attack
Recover	
This component assesses the organization's ability to restore systems and operations after a ransomware attack. Key controls include:	
Incident Recovery Plan	Documenting recovery processes to ensure swift return to normal operations.
Backup Management	Ensuring secure and regular backups of critical data and systems (e.g. air gapped backup sites, immutable backups).
Insurance Coverage	Evaluating insurance policies to cover ransomware-related costs.

Table 1. Key Components of Assessment Framework (continued)

b) Description of Controls: For each control the assessor provides references for the specific controls (policy, process, tools) implemented to address the control requirement.

c) Control Adequacy Assessment [CAA]: Self-assessment of the adequacy of the controls implemented, such as whether the controls have been adequately implemented across the organization. (e.g. Sufficiently Implemented - Controls implemented and in line with the policy/standard, Partially Implemented - Controls implemented, not in line with the standard, etc)

d) Asset Coverage (%) [AC]: The percentage of 'in-scope' assets for which the controls have been implemented. If a control (e.g. 2FA) is implemented but only for 50% of systems, then the control is not adequately implemented.

e) Control Testing [CT]: A documented measure to determine if the controls have been tested for effectiveness (e.g. red team exercise in last 12 months).

scoring and evaluation

Each control is assessed for its adequacy, coverage, and testing frequency based on pre-defined values and a score (e.g. 1, 2, 3). An overall control score [CS] is then calculated. The computation is a product of the individual values for CAA, AC, CT and not a summation. This is to ensure the score is weighted for the percentage of assets for which the control should be assessed on. A lower percentage of assets assessed results in a lower score highlighting the control as an area to be focused on. An example of the methodology follows in Table 2.

NIST CSF Category	Control Requirement	Assessment of Control Implementation [Have controls been implemented. Provide description/reference]	Description of controls (include references to available documentation/artifacts)	Control Adequacy Assessment (CAA)	Asset Coverage (%)	Control Testing	Control Score	Gaps / Improvement areas - Current and from assessment
Protect	Privileged account management	Is 2FA/MFA implemented for all privileged accounts? *[Asset coverage should refer to the % of assets for which the 2FA/MFA has been implemented]*	Policy in place. 2FA solution xyz rolled out	Partially implemented	50%-90%	At least once in last 2 years	2	1. Onboard remaining assets 2. Increase frequency of testing

Table 2. Example of Control Evaluation

The scores help quantify the effectiveness of the controls and highlight areas which need improvement. The assessment results can be summarized in a chart (Figure 1) that provides a visual representation of the organization's cybersecurity posture across the NIST CSF categories.

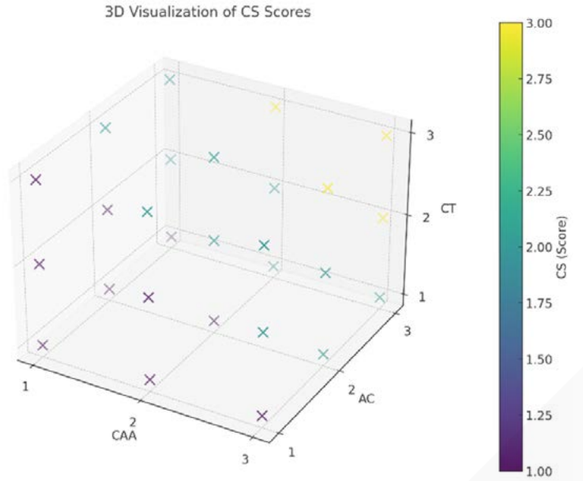


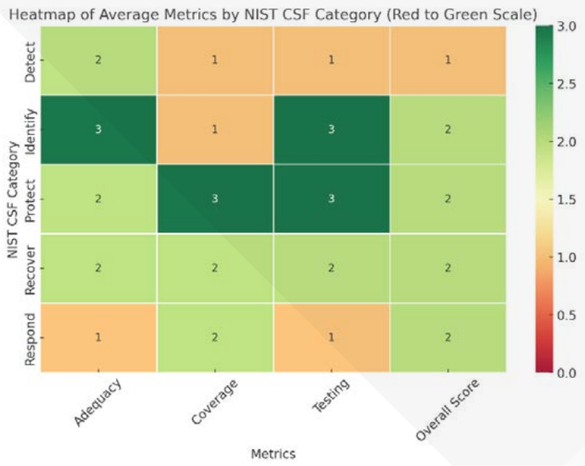
Figure 1. Visualization of control sores

responsibilities

The 1st line, with the system owners primarily responsible, completes the self-assessment including identifying actions to address gaps. The 2nd line function (risk management) reviews and validates the assessment providing the required assurance for the assessment process.

reporting and monitoring

The scores for each of the controls can be plotted in charts (Figure 2) for the risk owners and management to understand which areas they need to focus on. The chart provides a view into which category of controls is deficient – where the controls have a score less than 3 (e.g. Detect).



The category can be reviewed to understand whether the deficiency is due to inadequate testing and/or coverage – providing insights on what should be done to enhance the control environment. This provides asset level control deficiency information to enable effective risk management.

Figure 2. Heatmap of Average Scores for each NIST CSF Category

conclusion

With the growing threat of ransomware attacks, a ransomware risk assessment that is based on the underlying IT assets can be a vital tool for organizations to systematically and comprehensively evaluate their defences. By identifying vulnerabilities, assessing control adequacy at an asset level, and implementing necessary improvements, institutions can enhance their resilience against potential ransomware attacks.

Disclaimer: AI was used minimally during the editing phase of this article.

references

1. CBS News. (2024, March 28). UnitedHealth cyberattack: Change Healthcare hack and ransomware. https://www.cbsnews.com/news/unitedhealth-cyberattack-change-healthcare-hack-ransomware/
2. Chainalysis. (2024). Ransomware 2024: Trends, stats, and case studies. https://www.chainalysis.com/blog/ransomware-2024/
3. Digital Health. (2025, January). Cyber attack cost Synnovis estimated £32.7m in 2024. https://www.digitalhealth.net/2025/01/cyber-attack-cost-synnovis-estimated-32-7m-in-2024/
4. HIPAA Journal. (2024, March 13). Change Healthcare responding to cyberattack. https://www.hipaajournal.com/change-healthcare-responding-to-cyberattack/#:~:text=In%20the%209%20months%20to,to%20%242.87%20billion%20in%202024
5. ITPro. (2024, March 27). US energy contractor ENGlobal reveals ransomware attack. https://www.itpro.com/security/ransomware/us-energy-contractor-englobal-reveals-ransomware-attack
6. JPMorgan Chase. (n.d.). The anatomy of a ransomware attack. https://www.jpmorgan.com/insights/cybersecurity/ransomware/the-anatomy-of-a-ransomware-attack
7. Kott, A., & Arnold, C. (2019). A survey of current research in cybersecurity and artificial intelligence. Journal of Cybersecurity, 5(1), tyz003. https://doi.org/10.1093/cybsec/tyz003
8. National Institute of Standards and Technology. (n.d.). The five functions. https://www.nist.gov/cyberframework/getting-started/online-learning/five-functions
9. PubPub. (n.d.). A cyberattack on a hospital: Exploring the use of geospatial data in incident response. IJGIS. https://ijgis.pubpub.org/pub/57la3v2w/release/1
10. Tufin. (2023, October 30). Clorox breach: Why network segmentation is essential. https://www.tufin.com/blog/clorox-breach-why-network-segmentation-is-essential
11. Wikipedia contributors. (n.d.). Colonial Pipeline ransomware attack. Wikipedia. https://en.wikipedia.org/wiki/Colonial_Pipeline_ransomware_attack
12. Winder, D. (2024, July 31). Record-breaking $75 million ransom paid to Dark Angels gang. Forbes. https://www.forbes.com/sites/daveywinder/2024/07/31/record-breaking-75-million-ransom-paid-to-dark-angels-gang/

authors

Dr. **Martin** Leo, DBA, CISSP, FRM

Dr Leo is the Chief Risk Officer at the National University of Singapore, bringing with him a wealth of expertise accumulated over nearly three decades in the financial services industry. With more than 20 years dedicated specifically to risk management, he has held senior leadership positions in managing risk at global banks, with a particular focus on technology and cybersecurity risks. He has served in regional risk leadership roles at institutions such as Citibank, ING, Morgan Stanley, and State Street Bank, enhancing risk governance and incorporating transformative practices aimed at achieving effective risk identification and reduction.

Hany Roslie

Hany is a Management Associate at the National University of Singapore, working under the Office of Risk Management and Compliance. With a burgeoning interest in risk management, Hany has actively contributed to projects involving research and intelligence, and strategic risk planning. Currently, she is focused on monitoring emerging threats and developing risk assessment frameworks to address emerging cybersecurity challenges.

peer-reviewed by

Adam Ennamli

Synopsis

This article examines interdependencies between geopolitics and M&A, drawing on examples from high-profile deals, outlining assessment approaches, and summarizing relevant literature. This information will help risk practitioners manage the uncertainties of M&A activity within their respective geopolitical climate.

power plays and deal breakers: a risk practitioner's guide to M&A deals

by **Adam** Ennamli

introduction

Mergers and Acquisitions (M&A) involve the consolidation of companies through various financial transactions, including mergers, acquisitions, consolidations, and purchase of assets. They are a strategic lever that allows businesses to rapidly expand their market share, acquire a new technology, eliminate competition, or diversify offerings, effectively leapfrogging the process of building from scratch.

As they navigate a very fluid geopolitical and economic context, risk managers must realize that the geopolitical dimension has evolved from a peripheral consideration to a driving force that can make or break deals. Those who recognize this shift and integrate geopolitical analysis into their core M&A strategy will find opportunity where others see only risk.

> ***Data sovereignty, commensurate with the growing importance of data as an asset, is a determining factor in global tech mergers and acquisitions, at the intersection between politics, geography and technology.***

cases in point: geopolitics makes or breaks M&A

1. Broadcom's Failed Bid for Qualcomm (2018)

The failed Broadcom bid for Qualcomm in 2018, a $117 billion proposition, is a compelling example of how global risk can materialize in M&A. The US government's intervened, via CFIUS (The Committee on Foreign Investment in the United States), raising national security and research position concerns over 5G technology, as they feared the deal would advantage Huawei, a Chinese competitor. This first example highlights how strategic technology competition started shaping the fate of major corporate transactions[1].

2. Lattice Semiconductor and the U.S.-China Trade War (2017)

CFIUS blocked a bid from Chinese private equity firm for Lattice Semiconductor. Based on records, the decision was based on concerns about China's expanding footprint in semiconductors. That said, this happened during high trade tensions between US and China, underscoring the impact of geopolitics on M&A transactions when government entities have veto power[2].

3. Société Générale's Exit from Russia (2022)

In the immediate aftermath of the Russia-Ukraine conflict and the subsequent Western sanctions, Société Générale was compelled to sell its Russian subsidiary, Rosbank, at a loss of over $3 billion. This demonstrates how sudden geopolitical events can make companies rethink their M&A strategies with limited regard for financial implications[3].

4. TikTok's U.S. Operations (2020 -present)

Motivated by its concerns over data privacy and national security, the US government tried to force ByteDance, TikTok's parent company, to sell its US operations to an American firm. In 2020, President Trump issued executive orders to ban TikTok unless it was sold, citing risks of Chinese government access to user data. A year later, the Biden administration shifted its focus to broader, overarching data security measures rather than forcing a single deal. Data sovereignty, commensurate with the growing importance of data as an asset, is a determining factor in global tech mergers and acquisitions, at the intersection between politics, geography and technology.

approaches for risk practitioners as they navigate M&A deals

Geopolitical risk management in M&A demands an adaptive and proactive strategy. The right mitigation involves an approach which encompasses the following key elements:

1. Enhanced Due Diligence: Go beyond surface-level assessments. Deeply analyze the target's operating environment, considering not only political stability but also more ambiguous political risks: shifting government priorities, the influence of non-state actors, and latent social tensions. Multi-scenario due diligence also helps when likelihoods can be estimated.

2. Early Regulatory Engagement: Interaction with bodies like CFIUS and the European Commission with the necessary transparency is essential. As one anticipates potential objections and proactively shapes the narrative the deal's will strengthens, rather than simply reacting to concerns and patching the narrative. Build relationships with regulators and commit to compliance.
3. Strategic Portfolio Diversification: This is not just about geographic spread. Understand the interconnectedness of global markets and potential cascading risks. Analyze risk correlations across regions and avoid concentrated exposure in politically aligned or economically interdependent markets.
4. Strategic Local Partnerships: Local partners can provide critical information that you could use in your M&A conversation, but selection must be strategic. Consider political connections and reputation. Stay clean.
5. Robust Contingency Planning: Move beyond generic scenarios. Develop detailed, scenario-specific plans to deal with any possible scenario of disruptions: sanctions, regulatory blockades, political instability, and social unrest.
6. Strategic Government Relations: Cultivate relationships with government officials and policymakers long-term. Engage with relevant agencies and understand their priorities.
7. Integrated Social Factors and Trust Management: Social factors are fundamentally connected to political risk. Align transactions with sustainability principles to mitigate political and social risks, not just stakeholder trust damage.
8. Future-oriented Geopolitical Foresight: Do not take anything for granted, as you consider evolving geopolitical trends through scenario planning, forecasting, and grasping global power dynamics. For example, Syria pre-Arab Spring was a stable country for decades, before a civil war shattered any sense of security.
9. Specialized Expertise: Engage experts in geopolitics, international law, and regulatory compliance. Do not rely solely on lawyers and financial advisors.

conclusion

Geopolitical risks are an unavoidable reality in today's M&A landscape. From regulatory hurdles and trade wars to cyber threats and climate change, companies must compose with a web of challenges to succeed. By adopting a proactive, macro-approach—grounded in thorough analysis, early engagement with regulators, and a focus on long-term trends—businesses can turn these risks into levers to

The examples of Broadcom-Qualcomm, Lattice Semiconductor, and Société Générale illustrate the high stakes involved. But with the right strategies and mindset, companies can thrive in an increasingly uncertain world.

Those who can master this complex interplay of factors – combining deep technical understanding with nuanced geopolitical awareness – will be best positioned to execute successful M&A strategies in an increasingly interconnected yet fractured global landscape.

author

Adam Ennamli

Adam Ennamli serves as Chief Risk, Compliance & Security Officer at General Bank of Canada, where he leads enterprise-wide risk programs. Drawing on 15 years of leadership experience across global financial and technology institutions including Morgan Stanley, Thomson Reuters, and National Bank of Canada, he specializes in transforming risk management and compliance frameworks.

A recognized expert in enterprise trust, Adam has pioneered innovative approaches to cybersecurity, sustainability, and regulatory compliance that directly impact strategic growth. His MBA from HEC Montreal underpins his integrated approach to risk management, security, and operational resilience. Under his leadership, organizations have consistently achieved industry-leading risk management capabilities and compliance standards.

Adam contributes actively to industry dialogue as a member of the Forbes Technology Council and the Virtual Advisory Board, providing thought leadership on emerging risk management challenges and technology governance.

peer-reviewed by

Carl Densem

PRMIA United Arab Emirates Chapter

In recent years, the United Arab Emirate has solidified its position as a global trading and financial hub and has become a magnet for international enterprises and talent. The country now serves as a true center of excellence, attracting professionals across finance, compliance, analytics, and risk management. It is in this vibrant environment that we saw the opportunity to bring together minds and expertise under the respected banner of the Professional Risk Managers' International Association (PRMIA).

In 2024, we launched the PRMIA UAE chapter — a local initiative designed to foster collaboration, thought leadership, and knowledge-sharing within the risk management profession. Our goal is to serve as a platform for networking, education, and engagement on the most pressing challenges and emerging trends in the field.

Led by a passionate Steering Committee of seasoned professionals, the chapter brings together expertise from across a wide range of industries represented throughout the Emirates. With a focus on both financial and non-financial risk domains, the UAE chapter is committed to elevating professional standards, fostering interdisciplinary collaboration, and supporting the development of resilient risk practices. Through engaging events, thought leadership, and a growing network, the chapter aims to empower current and future risk leaders across the region.

The chapter's leadership team is made up of the following:

Regional Director

- Olga Kotina, Head of Risk Management practice, GMS FZE

Steering Committee

- Mohammad Salman, Risk Manager, Investment and Development Office of Ras Al Khaimah
- Najeeb Razzaque, Risk Manager and Compliance Director, Fuze
- Carl Saad, Credit manager, Ashon International DMCC
- Ekaterina Kokareva, Independent compliance advisor
- Pavel Lyubin, Head of Financial Risks, GMS

In 2024, the UAE chapter hosted its inaugural event: an open discussion on the "Global Risks Report 2025," published annually by the World Economic Forum. This landmark event brought together professionals from across the risk spectrum to examine the most pressing global risks anticipated in the near and long term. The discussion explored the report's insights on complex, interconnected risks in a globalized world and highlighted strategies for enhancing resilience and collaboration among governments, businesses, and global institutions. The event set a strong precedent for the chapter's future direction, focused on timely, high-impact topics.

Looking ahead to 2025, the UAE chapter is preparing to host a series of impactful events addressing some of the most pressing challenges in today's risk landscape. Planned topics include climate risks, trade wars and their impact on the global economy, and the rising risks associated with the widespread adoption of AI across industries. Additional subjects will be defined through a collaborative voting process among active UAE chapter members, ensuring that the chapter's initiatives remain relevant, engaging, and responsive to the community's needs. These events aim to deepen professional insight, encourage dialogue, and support innovation across both financial and non-financial risk domains.

To connect with your local chapter, contact uaesteering@prmia.org.

Synopsis

The rise of BRICS+ signifies a shift towards a more unpredictable and multi-lateral world. This change will give rising powers more leverage in global affairs, allowing them to drive events and potentially sideline traditional Western economic order. Risk managers must learn to recognize this shift and enable their companies to adapt.

rising powers and the coming multi-polar world: what does it mean?

by **Merlin** Linehan

The BRICS summit hosted by President Putin in Kazan in late October 2024 symbolised the growing power of the non-western world. Putin used the summit to demonstrate to the west that Russia could ignore the sanctions unleashed by the west to punish him for his invasion of Ukraine. The summit also threw the spotlight on the BRICS bloc itself. The summit has become a fixture of the global diplomatic calendar creating speculation around the agenda and attendees.

The BRICS grouping: originally Brazil, China, India, and Russia, later to include South Africa has become a proxy for the world's rising powers which are taking a growing share of the globe's economic pie.

Now boasting new members such as Egypt, Ethiopia, Iran, Indonesia, and the United Arab Emirates, with others such as Saudi Arabia and Türkiye weighing up membership in the near future. The expanded BRICS+ appears to have wind in its sails. But what are the BRICS+, an excuse for a yearly summit, an alliance, a powerless talking shop, or maybe the future of global power.

Shifts in global power often appear abstract, but as I shall argue we are entering a more unstable period in global politics which will have far reaching impacts that risk managers of all stripes should not ignore.

Firstly, the BRICS+ is not yet, or likely to become, a formal alliance. Members countries particularly India and China decades old border dispute and political tensions appear to preclude close cooperation. What does unite members is a desire to have a louder voice in global affairs and sideline the traditional powers of Europe and North America Resentment of the US led economic order is a common complaint. The power of the US dollar, plus the ability of the US and Europe to use trade and sanctions as a weapon against Iran, Russia and others has left many wary and willing to consider alternatives.

Distrust of the US has seen both talk of a BRICS currency and alternatives to western financial transactions. Talk of a common currency proved hollow and a reminder that member states' economies are wildly divergent. Perhaps more progress has been made on financial cooperation and use of national currencies in intra-BRICS trade. But talk of de-dollarization is premature.

China has developed an alternative to SWIFT, the European based payments system which enables international financial transactions between banks – making it the backbone of the global financial system and a subtly powerful tool. Control over SWIFT makes it easy to exclude Russian or Iranian banks from the rest of the world. Cut off from the financial system, China's alternative CIPS (Cross-border Interbank Payment System) could one day provide an alternative financial network.

BRICS+ in motion

But what does the BRICS+ mean for risk managers. For one, a messy, more unpredictable, multi-lateral world. As rising powers in and outside the BRICS+ steadily gain more economic heft, they will gain more leverage in global affairs, which will allow them to drive events, rather than merely influence them or watch as by-standers. Witness Saudi Arabia's recent willingness to forge ties with Iran and China and ignore the US demands to reduce oil prices. Or Türkiye's ability to remain in NATO while becoming a trade hub for Russia during the war in Ukraine.

Many will celebrate a world of slipping US hegemony and a louder voice for middle powers. But diverging interests and escaping the ties of superpowers mean more potential for tension. A world where rising powers are more willing to take risks in pursuit of their interests means a greater chance of conflict. Putin calculating the US would not intervene in Ukraine encouraged him to gamble on invading his neighbour with minimal pushback. Conflict does not just mean war. The high cost of military clashes will make economic tools such as blockades, sanctions, and export/import controls more tempting. The Trump administration's move to increase tariffs across the world and the counter tariffs put in place by many rising powers –most notably by China– sent financial shockwaves across the world. The episode demonstrates both US power, but also that rising powers are unwilling to back down without a fight.

what does this mean for multi-national companies

Risk managers need to be aware that the old certainties are fading and a world which has been becoming more connected and globalised is mutating into something new. Above all, observers need to understand the motivations, potential actions, and consequences of middle powers – and how these will map to their organisation's own objectives.

Many companies were surprised when Russia invaded Ukraine. Businesses doing business in Russia were hit with a web of onerous sanctions, plus painful reputational and operational impacts.

Naturally, many lost money as a result. At the same time many countries suffered higher inflation as the war triggered a rise in oil prices which in turn pushed up the prices of many products, but especially basic goods: food, drink, and household essentials. While predicting geopolitical events is difficult, investing in foresight (will countries go to war) and understanding second and third order impacts (sanctions, increasing oil prices) can allow companies to be better prepared in the future.

Rising powers are not the only dynamic in the global economy: a new administration in the US, increasing climate change induced extreme weather, and the spectre of disruptive technologies will all pose new risks for businesses around the world.

As we enter a dramatic new phase in global politics, companies need to be able to spot, understand and adapt to geopolitical flux. Soon after another turning point, the fall of the Berlin Wall in 1989, Toyota's President declared that the firm must "lead the times" and embarked on a three-decade long story of global expansion. Toyota embraced political risk, decentralising production, and adapting to local circumstances in spite of very real political risk, all of which ultimately made the firm one of the world's biggest car manufacturers. Not all firms will want to be as ambitious as Toyota, but one thing they cannot do in 2025 is ignore geopolitical risk.

author

Merlin Linehan

Merlin is a Risk Manager at the European Bank for Reconstruction and Development (EBRD). He has over ten years' experience in responding to global security, geopolitical and cyber events for the EBRD. He is a regular contributor to banking and risk publications covering geopolitical risk, climate change and resilience. Merlin is also a regular speaker at conferences and webinars focusing on managing global risks and building organisational resilience.

peer-reviewed by

Carl Densem

Synopsis

This article describes a framework that uses large language models to analyze unstructured customer complaints of digital banks. Through in-context learning and social network analysis, it extracts fraud signals and exposes insider-broker links to detect fraud in customer acquisition. Risk managers stand to learn a valuable application of LLMs to unstructured data puzzles that may be replicated in other domains.

unveiling shadows: an LLM-driven approach to detect occupational fraud in customer acquisition

by Terrence **Cai**

introduction

Imagine you are a small business owner urgently needing funds, only to face slow bank approvals. A loan broker then offers near-instant approval from a digital bank - albeit with a commission fee – which you accept right away. You later find that your contact details were accidentally misused. This scenario highlights a vulnerability in digital banks' customer acquisition strategies: Although they acquire customers digitally, these banks blend digital advertising with traditional channels like telemarketing to attract and convert applicants. Digital ads generate high traffic, but they might attract prospects who do not meet the lender's strict credit criteria. Telemarketing helps target eligible leads; yet during these interactions, sensitive customer information can be exposed and misused.

Occupational fraud risk in customer acquisition affects all banks - yet digital banks face even higher risks. Although statistical modeling is widely used in other areas of risk management (e.g., credit risk), its effectiveness in detecting occupational fraud is limited by the scarcity of documented cases. According to the ACFE (2024) , fraud is most often identified through tips such as customer complaints rather than through proactive monitoring. Despite their rich natural language content (see Figure 1), these complaints remain underutilized due to their unstructured format and manual processing. For example, customer service representatives review these complaints and then forward them to the relevant departments for analysis and resolution.

```
Hi, I'm a small business owner and I'm really frustrated with what
happened. I was added on WhatsApp by someone from cell #012345679 who
claimed to be a relationship manager with XYZ Bank. He told me I could
get a loan at as low as 2.8% interest rate if I paid a facilitation
fee to speed up the process. I trusted him and paid the fee via
WhatsApp, but later ended up with an insanely high 18% offer. He also
sent me a picture of his badge with XYZ Bank logo. If this isn't
sorted out immediately, I'll take this matter to the regulatory
authorities.
```

Figure 1. An anonymized customer complaint record

the potential of LLMs

Large language models (LLMs) offer unprecedented natural language processing capabilities that can extract valuable fraud signals from unstructured customer complaints. However, as most LLMs are pre-trained on generic internet data, they can underperform on highly specialized tasks such as detecting insider fraud cues in digital banking. This article proposes an LLM-driven approach that seeks to improve both the precision and efficiency of fraud detection in this context, including:

1. Adaptive compliance policy understanding: LLMs scan internal policies and contracts to compile a more nuanced list of misconduct scenarios.
2. Automated misconduct mining: LLMs identify complaint records matching these misconduct scenarios and extract broker-related data.
3. Integration with social network analysis: LLM outputs integrate with additional analytics to reveal hidden networks linking insiders to brokers.

methodology and key considerations in real-life applications

To adapt LLMs for specialized tasks, we employ an in-context learning (ICL) approach, where the model is guided by instructions and examples embedded in the prompt. Figure 2 illustrates the core components of the proposed approach, with a detailed breakdown of both LLM and non-LLM elements provided.

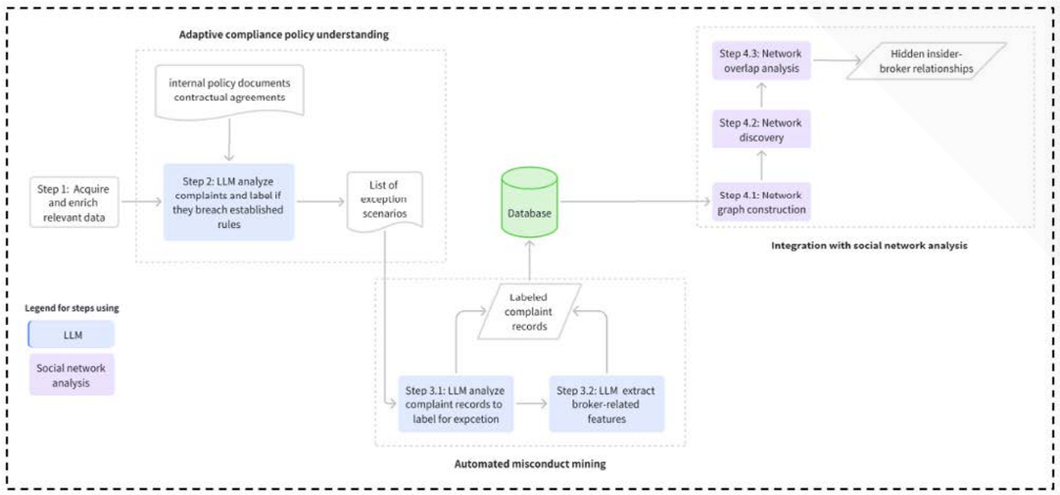


Figure 2. Overview of an LLM-driven approach to insider fraud detection

Step 1: Data filtering and enrichment

To maximize the accuracy of LLM outputs, it is essential to focus the input exclusively on the most relevant contextual data. To identify insiders (e.g., telemarketers) suspected of colluding with loan brokers, our approach specifically filters the input data so that the LLM processes only complaint records from customers contacted by telemarketing staff. Additionally, structured metadata is attached - such as customer identifiers and relationship manager details - to each record to facilitate downstream integration with other analytical techniques.

Step 2: In-context prompting: compliance policy understanding

Fraud investigations are inherently compliance-driven due to subsequent disciplinary and legal implications. While fraud detection must adhere to the guardrails defined by compliance policies, an LLM agent can leverage its natural language capabilities to proactively establish these guardrails. This can be achieved by embedding relevant policy documents and contractual agreements into a prompt query and instructing the LLM to compile a list of potential misconduct scenarios, as illustrated in Figure 3.

```
You are an expert in financial compliance and fraud detection within
XYZ Bank. Attached are the relevant policy documents and contractual
agreements for the bank. Analyze these attachments and compile a
comprehensive list of potential misconduct scenarios where non-bank
individuals impersonating bank staff.

Your output should serve as guardrails for subsequent LLM agents.
Please provide a detailed list with clear descriptions, potential
triggers, and implications for each exception scenario. For example:
Scenario#1:A prospective customer is approached by an offline loan
broker who falsely claims to be an XYZ Bank employee and displays a
counterfeit badge.
```

Figure 3. Template prompt for compliance policy understanding

Step 3.1: In-context prompting: misconduct labeling

Fraud investigations are inherently compliance-driven due to subsequent disciplinary and legal implications. While fraud detection must adhere to the guardrails defined by compliance policies, an LLM agent can leverage its natural language capabilities to proactively establish these guardrails. This can be achieved by embedding relevant policy documents and contractual agreements into a prompt query and instructing the LLM to compile a list of potential misconduct scenarios, as illustrated in Figure 3.

```
You are a misconduct inspector. Your task is to determine whether the
customer complaint record provided matches the misconduct scenario
below. Use only the information in the scenario as context.

Scenario: {context}

Complaint: {complaint record}

If the complaint corresponds to the scenario, respond with 'Yes' on
the first line; if not, respond with 'No'. On the next line, begin
with 'Justification:' and provide your reasoning.
```

Figure 4. Template prompt for misconduct identification

Step 3.2: In-context prompting: broker feature extraction

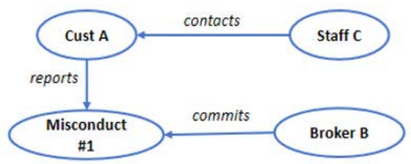
For each complaint record previously labeled as misconduct, an LLM-based feature extraction module scans for broker-specific details - such as cell phone numbers, social media IDs, or locations - associated with loan brokers. If these details are found, they are extracted and linked to the record for identifying brokers in subsequent analysis.

Step 4: Integration with other analytics

LLM labels from previous steps can be further integrated into social network analysis to examine both direct and indirect links between insiders - particularly telemarketers - and the misconduct identified in customer complaints. A practical integration approach includes:

Step 4.1: Social network graph construction:

This consists of both existing relationships from structured databases and new relationships from LLM-extracted information.



Existing relationship:
- A, a customer of XYZ Bank, is contacted by telemarketing staff C during origination process
- Cust A logs a complaint record

New relationship:
- Cust A's complaint is labeled as misconduct by LLM
- LLM also reveals that the act of misconduct was committed by B, a loan broker.

Figure 5. Integrating LLM outputs into social network graphs

Step 4.2: Network discovery:

Social network analysis can be an exhaustive process; however, this approach focuses on a few high-priority nodes and explores their relationships to reveal hidden networks of interest.

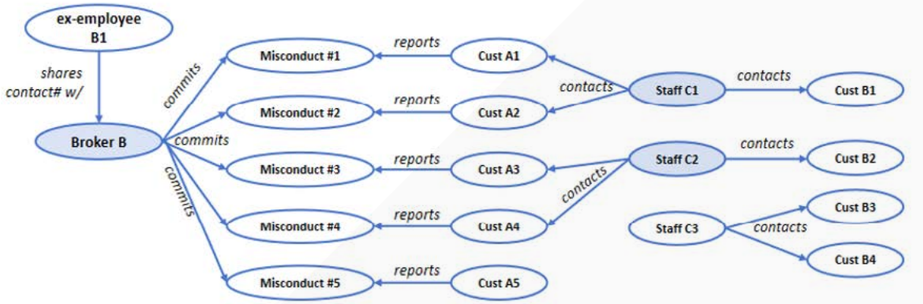
Such nodes are identified from two perspectives:

- Rule driven: Leverage human expertise or insights from prior investigations to define business rules for high-risk nodes. For instance, a broker may be flagged if evidence suggests this is a former telemarketer - determined by comparing contact information from complaint records with the employee database.

- Centrality driven: Use network centrality metrics, such as degree centrality - which counts a node's direct connections - to gauge influence. In our context, high degree centrality in telemarketers or loan brokers indicates that a significant percentage of their related customers have reported one or more cases of misconduct.

Step 4.3: Network overlap analysis:

Once the high-priority nodes' networks are mapped, overlapping connections may indicate risks of collusion. According to ACFE , fraud involving multiple perpetrators represent over half of identified cases and result in higher losses than those by a single perpetrator. While some overlap may be coincidental, a significant overlap is concerning. This can be quantified by calculating the percentage of a broker's network that shares connections with multiple high-priority telemarketers.



Node#	Degree Centrality	% reported misconduct	% linked to other high-priority nodes
Broker B	5	100.0%	80%
Staff C1	3	66.7%	66.7%
Staff C2	3	66.7%	66.7%
Staff C3	2	0.0%	0.0%

High priority nodes:
- Telemarketing staff C1&C2, 2/3 of their customers reports misconduct identified from complaint records
- Broker B, suspected as ex employee of XYZ Bank, 4/5 of customer who mentioned this broker are in network of staff C1&C2

Figure 6. Social network overlap analysis

methodology and key considerations in real-life applications

Our approach leverages LLMs to address the core challenges of occupational fraud by automating the extraction of fraud signals from complex, unstructured customer complaints and integrating these insights to map hidden insider-broker relationships. While further domain-specific calibration is needed, this work lays a practical foundation for holistic and efficient fraud detection in digital banking.

references

1. Association of Certified Fraud Examiners. (2024). Occupational fraud 2024: A report to the nations. https://www.acfe.com/-/media/files/acfe/pdfs/rttn/2024/2024-report-to-the-nations.pdf

author

Terrence Cai

Terrence Cai, FRM, CISSP, is an internal auditor at a leading digital-only bank based in China. He specializes in exploring machine learning and artificial intelligence to develop innovative analytics solutions for the bank's personal and SME lending business. Prior to joining the bank, he worked at Deloitte's Risk Advisory practice in China.

peer-reviewed by

Carl Densem

Synopsis

People make or break the teams we as risk managers work in. The author looks back over a career creating and running risk teams to assess what works and what fails. He lands on several easily glossed-over aspects: hiring properly, keeping things fun, transparency and involving everyone.

people lessons from a career in risk

by **Simon** Hillard

introduction

The key assets of any financial institution (FI) are its reputation and people; the former is probably determined by the latter. In the most open-minded FIs, people risk is the top risk. For example, at one asset manager, the leading risk in their stress testing process was the departure of their highest income generating team to a competitor.

As a risk manager, and indeed as any manager, the downsides of getting human relations wrong are serious. It's worth keeping in mind implications may include team underperformance, a potentially miserable working environment and numerous connected inefficiencies.

hiring: the crucial first step

Hiring is the core of a successful business, and yet I continue to be surprised at how badly this is often handled. Although it's accepted that the process should be meritocratic, far too often this is not the case. To ensure a meritocratic approach, the key skills required for the role should be agreed by management together with a set of practical questions designed to ensure the person has the requisite skills and experience. One step not always taken is ensuring there are AT LEAST two interviewers present to help make sure the process is truly fair; there is little point asking different candidates the same question if human bias clouds the judgement and demeanour of an interviewer. I am also keen on the candidate and team members meeting before a hire is concluded to help ensure a more transparent, consensual approach.

professionalism and fun

Successful teams need the correct culture. People are often afraid of raising fun in a work environment, and particularly in FIs, but combined with professionalism it becomes very powerful: an appropriate balance between the two is key. We spend so much of our lives in the office, we may as well enjoy it.

The best teams I have worked in have been particularly strong on these two core aspects. The two are by no means mutually exclusive and the fun side can often enhance professionalism if managed properly. As an example, team members will be far more willing to work longer hours or at weekends if required if they know they will have some fun doing it. A further benefit is that teams with this ethos will be more attractive to internal hires.

Bringing this to life could (include) INCORPORATE having a team offsite that accentuates these characteristics. Practically, this could include sub-teams preparing presentations on ways the team functions more effectively that are debated, actions agreed and minuted at the offsite. Follow-up should see that progress is discussed during the year with achievements covered at the next offsite. The offsite session should precede an afternoon of entertainment appropriate for the team.

If you are in a team that does not yet have offsites, it is worth suggesting the benefits of such an event to your management. These include getting to know each other better, working more efficiently as a team and hopefully having some fun.

transparency and appraisals

Transparency is vital for a happy and successful team. Clearly there will be confidential information that cannot be disclosed but erring on the side of openness will usually prove beneficial.

When a team member does something well tell them as soon as possible. Praise is undervalued and is such an easy way for a leader to enhance job satisfaction. Equally, it is important to properly handle situations when things go wrong. Issues have to be addressed promptly but always in private and whenever possible treated as a learning experience and not a “telling-off”. Related to this, appraisals should never have surprises; they should be a conclusion to what is already known and a discussion of ways to make things even better in the future.

I always encourage employees to maintain a directory of positives (and I do this myself) that includes any positive emails received and brief notes about achievements. This has many benefits including a source of positivity when you are having a bad day, examples that can be used to help justify pay increases and promotions, and a way to enrich your CV. Managers tend to have short memories and reminding them of your achievements throughout the year is beneficial to all.

covering all bases

Members of every team have valuable experience and opinions that should be effectively utilised. Managers can ensure these are expressed by new members of the team introducing themselves and flagging skills and experiences that could be pertinent, as well as and ensuring the team summarizes learnings from courses and conferences attended with a verbal overview at the daily or weekly meeting.

A skill that I (embarrassingly) only picked up recently was specifically asking more introverted people for their opinions during meetings. Introverts tend to have some of the best ideas but often will not disclose them without encouragement.

If you are at the earlier stages of your career, it is incumbent on you to learn from the good and bad you see in teammates, then emulate or banish them as appropriate. One of the best examples, from a former employer, was when management sent an email to a large division asking them to vote for the most inspirational person in the division with tickets to a prestigious sporting event as the prize. I am convinced the right person won and they are still happily working at that company.

conclusion

As is clear from this, I am a big fan of being open, social and hopefully inspirational. Just be careful not to ruin it, as a former colleague did after inviting the team to his house for a barbeque at the weekend and then asking them for payment on Monday morning!

author

Simon Hillard

Simon is a member of the London PRMIA chapter’s steering committee and currently a senior consultant at OneRisk Consulting. He’s had a long and varied career working at major financial institutions and has led and established new teams – including front office and risk – at many of them.

peer-reviewed by

Elisabeth Wilson

Synopsis

Shadow banking has been created, to some degree, by efforts to prevent future banking crises. The author explains this background, explores the players and their activities (both legitimate and illicit), then offers a fundamentally new and proven way to approach this thorny issue.

shadow banking: when demand turns dangerous

by **Stella** Grossu

shadow banking: when demand turns dangerous

In finance—much like in life—unmet demand always finds a supplier. When formal channels become too restrictive, costly, or cumbersome, alternative pathways spring up. That is precisely how shadow banking has flourished: providing services that traditional banks can not—or will not— offer. While it can foster innovation and fill legitimate market gaps, it can also become a safe harbor for money laundering, terrorist financing, and sanctions evasion. Understanding its origins, types, and impact is crucial for devising more effective ways to police financial crime—without putting a chokehold on economic growth.

defining shadow banking

Economist Paul McCulley popularized the term “shadow banking” in 2007 to describe credit intermediation largely occurring outside conventional banks. This realm spans hedge funds, money market funds, peer-to-peer lending platforms, special-purpose vehicles, and more. While such entities can effectively fund start-ups or bridge short-term capital needs, they generally face fewer regulations than mainstream banks. This lighter oversight makes them agile and innovative but also opens the door to questionable or even criminal practices.

The boundary between a non-bank financial intermediary and “shadow banking” isn’t always black and white. Broadly, it refers to any setup that mirrors the lending or payment functions of banks while circumventing the scrutiny placed on depository institutions. Thus, shadow banking can offer real economic benefits yet also attract criminals who exploit its relative opacity.

regulations gone awry

Post-2008, policymakers worldwide launched stricter banking rules—like Basel III, tighter Anti-Money Laundering (AML) directives, and enhanced Know Your Customer (KYC) requirements. These aimed to preempt future meltdowns by demanding bigger capital buffers and more compliance from banks. Yet higher capital thresholds mean tying up funds that might otherwise be used for lending, hurting banks’ returns on equity. Rather than take the hit, many institutions “de-risk,” withdrawing from riskier or lower-profit activities such as trade finance for small exporters or cross-border remittances to emerging markets. While the supply is cut off, the demand for those activities does not vanish; it shifts into corners of finance unencumbered by the same rules, thereby enlarging the shadow banking sector.

Fear of reputational damage and colossal fines also spurs banks to cut ties with entire customer segments deemed even mildly suspicious. While intended to thwart money laundering and terrorist financing, it often ostracizes legitimate enterprises. Shadow banking outfits, facing fewer constraints, then swoop in to serve these sidelined players—sometimes for legitimate purposes, sometimes for dubious ends.

legitimate shadow banking

Shadow banking need not be synonymous with crime. A host of non-bank intermediaries brings genuine value to markets:

- Hedge Funds and Money Market Funds - these pooled investment vehicles inject liquidity and credit, often exploring higher-risk niches that traditional banks avoid. Though governed by less rigid rules than depository institutions, they typically function within a legal framework, broadening options for both businesses and investors.
- Fintech Companies - from peer-to-peer lending to mobile payments, fintech ventures leverage technology to reach customers who may lack access to traditional banking. They can expedite cross-border transactions, lower fees, and boost financial inclusion.
- Alternative Investment Fund Managers (AIFMs) and Private Equity Firms - targeting institutional and high-net-worth clients, these entities invest in specialized or higher-risk ventures. Less regulated than banks, they channel capital into areas where mainstream lenders are hesitant, fueling innovation and growth.
- Trade Finance Specialists - by purchasing unpaid invoices (factoring) or extending short-term credit, these specialists help small importers and exporters keep goods moving, especially in markets where big banks have withdrawn.

Each of these legitimate channels delivers real economic benefits. However, even lawful shadow banking can amplify systemic risks if leverage or credit exposure ramps up without adequate oversight.

illicit shadow banking

Alongside legitimate endeavours lies a darker undercurrent. Criminal enterprises exploit minimal monitoring to transfer funds across borders, mask their origins, and bankroll illegal ventures:

- Underground Currency Exchanges - unregistered remittance networks use minimal documentation to shuffle huge sums globally, sometimes via “mirror” trades that hide the physical movement of money.
- Shell Companies and Gold Transfers - groups avoiding sanctions or seeking anonymity deploy opaque corporate structures and trade gold to dodge electronic traces, frustrating investigators’ efforts to track beneficial owners.
- Money Laundering Networks - whether rooted in narcotics, terrorism, or corruption, these networks funnel illicit proceeds through multiple “shadow” conduits. Their evasion tactics exploit differing rules across jurisdictions and lax reporting requirements.

By operating beyond the reach of strict bank regulations, illicit shadow banking threatens not just the financial sector’s integrity but public safety too. It fuels crime, erodes trust, and can undermine entire economies.

a bold new direction: let banks be banks

Rather than forcing banks to wear the badge of crime-fighting—drowning them in compliance tasks—policymakers could adopt a more strategic approach grounded in three pillars: focusing banks on core banking, empowering specialized law enforcement, and ensuring data-access safeguards. The biggest pitfall to avoid is creating an Orwellian surveillance regime, so proper guardrails are essential.

A well-structured system would limit law enforcement access strictly to data relevant for criminal probes, ensuring each request is documented and authorized (Eurojust, 2022). For instance, regulators in the EU now provide cross-border account registries to investigators, but each query is tracked for legitimacy. Meanwhile, FinCEN in the United States centralizes suspicious activity reports, allowing investigators to share intelligence swiftly, though only under usage agreements that discourage fishing expeditions.

Privacy remains paramount. Authorities might see who controls an account and transaction patterns but not unrelated personal details like health status or political leanings. Court warrants can further protect against unwarranted searches, giving innocent clients confidence that their everyday banking remains private. This structure frees banks to innovate and serve, while dedicated law enforcement can more effectively combat large-scale financial crime.

It is a model that has already shown promise. In the UK, the Joint Money Laundering Intelligence Taskforce (JMLIT) closed thousands of fraudulent accounts and recovered millions in illicit funds by fostering collaborative data exchange without strangling banks in red tape. On a larger scale, bridging formal regulation with targeted enforcement could reshape shadow banking globally, trimming the gray areas criminals exploit while preserving fast, flexible finance for legitimate users.

conclusion

Regulations like higher capital requirements were introduced to prevent financial disasters, yet they often spur the growth of the very shadowy networks they are meant to constrain. By diminishing profitability and fueling “de-risking,” these rules sometimes push otherwise routine financial activities into darker spaces. While countless non-bank entities offer beneficial, innovative services, others open the door to large-scale money laundering and terror funding.

Rather than piling on more compliance, lawmakers could strike a balance: let banks stick to banking and let specialized agencies tackle crime with well-defined, transparent data-access rules. This dynamic approach promises to curb illicit finance without suffocating the innovation and flexibility that serve legitimate businesses. If carried out effectively, it may finally bring enough daylight into the shadows to preserve market vitality while stamping out the worst abuses.

Disclaimer: AI was used by the author during the editing phase of the article.

references

1. Basel Committee on Banking Supervision. (2011). Basel III: A global regulatory framework for more resilient banks and banking systems. Bank for International Settlements.
2. Eurojust. (2022). Eurojust annual report 2022. https://www.eurojust.europa.eu/annual-report-2022
3. McCulley, P. (2007). Teton reflections. PIMCO Global Central Bank Focus.
4. National Crime Agency. (n.d.). Joint Money Laundering Intelligence Taskforce (JMLIT). https://nationalcrimeagency.gov.uk/
5. United Nations Office on Drugs and Crime. (2020). Money-laundering and global financial flows. https://www.unodc.org/unodc/en/data-and-analysis/iff.html

author

Stella Grossu

Stella Grossu is an experienced financial risk management professional specializing in credit, market, and liquidity risks. She develops and oversees frameworks aligned with stringent regulatory requirements, including credit underwriting, portfolio performance monitoring, and capital reporting. Having led audits and contributed to ICAAP assessments, Stella is committed to cultivating resilience in financial systems. In addition to mentoring emerging risk professionals, she actively promotes innovation in risk management, ensuring sustainable growth and robust safeguards in a complex, fast-evolving market landscape.

peer-reviewed by

Rick Nason

Synopsis

Behavioral finance is starting to influence how risk managers view the market and its participants. By understanding biases that evolved in our species for survival in the context of financial markets, risk managers can notice them arise and better consider their options.

why is behavioral finance important to risk managers?

by **Maya** Katenova

Behavioral finance is a new discipline today. It grew rapidly in the 1990s, but has a much longer history. The concept of behavioral finance came into existence in 1912 when George Seldon published “Psychology of the Stock Market.” However, this theory gained popularity only in 1979 when Daniel Kahneman and Amos Tversky proposed that investors tend to make decisions based on subjective reference points, emotions and perceptions rather than objectively choosing the best option. In other words, the efficient market hypothesis is not taken into account and investors are not rational in their decisions.

One year later, Richard Thaler introduced the notion of “mental accounting,” which is the idea that people treat their money differently based on its function, whether it is for retirement or a college fund. "Behavioral finance is the application of cognitive psychology to finance,” says Bradley Klontz, PsyD, CFP®, associate professor of practice in the Department of Economics and Finance at Creighton University. “Cognitive psychology examines how people acquire, process and store information, and it explores ways in which that affects emotions and behavior.

Financial professionals as well as risk managers use behavioral finance to help their clients identify and overcome certain psychological biases so they can make better financial decisions. “If we understand what drives people to act irrationally in regard to their finances, experts can begin to build a framework to help people make better decisions—and that can help us better understand market behavior overall,” Klontz says. “Understanding behavioral finance can help you better serve your clients,” he adds.

From the perspective of a risk manager, behavioral finance provides an opportunity to refine the analysis of market dynamics and investor interactions. While some investors disregard established theories, relying entirely on their emotions, their decisions are often characterized by irrationality, treating the stock market as if it were a giant casino. To better understand market behavior and its participants, this section explores five biases central to behavioral finance.

five common biases in the sphere of behavioral finance

When we become emotionally charged, we become rationally challenged and biases kick in. We make decisions from our emotional brain—which can work great in terms of our survival as a species—but it may not be as beneficial to us in our investment decisions.

1. Loss aversion

Loss aversion is our natural tendency to avoid a real or perceived loss. This, in turn, affects how we make decisions relating to our personal finance investments. Our disposition is to hold losing stocks, allowing losses to accumulate. For example, excessive trading losses are usually limited among professional traders. “Stop losses” help prevent this instinct to hang on until the losses reverse. Risk managers should be aware that investors who have lost money may try to take excessive positions to “win” it back.

2. Familiarity bias

Familiarity bias is a cognitive bias that causes people to prefer familiar options over unfamiliar ones, even when the unfamiliar options may be better. “The more familiar we are with something, the more likely we are to make wrong decisions about it,” says Professor Klontz. Investors may prefer investing in familiar stocks or companies rather than exploiting new investment opportunities. For example, despite the fact that new investments offer better return, investors still prefer those which are familiar. This bias leads to a less diversified and less profitable investment portfolio.

3. Herd instinct

Herd instinct refers to investors’ tendencies to follow what other investors are doing rather than their own research and analysis. If everyone does it, why not do the same? We are lazy to think and make our own decisions. “If everyone in your tribe got up and started sprinting south, it's a good idea for you to get up and start sprinting south,” Klontz says. The herd instinct affects all investors indiscriminately and causes irrational decisions. For example, investors may follow the crowd in purchasing overvalued stocks, leading to financial bubbles and subsequent crashes. The dot-com bubble and the housing bubble are prominent examples of how herd mentality can lead to market instability and even financial losses.

4. Overconfidence bias

Overconfidence bias is the tendency of investors to overestimate their knowledge, skills and abilities. One of the key ways we see this bias play out is that, on average, women are better investors than men. “One of the reasons for this is that women may possibly feel less confident in their ability to predict the right/correct investments,” Dr. Klontz says. “Men tend to feel overconfident in their abilities, which causes them to trade more than women. By trading more, they hurt their performance.” A study by Fidelity Investments confirms this fact.

Based on an analysis of the annual performance of 5.2 million accounts, the study discovered that female investors tend to achieve positive returns and outperform men by 0.4%. Despite uncertainty felt by managers about the market, the tendency is to be fully invested with a small allocation to cash. This displays and overconfidence in the ability to outperform even when cash (and cash-like positions) offers better downside protection.

5. Status quo bias

The status quo bias is people's preference for things to stay as they are by sticking with a decision made previously. Stability is not always good for risk managers. The market changes rapidly and risk managers need to adapt quickly. Why do investors fall into this trap? Sometimes, investors simply become complacent and think existing conditions are going to "go on forever and will never change." This belief can lead them to take no action on, say, interest rate changes or stock market trends, even if doing so would better align their portfolios with their goals. Thus, when conditions eventually do change, their portfolios suffer and a less-than-desired financial outcome is the result. In today's market, status quo bias is taking place on a macro scale. For example, investors have enjoyed a bull market in bonds for the past 20-30 years. Some investors' portfolios are not ready for the fact that interest rates are likely to rise next year. However, status quo bias will likely persist, and investors will keep their bond positions static.

conclusion

Understanding behavioral finance can help financial planners, risk managers and investment analysts better serve their clients. Financial professionals, who can use behavioral finance at their job place to help their clients, identify and overcome financial biases and mistaken heuristics will provide more valuable advice. In addition, experts in behavioral finance are viewed as thought leaders in the financial industry, which can further advance their career. Behavioral finance is not a new science but it offers new approaches for risk managers to understand investing. It continues to expand further and explain more about how humans behave toward markets.

author

Maya Katenova DBA, PRM, CMA

Dr. Maya Katenova is an Assistant Professor of Finance at KIMEP University. Maya teaches bachelor's and master's students, including Executive MBA students. She received a Teaching Excellence Award in 2017. She taught numerous finance courses. She supervised master's thesis dissertations of several students and has numerous publications in different journals including high-quality journals. Her research interests are mostly related to corporate social responsibility and global ethics. Maya holds the Professional Risk Manager designation. Maya is also a Certified Management Accountant (CMA) and active researcher.

Synopsis

This article examines the strategic role of risk management in modern organizations, emphasizing the importance of aligning risk management with business objectives. It highlights the challenges of integrating risk management due to the varying performance metrics used by different business units and suggests that a unified approach is essential for optimizing business performance and risk mitigation.

improving organization performance using risk management

by **Damilola** Fene-Osakwe

introduction

Risk management is increasingly taking on a more strategic role within organizations, serving as a catalyst and business partner to reinvent operating models, support decision-making, and create value in a dynamic and ever-changing economic landscape. Over the years, this discipline has evolved, and the application of risk management principles in businesses of all sizes is becoming more widespread. Significant global events at the turn of the 21st century, particularly the Global Financial Crisis of 2007-2009, the COVID-19 pandemic, and various nation-state conflicts, have heightened interest in risk management. These events have encouraged business leaders to explore different models and governance structures to maximize the benefits of risk management.

Box 1. Definitions

Risk Sponsor: A senior-level individual within an organization who actively advocates, supports, and oversees risk management process for a specific area, function or subject matter.

Risk Vision: A shared view of the role of risk management in an organisation and the capabilities desired to manage its key risks; articulated and agreed by senior executives; and aligned with the organisation's strategic objectives.

Risk Appetite: A description of the amount and types of risk an organisation is willing to seek or accept in order to achieve its objectives.

Risk Maturity: The level and quality of integration of an organization's risk.

role of risk management and the expectations of business leaders

Organizations are adopting proactive risk management strategies to protect assets and reputations amidst geopolitical events. Business leaders are engaging in risk discussions and investing in programs that uncover opportunities, create value, and offer a competitive advantage.

Aligning business and risk involves embedding risk management in strategic planning, decision-making, and operations. Early identification and addressing risks lead to improved financial planning, informed decision-making, and resilient strategies. Optimized risk frameworks enhance the evaluation of opportunities, proactive mitigation, and better interpretation of business insights.

Despite recognition of risk management's role in achieving strategic objectives, challenges persist due to differing views on its role and benefits. For sustainable growth, senior stakeholders must maintain a unified strategic perspective on risks and align with a clear vision. The risk management sponsor plays a crucial role in engaging stakeholders, facilitating discussion on the importance of risk, and investing in capacity and technology to achieve the vision. Defining a risk vision and establishing a risk appetite are also crucial. Active risk management support is essential for business growth and must be developed alongside the core business.

disconnect between objectives and performance metrics

> ***Data sovereignty, commensurate with the growing importance of data as an asset, is a determining factor in global tech mergers and acquisitions, at the intersection between politics, geography and technology.***

High-performing organizations with well-defined risk strategies and operational models still face practical challenges. When the metrics used to assess the performance of business processes differ from those used for risk processes, the results often become disparate. For instance, while product, sales, and customer-facing teams focus on targets and performance measures such as sales growth, market share, and return on investment (ROI), risk metrics typically relate solely to risk activities - such as risk culture, risk maturity, risk framework implementation, and tracking of risk mitigation efforts.

As a result, while businesses measure success through financial performance and customer trust, risk functions focusing on non-financial metrics without a direct link to business performance tend to become isolated. This disconnect presents a significant challenge in successfully integrating risk into business processes, even for organizations that are considered high performing with mature risk processes. Many of these organizations still struggle to keep pace with business changes, with risk teams lagging in data insights, technology tools, and executive support compared to core business functions.

The misalignment of performance and risk measures is also evident in the hiring process for risk managers. I have observed that the criteria for evaluating candidates for risk management roles primarily focus on skills related to building and implementing risk frameworks, risk assessment and evaluation techniques, the use of data and technology tools, and sometimes stakeholder communication and engagement. However, there is often less emphasis on connecting risk management performance to overall business success. Organizations seeking to become industry leaders must create strategies that enhance the synergy between risk and business performance, and factor this into the hiring process.

maximising synergies beyond collaboration

Business leaders can harness the synergies between risk and business better when they can ensure operational teams, risk owners, and risk managers work together with a common understanding of what constitutes organizational success. Every employee should have, to some degree, key performance indicators (KPIs) related to risk mitigation, risk-based decision-making, and accountability included in their performance evaluations, which should be communicated clearly from the beginning of the business relationship.

Furthermore, the risk team's KPIs should include metrics that demonstrate the value of risk management to the business, such as the cost savings from operational controls compared to the costs incurred from risk materialization, as well as the costs of incident response versus the savings realized from early risk identification and scenario planning.

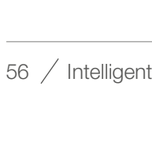
Take a manufacturing company facing potential obsolescence and revenue impact due to disruptive innovations. An integrated strategic risk management framework helps define the business's risk appetite for technology and growth, aligning it with the vision, mission, and strategic objectives. This framework sets the basis for "early warning signs," tracking technological trends, market changes, and business responses. These warning signs, which can be called key risk indicators (KRIs), help the organization proactively identify and mitigate potential disruptions, making it agile and resilient; turning threats into opportunities and positioning it as a market leader.

conclusion

Ultimately, it is an “all-hands-on-deck” approach to maximize synergies through Enterprise Risk Management. Holistic risk management goes beyond Risk Control Self-Assessments (RCSAs), Key Risk Indicators (KRIs), and traditional risk methodologies. It requires active collaboration and a shared focus among stakeholders to align their expectations and priorities. A proactive, technology-driven approach ensures that risk management remains a competitive advantage, enabling businesses to navigate uncertainties while seizing new opportunities for long-term success. It also involves fostering a culture that embraces technology, consistent performance management, and agile adaptation to the ever-changing business environment.

author

Damilola Fene-Osakwe



Dami has over a decade of experience in risk management across various sectors, including telecoms, financial services, and hospitality in the EMEA region. She has worked with renowned consulting firms like Accenture, Deloitte, KPMG, and BDO.

Dami specializes in Enterprise Risk Management and facilitates strategic risk workshops for senior management. She holds respected certifications in risk management and business continuity. She is also a speaker, writer, and thought leader with several published articles on risk management. Additionally, she co-founded the Fene Osakwe Foundation, engaging in community projects in Nigeria.

peer-reviewed by

Shachi Sayata

Synopsis

Understanding and managing "human data"—the knowledge and skills of employees—is crucial. This article discusses the importance of continuously updating employee knowledge to minimize risks and enhance organizational performance, emphasizing that outdated skills can lead to costly mistakes and compliance issues.

human data: the key to managing people risk?

by **Kenneth** Owusu Asante Amponsah

Managing employee knowledge and skills—often termed "human data"—is a critical yet often overlooked aspect of risk management in financial institutions. Ensuring that employee knowledge remains dynamic and up to date not only minimizes risk but also improves decision-making processes and boosts organizational performance.

human data: a double-edged sword

Employees represent both the greatest source of risk and most promising opportunity for financial institutions. A single poor decision - often stemming from outdated or incomplete knowledge - can undermine years of effort to optimize business practices. Conversely, informed, well-trained employees can deliver significant rewards. For instance, a risk officer with outdated regulatory knowledge may inadvertently expose an institution to compliance violations, while an informed professional can proactively ensure adherence to evolving standards.

Throughout my career, I've witnessed both positive and negative outcomes stemming from employee knowledge management. The key factor was whether sound risk principles were applied or neglected.

the problem: outdated human data

Many organizations focus on one-time training initiatives yet fail to implement systems for continuously updating employee knowledge. Traditional approaches, such as annual workshops or standardized e-learning modules, often fall short in providing the necessary agility and resilience required in today’s rapidly evolving business environment. As the pace of change accelerates, the "half-life" of skills—the period within which a skillset becomes half as relevant—is estimated to be just five years. Without continuous updates, employees risk making costly errors.

Performance consultant Jane Hart notes that skill relevancy declines significantly over time. By the time employees gain confidence in their roles, their knowledge may already be outdated. This underscores the urgent need for processes that enable learning.

Neglecting regular enhancements to human data leads to increased risks, higher costs due to errors, and missed opportunities. Employees themselves often recognize the importance of staying professionally current. They understand the personal stakes—retaining their jobs, advancing their careers, and remaining competitive in a fast-evolving landscape.

the solution: dynamic learning environments

Financial institutions must move beyond static, one-time training programs to adopt comprehensive approaches that integrate formal training, self-directed learning, and social collaboration. In most traditional setups, employees rely on employer-led training initiatives without proactive opportunities for self-improvement. However, this approach is no longer sustainable in an era where regulatory frameworks, technological advancements, and risk landscapes evolve continuously.

A more effective approach, referred to as a "learning and performance ecosystem," connects employees to diverse learning opportunities while maintaining organizational oversight. According to Marc J. Rosenberg and Steve Foreman, such ecosystems enhance individual and organizational effectiveness through six interconnected components:

1. Talent Management –Actively tracking employee skills and addressing gaps to inform training priorities.
2. Performance Support – Providing employees access to on-demand resources, such as quick-reference guides or AI-driven assistance.
3. Knowledge Management – Creating centralized knowledge repositories to ensure preservation and accessibility of institutional knowledge.
4. Access to Experts – Facilitating mentorship and knowledge-sharing networks within the organization.
5. Social Networking and Collaboration – Encouraging peer-to-peer learning through digital communities and collaborative tools.
6. Structured Learning – Reinforcing formal training with interactive assessments and ongoing learning opportunities

By incorporating these components, institutions can ensure employees have continuous access to timely and relevant knowledge, reducing risks while fostering innovation and growth.

integrating technology to optimize human data

Modern technologies can play a transformative role in managing human data effectively. AI-powered tools and machine learning algorithms can:

- Personalize Training: Tailor learning programs to individual needs and job roles.
- Monitor Skill Development: Use analytics to monitor employee progress and identify gaps in real-time.
- Automate Routine Tasks: Enable employees to focus on strategic decision-making by automating repetitive processes.

For example, virtual reality (VR) simulations can offer hands-on learning experiences, while AI chatbots can provide instant support for complex tasks. These technologies not only enhance human data but also improve employee engagement and job satisfaction.

By adopting integrated learning ecosystems powered by advanced technology, financial institutions can gain a significant competitive edge.

clarifying employer vs. employee responsibilities in training

A key challenge in continuous learning is defining the responsibilities of employers and employees. Employers are responsible for providing structured training programs, access to learning resources, and fostering a culture that values skill development. Meanwhile, employees must take ownership of their learning by seeking out opportunities, engaging with training materials, and applying new knowledge in their roles.

Organizations that clearly define and support these roles will see greater success in cultivating a skilled and adaptable workforce, leading to reduced risks and enhanced overall performance.

conclusion

Managing human data is essential for financial institutions aiming to minimize risk and maximize reward. By adopting integrated learning ecosystems, leveraging technology, and fostering a culture of continuous learning, organizations can reduce errors, improve decision-making, and unlock potential.

Institutions that prioritize the development of human data will not only shift the balance decisively toward reward over risk but also achieve sustained growth, by harnessing the incredible potential of their employees.

author

Kenneth Owusu Asante Amponsah

Kenneth is a visionary and results-driven banking executive with over 15 years' experience (8 years' leadership) in the financial services sector. Proven expertise in strategic leadership, risk governance, financial performance optimization, and corporate transformation. A dynamic leader with a strong track record in ensuring risk & regulatory compliance, driving profitability, and managing stakeholder relations.

He is adept at aligning business strategies with risk policies to drive sustainable growth and resilience in the banking sector. He is married with two kids and often writes on financial risk management.

peer-reviewed by

Jammi Rao

Synopsis

This article highlights the lessons learned from recent financial crime regulatory actions and outlines strategies for financial institutions to develop robust risk management frameworks. Readers will gain insights into navigating the complexities of financial crime risk management in an evolving regulatory landscape and learn how leveraging advanced technologies like AI and machine learning, and fostering a strong culture of compliance, helps institutions to effectively detect and prevent illicit activities.

managing financial crime risks in a challenging business and regulatory environment

by dr. **Artur** Preus

In today's rapidly evolving business and regulatory landscape, managing financial crime risks has become a paramount concern for financial institutions. Increasingly stringent regulations, technological advancements, and the complexities of global financial systems create a challenging environment for banks and financial services providers.

This article explores these challenges, lessons learned from past failures, and strategies that financial institutions should adopt to create effective and compliant financial crime risk management frameworks for risk prevention and detection.

lessons from regulatory actions

The financial services sector operates within an environment shaped by rapid technological evolution, shifting approaches to globalisation, and increasingly dynamic regulatory requirements.

Advancements in artificial intelligence, machine learning, and blockchain are redefining how financial institutions detect and prevent illicit activities. They also introduce new risks, such as exploitation of digital assets for money laundering and fraud.

Simultaneously, recent geopolitical developments and economic fragmentation are leading to more localised regulatory approaches and increased divergence in financial crime compliance standards. Countries are likely to either adjust their already defined approach to balance innovation with oversight – or further tighten their financial crime regulations to protect national security and economic interests, resulting in an even more complex, multi-jurisdictional compliance landscape for financial institutions. In addition to this, many regulators have stepped up their oversight activities and conducted an increased number of audits, resulting in a string of actions against some of the leading financial institutions.

Notable examples include TD Bank's case. In October 2024, TD Bank agreed to pay over $3 billion in penalties after pleading guilty to violations of the Bank Secrecy Act and anti-money laundering regulations. From 2014 to 2023, the bank's inadequate AML controls allowed criminal networks to launder more than $670 million through its accounts, including over $470 million linked to drug trafficking. Internal reports and regulatory warnings about insufficient transaction monitoring were ignored, and the bank failed to file Suspicious Activity Reports for over $1.5 billion in suspicious transactions.

In November 2024, Metro Bank was fined £16.7 million by the UK's Financial Conduct Authority for failing to adequately monitor over 60 million transactions, totalling more than £51 billion, for money laundering risks between 2016 and 2020.

Additionally, in December 2024, Wise, a fintech company, was reprimanded by the National Bank of Belgium for inadequate anti-money laundering controls including the absence of proof of address for numerous customers.

The above and other recent financial crime regulatory failings have underscored significant deficiencies within financial institutions' compliance frameworks. The most common issues pointed out by regulators include the following:

- Inadequate risk assessments: Many organisations fail to fully understand their exposure to financial crime risks, leading to incomplete or superficial risk evaluations. This often results in misaligned controls and resource allocation, leaving institutions vulnerable to exploitation.
- Weak governance and oversight: A lack of accountability, fragmented responsibilities, and inadequate communication between compliance and other teams hinder institutions' ability to respond effectively to existing and emerging threats.
- Ineffective risk monitoring: Institutions often rely on outdated or poorly calibrated systems that fail to identify changes in customer circumstances or suspicious activities.
- Deficient culture of compliance: Insufficient training, inadequate awareness among employees, and the perception that compliance is secondary to other business priorities weaken the overall compliance culture.
- Failure to use technology and data effectively: institutions struggle to harness the full potential of advanced technologies and data for risk management due to the complexities of legacy systems, data silos and quality.

These issues and regulatory observations emphasize the necessity for robust, dynamic, and supported by the advanced technologies compliance programmes withing financial institutions.

sustainable financial crime risk management framework

To address these issues and meet regulatory expectations, financial institutions must implement a financial crime risk management strategy that ensures sustainable compliance. This requires a holistic approach that integrates strategic, operational, and technological components (see Figure 1).

First institutions should establish a comprehensive and dynamic risk management framework that integrates risk appetite and risk assessment components into an ongoing process. This model should continually evaluate risk factors and their impacts on controls and performance, ensuring that the institution's risk appetite remains informed by feedback.

Next, a robust governance and organisational structure should clearly define roles, responsibilities, and accountability for financial crime risk management. This includes ensuring senior management's involvement, as their support is crucial in fostering a culture of compliance. Moreover, risk management responsibilities should be supported by adequately staffed teams at all organisational levels, from front-line to leadership, across all lines of defence.

Figure 1. Holistic and sustainable Financial Crime Risk Management framework.

Advanced technology and a comprehensive data framework play a pivotal role in sustainable risk management. Institutions should invest in technologies like AI, machine learning, and data analytics to enhance their ability to detect and prevent financial crimes in real time.

These technologies can help identify potential risks during customer onboarding and before transaction execution, as well as patterns of suspicious activity throughout the customer journey that might otherwise go unnoticed, improving the accuracy and efficiency of risk assessments and monitoring systems.

FIs should ensure that regardless of technology type they are supervised by humans during their implementation and ongoing use, and that their outcomes are compliant and explainable.

Collaboration with internal and external stakeholders – such as regulators, law enforcement agencies, and other financial institutions – is also essential. By participating in information-sharing initiatives and adhering to international standards (e.g., Financial Action Task Force (FATF), Basel Committee on Banking Supervision (BCBS), Wolfsberg Group), institutions can ensure that their financial crime risk management approaches align with global efforts to combat illicit activity.

Finally, financial institutions should also adopt a continuous learning and improvement mindset. Staying current on the latest trends in financial crime, regulations, and best practices ensures that risk management practices remain relevant. This may involve regular staff training and conducting independent tests and assurance assessments.

Through these combined efforts, financial institutions can build a financial crime risk management framework that is not only effective but also sustainable in the long run, evolving as new risks and technologies emerge.

the path forward

Managing financial crime risks in today's challenging business and regulatory environment is a significant undertaking. However, by addressing recurring issues and adopting a sustainable, compliant framework, financial institutions can better protect themselves, their customers, and the global financial system.

Moving forward requires a holistic approach that balances regulatory expectations, technological advancements, and a strong commitment to ethical practices.

As financial institutions work to maintain trust and integrity, they must recognise that effective financial crime risk management is not just a regulatory obligation, but a crucial component of long-term success. By fostering a culture of compliance, leveraging cutting-edge technologies, and committing to continuous improvement, institutions can navigate today's complexities and emerge stronger and more resilient.

author

Dr. **Artur** Preus

Financial crime strategist and practitioner with over 25 years in designing, developing and implementing financial crime and client lifecycle operating models across the 3 Lines of Defence in the financial services industry.

Acquired valuable experience at top-tier financial institutions, including HSBC, Deutsche Bank, Standards Chartered, Nordea, Allianz and WorldPay.Important achievements include the transformation of the 1st and 2nd LoD framework for a global bank operating in 44 jurisdictions, addressing the requirements of the US Deferred Prosecution Agreement ($1.9B fine). Member of ACAMS and ICA, holding professional certificates from each organisation. Additionally, affiliated with the Business Architecture Guild and participating in its Financial Services Industry Reference Model working group.

peer-reviewed by

Mayank Goel

Synopsis

In April, the PRMIA Kingdom of Saudi Arabia Chapter brought together two Intelligent Risk authors to speak to their local members on seemingly different topics. However, deep connections exist between the discussion of the financial system and fraud detection using GenAI, which would have been difficult to uncover without events like this.

from systemic risk to self-attention: bridging global banking vulnerabilities and gen.AI models in financial crime detection

by **Sara** Ricci

introduction

In an era defined by interdependence, modern financial risk management faces two parallel challenges: understanding the fragility of the global banking system and adapting to the accelerating capabilities of artificial intelligence. At the April 2025 PRMIA Kingdom of Saudi Arabia (KSA) Chapter event, two distinct yet thematically connected talks highlighted this duality. The first, by Andrea Calef, examined systemic risk from a structural and regulatory lens. The second, by Chandrakant Maheshwari, showcased how transformer-based GenAI models can bring context-aware intelligence to fraud detection. Together, they framed a compelling narrative about the future of risk monitoring—one that spans systemic fragility and model-based foresight.

session 1: systemic risk and the banking ecosystem

Andrea Calef opened his session by questioning a foundational blind spot in the risk discourse: what exactly constitutes a "system"? He argued that the literature often skips over this definition, even though understanding a system's components and interconnections is vital to identifying how systemic risk propagates. A financial system, Calef emphasized, is not merely a collection of institutions but a web of evolving interactions—among banks, households, firms, and markets.

He framed this network using the analogy of a financial circulatory system. Just as the heart pumps blood throughout the body, banks circulate capital across the economy. Disruption in this flow—whether through a liquidity crunch or a confidence shock—can impair the system's function, much like cardiac failure.

Calef contrasted direct finance (capital flowing through markets) with indirect finance (capital mediated by banks), underscoring the indispensable role of intermediaries in economic resilience.

Banking, he continued, involves three fundamental transformations: liquidity, maturity, and risk. These functions—turning short-term deposits into long-term loans, managing interest rate mismatches, and transforming risk through diversification—enable economic stability but also introduce vulnerabilities. These vulnerabilities manifest as confidence, liquidity, or solvency risks, each with the potential to spiral into systemic threats.

To manage these threats, Calef reviewed regulatory safeguards including capital adequacy ratios, liquidity coverage metrics (LCR, NSFR), and deposit insurance schemes. He cautioned, however, that such protections must balance stability with moral hazard. Systemic risk, in his view, is not a distant crisis but a constant negotiation between structure, behavior, and oversight.

session 2: gen.AI and self-attention in fraud detection

Chandrakant Maheshwari transitioned the discussion from macro systems to micro-patterns—specifically, how transformer-based GenAI models detect fraud. Using a classroom analogy, Maheshwari illustrated the concept of self-attention: a teacher asking four students with different areas of expertise to answer a question, then weighting each response based on relevance. This, he explained, is akin to how transformers calculate query, key, and value scores to interpret language—or, in this case, transaction data.

The power of this approach lies in its contextual awareness. Traditional rule-based fraud systems treat each transaction in isolation. Transformers, by contrast, analyze sequences of transactions as interconnected narratives. This allows the model to detect subtle shifts and patterns that static models overlook.

Maheshwari walked the audience through a case study involving six transactions. He described how each transaction was embedded with numerical vectors representing its attributes, then passed through self-attention layers. By dynamically learning which parts of the sequence are most indicative of fraud, the model effectively "reads" behavioral intent over time. The result: a fraud detection system that mimics human reasoning but operates at machine speed and scale.

bridging the talks: complexity, context, and clarity

Though operating at different altitudes, both sessions converged on a key insight: risk is no longer static or siloed. Calef's macro-level examination of systemic interdependence and Maheshwari's micro-level use of self-attention both illuminate the complexity of modern financial systems. Risk today demands not only robust structures but also adaptive intelligence. In this light, GenAI is not a replacement for traditional safeguards—it's an interpretive layer that helps make sense of evolving behaviors.

Moreover, both talks underscored the value of explainability. Whether through regulatory transparency or model interpretability, the ability to trace how conclusions are reached—be it a policy response or a fraud alert—is central to building trust in both systems and models.

conclusion

The PRMIA KSA Chapter event succeeded not just in delivering expert knowledge, but in stitching together a coherent narrative about the future of risk management. From defining what constitutes a financial system to demonstrating how attention-based models learn from transactional behavior, the event exemplified why cross-disciplinary, international discussions are vital.

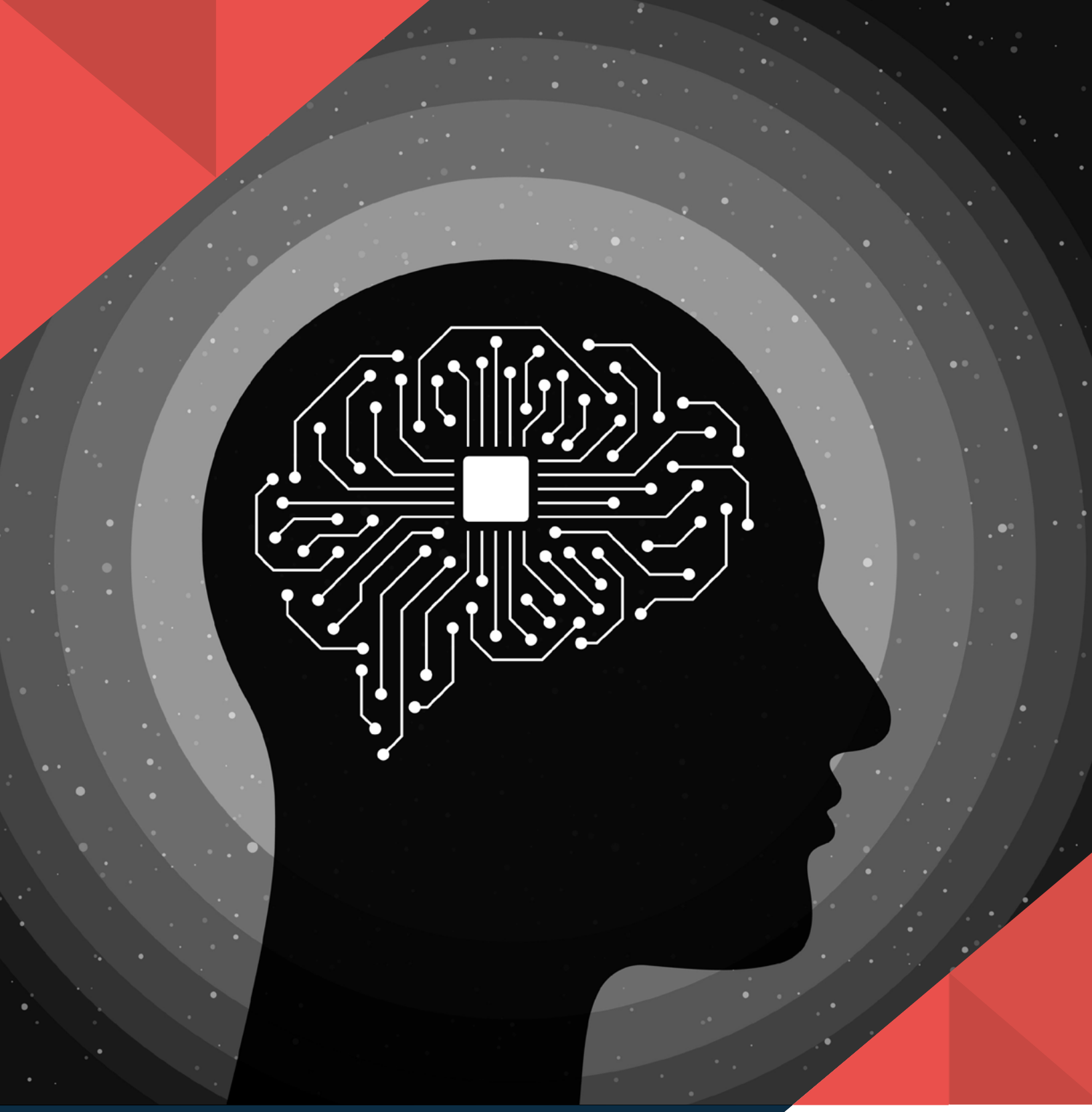
For model risk management professionals, the message is clear: systemic awareness and model intelligence are no longer separate domains. As banking becomes more interconnected and adversaries more sophisticated, the tools to monitor risk must evolve accordingly. Events like this offer a rare but necessary space to understand that evolution—and prepare for it.

author

Sara Ricci MBA CBCP CRISC CDPSE SCR

Sara Ricci is an internationally sought after speaker, mentor and C-suite advisor with proven expertise in Risk Management and Technology enablement in highly regulated financial and energy sectors, information technology services and retail. She specializes in global leadership of strategic initiatives in Enterprise Risk, Resilience, Operational Risk, IT Risk/Information Security, including Cybersecurity and Third Party Risk Management.

Her role as Global Head of Oversight and Control, Strategic Sourcing at JPMorgan Chase followed similar, wide ranging and impactful positions at Citi, Bank of America and UBS. Sara also leverages experience as Head of Information Risk Governance and Resilience at HBC and executive roles at HCL Technologies and New York Power Authority. She helped develop guidance for the financial and energy sectors, including maturity models in Resilience and Cybersecurity, whitepapers and benchmarking studies in Risk Appetite and Resilience.



INTELLIGENT RISK

knowledge for the PRMIA community

PRMIA
Professional Risk Managers'
International Association