INTELLIGENT RISK

knowledge for the PRMIA community

October 2019

PRMIA
Professional Risk Managers'
International Association

PROFESSIONAL RISK MANAGERS' INTERNATIONAL ASSOCIATION

SPECIAL THANKS

Thanks to our sponsors, the exclusive content of *Intelligent Risk* is freely distributed worldwide. If you would like more information about sponsorship opportunities contact sponsorship@prmia.org.

FIND US ON

prmia.org/irisk @prmia

INSIDE THIS ISSUE

editor introduction

Steve Lindo
Editor, PRMIA

Dr. **David** Veen
Editor, PRMIA

Nagaraja Kumar Deevi
Editor, PRMIA

The October 2019 issue of Intelligent Risk features articles addressing the topic Managing External Risks, which arise outside an organization and are beyond its influence or control such as macroeconomic shifts, regulatory change, cyber-attacks, natural and man-made disasters, and political and military conflict. Organizations cannot control the timing, location or severity of such risks, but they can implement alerts and contingency plans to mitigate their impact and recover from their occurrence. The articles submitted by PRMIA members for this issue cover a broad set of perspectives on this specific topic including: External Risks and the Challenge of Two Cultures, Managing Cybersecurity Risks in Corporations, A Case Study - Managing the Business Impact of Pandemics: The case of Ebola Virus Disease, Negative rates: Its Impact on the Economy and Banks, Risk – An alternative Approach, Single Counterparty Credit Limits (SCCL) – Overview – Challenges and Opportunities, Setting an Effective External Risk Management Program, Taming the "Known Unknowns", Key Challenges - Within the Transition from IBORs to RFRs and finally, Innovation to the Core.

We hope the PRMIA member community will find them interesting and enjoy reading the articles published in this issue as much as we did reviewing and editing them.

have you deployed Digital Financial Services (DFS) in your organization?

"What are the greatest challenges facing financial institutions today?"

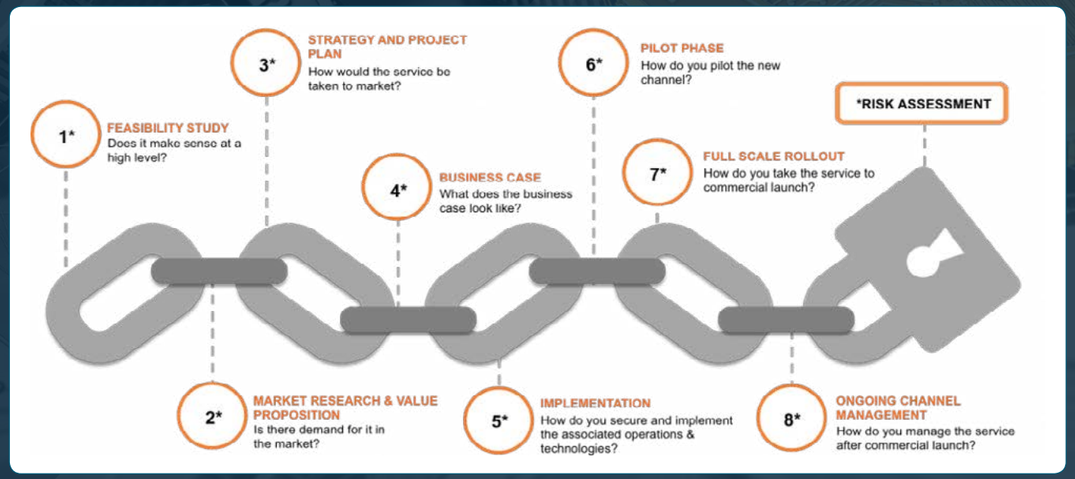
by **Faheem** Ali

Digital finance could give 1.6 billion people access to a financial account for the first time and turbocharge growth in developing countries. With the prospect of reaching billions of new customers, banks and nonbanks have begun to offer DFS for financially excluded and underserved populations, building on the approaches that have been used for years to improve access channels for those already served by banks and other financial institutions.

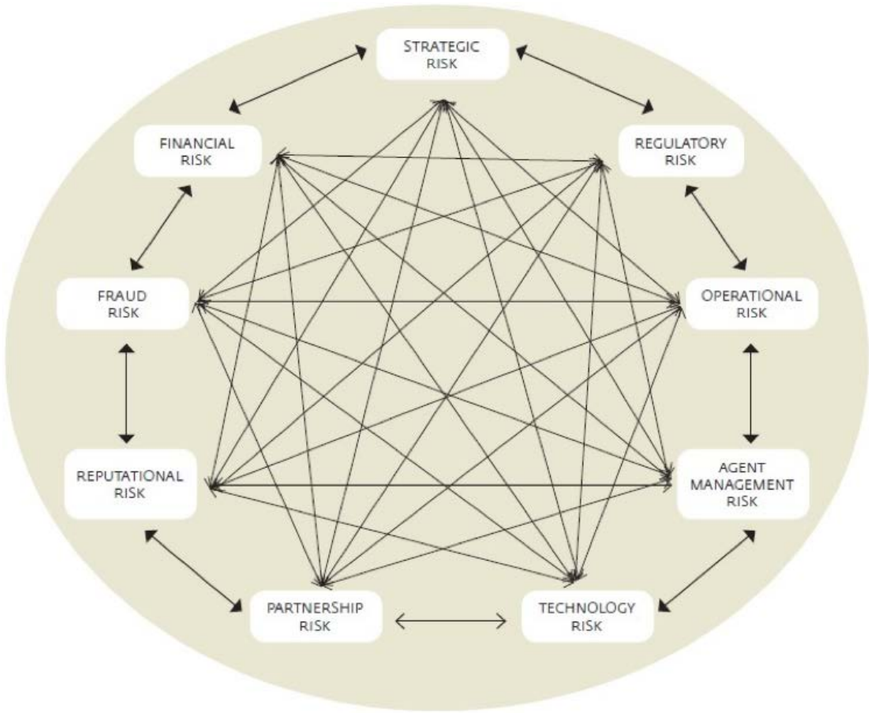
Policy and decision makers seeking to implement smart and proportionate financial regulation are urged to identify and assess the risk associated with these services. As with any innovation, there are bound to be unforeseen issues.

New types of products, new distribution models (i.e., agent networks) and channels (i.e., mobile phones), atypical providers (such as Mobile Network Operators, or MNOs) and customers with distinctive needs and circumstances (the poor) require innovative regulatory approaches and solutions.

Roll-out of new technologies and channels would be increasingly well-executed if management teams and boards understood the ins and outs of the business models.



Digital Financial Services (DFS) Risks:



The potential for DFS comes with inherent risks, as operations and client interactions are outsourced to agents who open accounts and conduct transactions on behalf of the provider. These include: strategic, regulatory, operational, technology, financial, reputational, partnership risks and many others.

strategic risk

"What are the greatest challenges facing financial institutions today?"

In the recent survey (MicroFinance Banana Skins 2016) conducted by CFSI (Centre for the Study of Financial Innovation) & Accion, the top rated/ biggest risk was "Strategy" (last time it was ranked at 6).

Strategic risk is broadly defined as the actual losses that result from the pursuit of an unsuccessful business plan or the potential losses resulting from missed opportunities. Some examples of this may be ineffective products, failure to respond to change in the business environment, or inadequate resource allocation.

Essential questions

- How well is my strategy actually defined?
- How broad are the risks that we are considering?
- Have we considered all internal and external factors?
- What risk scenarios have we considered to test our plans?
- Have we mapped our risks to key performance indicators and value measures?

regulatory risk

“Have I identified potential areas for risk of non-compliance?”

Regulatory risk refers to the risks associated with complying (or not complying) with regulatory guidelines and rules, such as anti-money laundering/combating financing of terrorism (AML/CFT), Know Your Customer (KYC), data privacy, account and transaction limits, trust accounts, and regulations regarding the use of agents. Regulatory risk also includes broader rules relating to the operation of a particular institution such as licensing, capital and liquidity.

Customer Due Diligence is one of the key areas which needs to be covered in DFS regulator.

Agent Management: The use of agents to act on behalf of financial institutions is strictly governed by regulators in most markets.

Essential questions

- Do I fully understand all the regulatory requirements and implications applicable to my institution, my agents, and my customers?
- Am I in full compliance with these regulations?
- Have I identified potential areas for risk of non-compliance?

operational risk

“Is there an operations manual that details all business processes?”

Operational risk is inherent in any business and refers to risks associated with products, business practices, damage to physical assets, as well as the execution, delivery and process management of the service.

This can include functions from every part of the business, such as: Sales operations, Customer service operations, Back office operations, Finance operations, Technical operations, Business Processes, Internal Control, etc.

Essential questions

- Is there an Operations Manual that details all business processes that is regularly reviewed and updated?
- Are critical business processes identified and relevant controls assessed?
- Is there adequate segregation of duties?
- Is there a daily reconciliation process between the bank and e-money accounts to minimize errors and detect fraud?

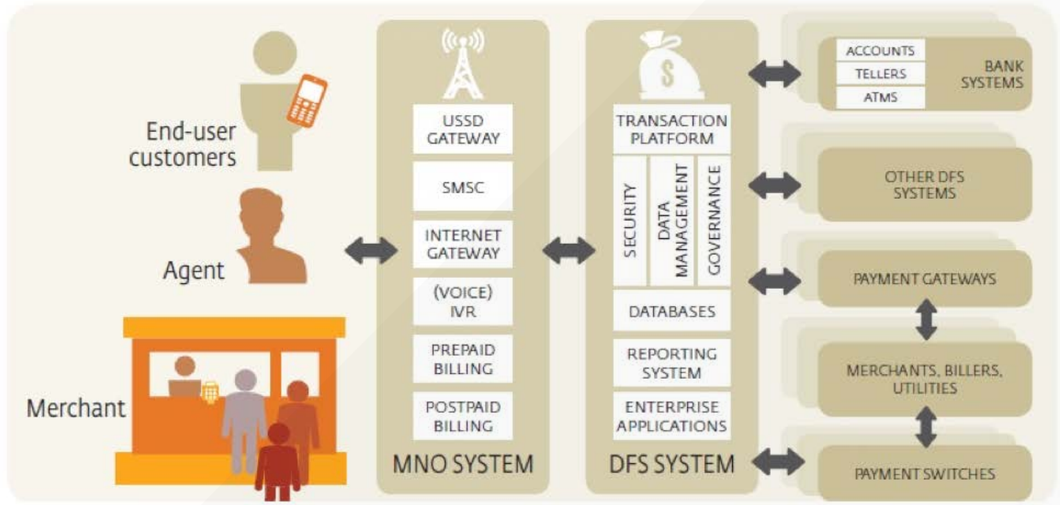
technology risk

“Am I able to measure the service level from an end-user perspective?”

Technology Risk refers to technology failure that leads to the inability to transact. It is closely linked to operational risk.

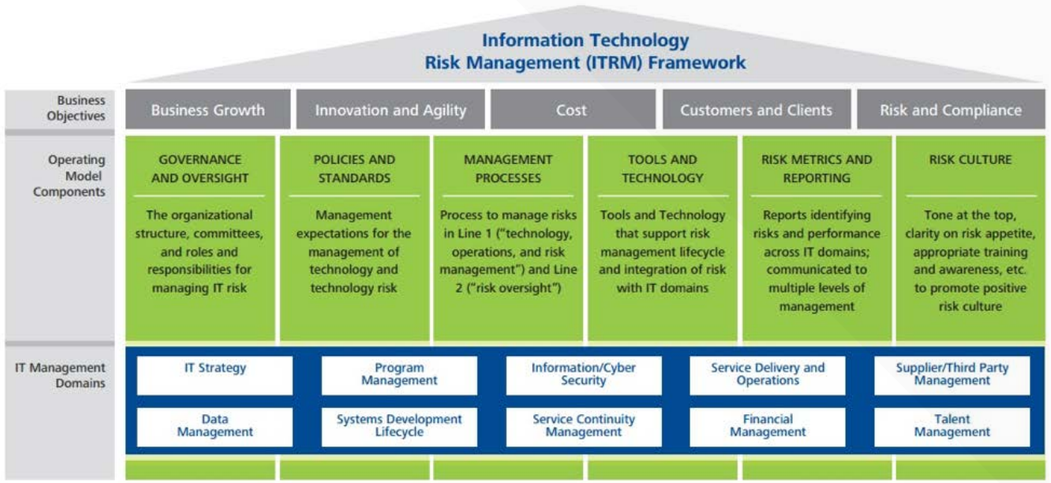
If technology failure is persistent and severe, the regulator may step in and impose penalties or revoke the license, or customers may abandon the service.

As DFS systems become more connected, the number of potential points of failure increases.



Essential questions

- Do I have Service Level Agreements (SLA) with my system provider to ensure software uptime?
- For which cyber scenarios do we have controls in place?
- Have we tested our Cyber Incident Response plan? Are we well-rehearsed?
- Is my software adequately communicating with devices to minimize transaction failures?
- Are third party providers and vendors effective and adequate in their security protocols and risk management approaches?
- Is access to corporate IT assets restricted and only granted based on an established role-based access framework?
- Do I have any mechanism in place to prevent loss or leakage of sensitive information (confidential information, intellectual property, personally identifiable information) from the organization?



financial risk

"Are my trust accounts adequately diversified?"

Financial risk is one of the most impactful risks related to DFS.

There are specific risks related to the financial management of a DFS provider as liquidity risk, credit risk, interest rate risk, foreign exchange risk, concentration risk etc.

Essential questions

- Do I have sufficient funding and cash to meet obligations and buffer for unexpected cash flows?
- Do I have credit risk policies in place, including credit risk assessments and KPIs for portfolio monitoring?
- Am I aging my portfolio at risk and creating loan loss reserves as per my regulatory requirements?
- Is my foreign currency hedged?
- Are internal back-office processes, reconciliations and controls adequately designed, verified and monitored regularly?

fraud risk

"Have we developed detective controls for fraud?"

There are many reasons why people commit fraud, but a common model to bring a number of these together is The Fraud Triangle. The premise is that fraud is likely to result from a combination of three general factors: Pressure (or motivation to commit fraud); Opportunity (typically because of poor systems or processes); and Rationalization (typically that they will not be caught).

The most common types of DFS – related fraud are summarized below:

Customer Fraud

CUSTOMERS DEFRAUDING AGENTS

- *Counterfeit currency: the risk that customers deposit counterfeit currency at an unknowing agent in exchange for electronic value, and then withdraw legitimate currency from another agent.*
- *Unauthorized access of agents' transaction tools: customers access agent POS devices to conduct fraudulent transactions.*
- *Fraud on agent web channel: Customers access agent web channel without authorization and conduct fraudulent transactions.*
- *Voucher fraud: fake vouchers are made to represent genuine vouchers from NGOs or government and given to agents in exchange for cash or electronic value.*

CUSTOMERS DEFRAUDING CUSTOMERS

- *Unauthorized PIN access: customers gain access to other customer's PIN numbers and conduct unauthorized transactions.*
- *Identity theft: customers use IDs of other customers to gain access to accounts.*
- *Phishing, SMS spoofing, fake SMS: fraudulent customers send fake SMS to agents either from their own handsets or generated from computers. The SMS looks genuine to the recipient.*

Agent Fraud

AGENTS DEFRAUDING CUSTOMERS

- *Unauthorized access to customer PINs: agents gain access to customer PIN numbers and conduct fraudulent transactions.*
- *Imposition of unauthorized customer charges: agents charge customers fees for transactions above and beyond the list price and fraudulently keep the fees instead of remitting to the provider.*
- *Split withdrawals: customers request a withdrawal from the agent, and the agent splits the withdrawal in two or more transactions in order to collect more cash out commissions from the customers.*

Other frauds can also be defined as Business Partner Driven Fraud (employees defrauding businesses), System Administration Fraud, Provider Fraud, Sales, Channel Staff Fraud, etc.

Essential questions

- Have you determined your level of acceptable financial losses due to fraud?
- Have you identified the key areas for potential fraud risk for your institution?
- Have you developed preventative and detective controls for fraud?
- Are you actively monitoring and reviewing your fraud risk management strategy?

author

Faheem Ali

Faheem Ali is an international speaker and has a strong management background in the Inclusive Finance and Banking domain with insightful understanding of the financial sector in various markets in Central Asia, Asia Pacific, and Africa.

Faheem has extensive experience in financial product development, digital financial product development and deployment, corporate and product marketing strategies formulation, transformation of MFIs, and credit operations. He has worked in different countries and provides training, consulting, and executive coaching services for inclusive financial service providers. Faheem has also conducted market research and numerous sessions/workshops in East African and Sub-Saharan countries, Central Asia, Asia Pacific, West Africa, and Gulf countries for financial institutions, mobile money operators, and non-financial providers including NGOs.

Faheem's other areas of interest include digital financial services, risk management, social performance management (SPM), capacity building, and youth inclusive financial services.

managing cybersecurity risks in corporations

by **Vivek** Seth

Cybersecurity incidents have made some of the biggest headlines in recent years across the world. Data breach incidents have been witnessed across corporate giants worldwide. For example, Facebook[1], Wetpac[2] as well as government institutions such as Bulgarian revenue agency[3]. Cyber-attacks can be motivated not only by financial gain but also for having access to sensitive company and customer information, which can be utilized for further attacks. Additionally, the perpetrators may intend to damage an institution's reputation and brand and weaken its customer confidence and trust.

In an age of increasing digitalization, all sectors of economy are exposed to cyber threats, and often cybercriminals are anonymous attackers hiding behind internet veils, located in a remote jurisdiction with weaker regulations. As cyber threats grow in scale and sophistication, it is not a question of "if", but rather "when" a cyber-attack will affect an organization. It is therefore crucial for corporations to have a robust cyber security framework to respond to and be prepared against a cyber-incident.

As cybercriminals adapt to new technologies and shift their tactics on attacking organizations' system vulnerabilities, corporations can keep a check on such potential attempts via putting the following in place:

Robust IT infrastructure

Timely investing in IT infrastructure (both in-house and outsourced) is crucial in protecting firms against cyber incidents like DDoS attacks, data sabotage, phishing attempts and ransomware attacks. This can be achieved by putting in place state-of-the-art network perimeter tools like firewalls, intrusion detection & prevention systems for internet facing systems as well as deploying up-to-date antivirus and antimalware tools across host and end point systems. Applying system security patches on a timely basis also plays an important role in addressing any new system vulnerabilities.

Policies, IT standards and cyber risk training

Even with the most secure IT systems, cyber incidents can materialize in absence of well documented IT policies and standards. It is crucial that key cyber security principles such as secure coding design in system development, cryptographic standards on protecting sensitive data, approved change management framework on system enhancements, etc. are well documented to avoid any miscommunication or human errors in system implementation. Documented procedures to address business risks also greatly enhances cyber security robustness. These include regular training across staff on cyber risks and emerging attack trends, cyber security crisis planning, and encouraging staff with privileged system access to undergo professional learnings.

Cyber security assessment

The cyber threat landscape is evolving, and cyber criminals' techniques are becoming increasingly sophisticated with the use of advanced technologies and data analytics. To counter such evolving threats, firms should periodically conduct vulnerability assessment to identify security vulnerabilities. Penetration testing can help a corporation obtain an in-depth evaluation of its cyber security defenses. Implementing cyber surveillance systems to check against any suspicious or malicious system activities and identifying correlation of multiple events plays a crucial role in protecting a firm against cyber threats.

Checks against emerging technology risks

As part of digital transformation, organizations should ensure that the key risks associated with innovative technical solution is well understood and adequate controls are in place. While adopting Cloud computing, tools to monitor and enforce checks against customer data and privacy misuse need to be deployed. Monitoring system logs for data security and service offering need to be in place in systems especially for third-party vendor tools. When personal mobile devices and personal end point systems are allowed in company networks, restricting inbound and outbound network traffic for smart devices and segregated network controls need to be in place for restricting smart device connectivity to confidential data.

Controls against insider threat

It is crucial for corporations to have adequate checks against cyber-attacks perpetrated by internal staff, as technology alone can't address such risks.

In an age where job retrenchments and reorganization are becoming standard work phenomenon and with the presence of newer technology such as small flash drive, smartphone etc., the risk of a disgruntled employee deliberately compromising the institution has become more probable than ever. Key controls include limiting and logging privileged IT access such as an administrative account to prevent any unauthorized access or misuse of such accounts. Implementing multi-factor authentication for online system or IT platforms that have access to confidential information via internet is another such key control. Periodic staff IT Access reviews to identify instances of privileged creep, access that are not aligned with need-to-know principle also prove helpful. Deploying Data Loss Prevention tools across company systems can greatly reduce the probability of internal data theft attempts.

Combating cyber threat is akin to guerrilla warfare, where hidden enemies operating behind the scenes are extraordinarily difficult to detect and may have allies inside the organization. While organizations cannot completely avoid materialization of such cyber incident's risks, they can implement timely detection, limit severity impact, and build upon contingency plans against cyber threats. To achieve this goal, an organization needs to timely invest in its IT infrastructure, build robust internal policies and IT standards, conduct period cyber threat assessments, and put effective controls against emerging technologies and internally perpetuated cyber-attacks. With such preparation, institutions would be well prepared in winning the battle over cybercriminals.

Sources

1. The Guardian, Sep 2018, "Facebook says nearly 50m users compromised in huge security breach" (link)
2. 7news.com.au, Aug 2019, "Hackers successfully breach tens of thousands of Australian banking accounts" (link)
3. Reuters, Jul 2019, "In systemic breach, hackers steal millions of Bulgarians' financial data" (link)

author

Vivek Seth

Vivek Seth is a Singapore citizen, working in the Risk Management discipline in Financial Industry for 15 years. His work experience spreads across Singapore, Dubai and Australia along with business assignments carried out in Hong Kong and Switzerland. He holds an M.B.A. and also the PRM™ professional certification. This article presented here represents author's personal views and not that of his current/previous employers or any professional bodies he is associated with.

managing the business impact of pandemics: the case of Ebola virus disease

by **Famien** Konan

First identified in 1976, Ebola Virus Disease (EVD) is a severe illness with a high death rate up to 90% caused by Ebola Virus. Although cases of Ebola have remained contained to Africa for nearly 40 years, the 2014 EVD outbreak has affected over 10 countries worldwide in three continents. It was the deadliest in history, having killed 11,316 people in the countries of Guinea, Liberia and Sierra Leone according to the Centers for Disease Control and Prevention (CDC). Aside from the major loss of lives, the Ebola epidemic severely impacted business operations by disrupting the supply chain and causing high absenteeism among the workforce.

Although it is impossible to predict when an Ebola outbreak will occur, appropriate planning is critical to minimize loss of life and productivity. Organizations need to assess their risk exposure to Ebola, then develop and execute a solid business continuity plan to manage the financial impacts and meet their legal obligations to their employees.

understanding the threats and consequences of Ebola

Organizations with operations in an area affected by Ebola are exposed to:

- Personnel risk which arises from the potential of employee to be sickened, evacuated or die after the virus infection
- Financial risk due to interruption of normal business operations leading to a loss of revenue

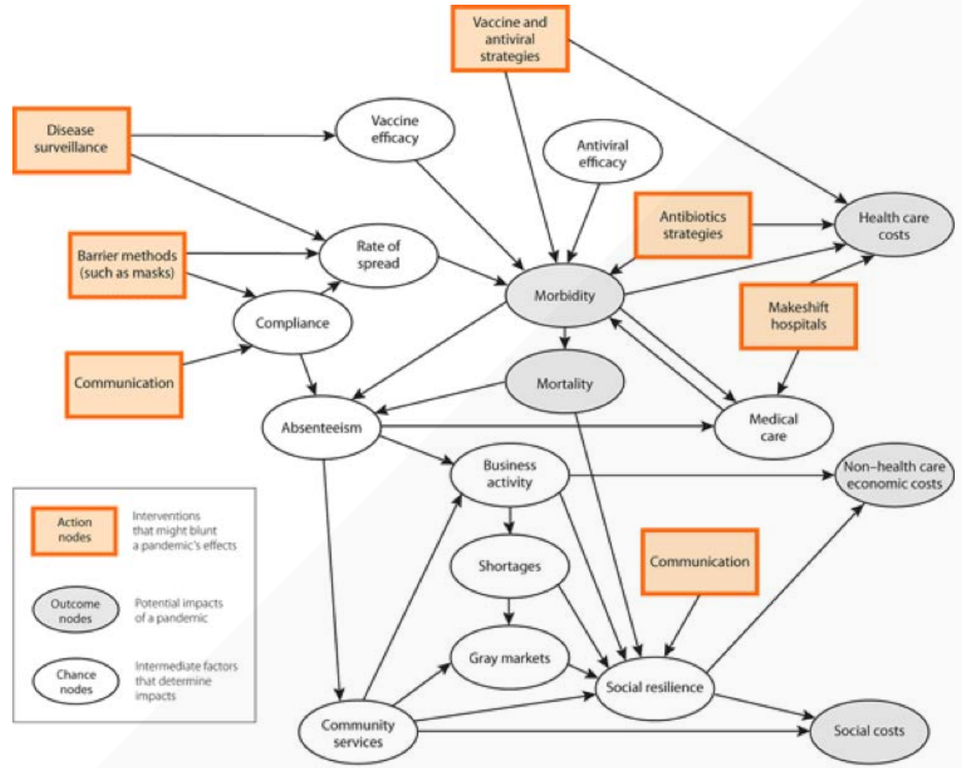
By recognizing and understanding these two aspects of risk when facing a pandemic, organizations can effectively assess their vulnerabilities and exposures to EVD.

Many organizations in West Africa monitored the early stage of the Ebola outbreak carefully to understand the transmission mechanisms of the virus and assessed adequateness of healthcare facilities and sanitation services in the region. One possibility for how this could be done is to develop an EVD risk-scoring framework that predicts the outbreak risks for a country in terms of morbidity and mortality, based on socioeconomic, environmental, geographical, cultural, and health systems-related risk factors. An application of this approach by researchers from the University of New South Wales in Sydney assigned the highest scores to the three worst affected West African countries (Guinea, Sierra Leone, and Liberia), and demonstrated the utility of a risk-scoring framework for pandemic planning.

The risk assessment must also focus on how the outbreak affects the business operations. In this context, scenario planning is an important tool for anticipating possible future developments of a pandemic. It allows planners to evaluate assumptions and reflect the consequences of real-world disaster scenarios on business plans and operations. Risks scenarios can be developed from the 2014 outbreak features in Ebola-affected countries, like those recommended by the US department of Homeland Security for pandemic influenza. A worsening scenario could assume, for example, a disaster of national significance over 18 months, high disruption of basic infrastructure (telecommunications, transportation and road systems), difficulty for local health systems to trace and isolate infected individuals, and a low level of cooperation with international agencies.

Finally, organizations can use an influence diagram to evaluate the relationships between the two aspects of EVD risk. Analyzing risks in all aspects provide organizations the capability to align the EVD business continuity planning with their specific risk profile.

Figure 1: Making an influence diagram for a pandemic



Source: Preparing for a pandemic, HBR May 2006 issue

business continuity planning

An effective business preparedness and response program for EVD requires a specific focus on the 4 steps of the PPRR model (Prevention, Preparedness, Response and Recovery). These steps should be geared to the 6 phases of the World Health Organization (WHO) pandemic tracking model as illustrated in figure 2.

As with any pandemic planning process, lessons learned from the 2014 West Africa Ebola outbreak show that organizations need to:

- Stay informed on developments and announcements made by key health organizations (WHO, CDC)
- Identify critical business processes, alternative production sites and supply chain partners / sites to be used to reduce the impact on revenues
- Identify staffing arrangements, such as telecommuting, back-up personnel, and technology facilities
- Protect the health and safety of staff, and provide training on their ability to conduct business during a sustained outbreak
- Identify contingency plans for the interruption of essential services such as electricity, water, telecommunications, transportation and security
- Develop a communications strategy for employees, shareholders, suppliers, customers and communities
- Review health insurance and travel accident policies, and travel restrictions to and from countries at risk

Figure 2: Pandemic planning model for EVD

Phase	Description	Main actions
Interpandemic phase New virus in animals, No human cases	Low risk of human cases	**Risk Analysis** • Identify the specific risk profile of core business operations in the context of EVD • Align internal planning and preparedness with relative risk
	Higher risk of human cases	
	No or very limited human-to-human transmission	**Prevention & Mitigation** • Identify venue or business-specific risk controls • Develop proactive risk communication tools
Pandemic alert New virus causes human cases	Evidence of increased human-to-human transmission	**Preparation** • Appoint a crisis management team • Review business continuity considerations
Pandemic	Evidence of significant human-to-human transmission	**Response** • Activate contingency plans
	Efficient and sustained human-to-human transmission	
Post peak period	Possibility of recurrent events	
Post Pandemic	Disease activity at low levels	**Recovery** • Devolve crisis team and resume steady-state operations • Conduct After-Action Review and apply lessons learned • Continue proactive risk communications to manage messages

Sources: World Health Organization; US Travel Association

Organizations should also consider developing joint responses with other members of the community, even competitors. An example of cooperation in the case of EVD is the Ebola Private Sector Mobilization Group (EPSMG), a coalition of more than 48 companies operating in West Africa, established in July 2014 to facilitate a mobilized and coordinated private sector response to the Ebola virus. The contribution of the EPSMG during the response phase helped to protect people, assets and continued operations of members of the group. The EPSMG also played a significant role during the recovery phase, as a hub to share lessons learned about the outbreak, and its members contributed to the private sector recovery in the affected countries.

Most companies that kept business running post-Ebola in affected countries have been those who achieved rigorous risk-planning, and jointly contributed to develop stronger healthcare and safety systems. EVD, as any other pandemic is, by definition, a global risk event. Addressing pandemic risk is different from traditional business continuity threats, as the event could remain up to several months. The 2014 Ebola outbreak in West Africa reminded organizations that risk management processes for pandemics should not look only at preserving business operations but should also consider the health and safety of the workforce.

references

1. Ajisegiri, W. S., Chughtai, A. A. and MacIntyre, C. R. (2018), A Risk Analysis Approach to Prioritizing Epidemics: Ebola Virus Disease in West Africa as a Case Study. Risk Analysis, 38: 429-441.
2. https://hbr.org/2006/05/preparing-for-a-pandemic
3. https://www.cdc.gov/vhf/ebola/pdf/cost-ebola-multipage-infographic.pdf
4. https://www.otia.info/docs/10.29.14EVDPlanningCrisisManagementGuideforUS_TravelMembersFINAL.pdf
5. https://www.bitc.org.uk/print/resources-training/impact-stories/arcelormittal-ebola-private-sector-mobilisation-group-epsmg
6. https://corporate.arcelormittal.com/news-and-media/news/2016/april/18-04-2016
7. https://www.business.qld.gov.au/running-business/protecting-business/disaster-resilience/pandemic-risk-management
8. https://www-cdn.oxfam.org/s3fs-public/file_attachments/ebola_and_the_private_sector_-_bolstering_the_response_and_west_african_economies.pdf
9. https://www.who.int/csr/disease/swineflu/phase/en/
10. https://www.bitc.org.uk/print/resources-training/impact-stories/arcelormittal-ebola-private-sector-mobilisation-group-epsmg
11. https://www.foreign.senate.gov/imo/media/doc/040716_Knight_Testimony.pdf

author

Famien Konan

Famien Konan is a Principal Treasury Risk Officer at the African Development Bank with 11 years of experience in the financial services industry. Prior to joining AfDB, he worked at EIB and CNP Assurances in quantitative finance roles. Mr. Konan began his career as a financial software consultant on the credit derivatives markets. He holds a master's degree in telecommunications engineering from IMT Atlantique (Telecom Bretagne), as well as a mathematical degree from Université de Bretagne-Occidentale. He is a PRM holder since 2010.

risk – an alternative approach

by **Andrea** Luzzi

What is risk? Hard to say. Under Modern Portfolio Theory (MPT), pioneered by Harry Markowitz, risk is identified with volatility. Variance and correlation are the main statistical measures to assess the level of peril of a portfolio.

The European Securities and Markets Authority (ESMA) designed the risk framework for UCITS funds on those assumptions: Value at Risk, PRIIP (Package Retail and Insurance-based Investment Products) regulation and SRI (Summary Risk Indicator) in particular are all grounded on the principle that volatility is a synonym of risk. The new SRI is unhurriedly making a step up with the introduction of a Credit Risk Measure and a Cornish-Fisher expansion. It is undoubtedly a progress in the right direction.

When you manage a portfolio of hedge funds you realize that the traditional framework of modern portfolio theory is neither modern, as it likes to be called, nor satisfactory.

Volatility is symmetric: under certain conditions, the deviations from the mean not only measure the predictable size and likelihood of potential losses, but they may identify opportunities too. Upside volatility, especially in active management, is a blessed bounty that is hard to classify as pure risk.

As an example, suppose we may choose between two bets which are based on the results of one hundred flips of a coin: in the first bet, you can earn $100 if you get one head, but then you lose $1 if you get one tail. In a second bet, you earn $10 for one head and lose $10 if you get one tail.

It is obviously not wise to take the second bet. However, according to MPT and UCITS regulation, the first choice is 5 times riskier.

This counterintuitive result is not the only pitfall.

From an allocator's perspective, a fund with an annualized return of 10% and a volatility of 10% is certainly preferable to a fund that delivers the same Sharpe Ratio with half of the volatility. It allows the asset manager to put less cash at work for a similar result. Once again, volatility represents more of an opportunity than an additional threat.

If volatility is an inaccurate definition of risk, correlation is not any better. Symmetry is once again an annoying feature. Who does not want to be correlated to the stock markets during the bull rally of the first half of 2019? Hard to define that common trend as "risky". Downside correlation may give a better indication of the risk underneath, but it misleads analysts by scaling the co-movements with the product of volatilities.

As fund managers, we had to make a decision: should we stay with the orthodox doctrine, or should we go?

We found our own heresy developing a new risk measure: The Downside Capture Ratio. Like Columbus' egg, the idea is pretty straightforward. We abandoned descriptive statistical measures and we concentrated on the only information that we want to extract from data: "How much money do I lose if…?"

The only ex-ante question that really matters for asset allocation.

We implemented the following Bayesian measure:

$DCR=\sum R_a/\sum R_i$ where R_i is defined as the negative performance of an index and R_a is the performance of a certain asset at the same point in time.

The end result is the ratio of the index loss which is embedded in the asset performance. A negative outcome shows a tendency of the asset to make money when the index (benchmark) marks a loss.

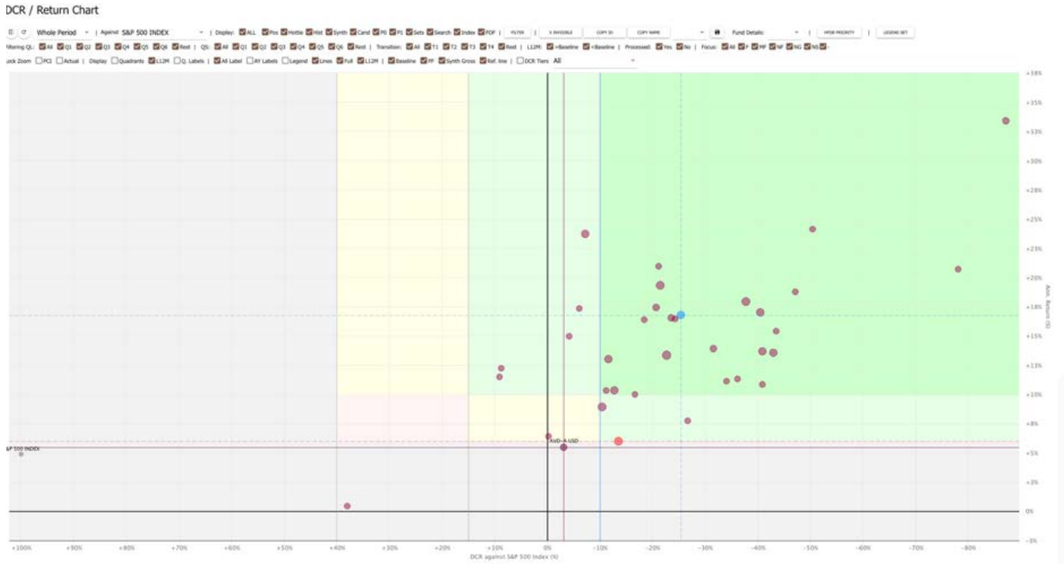
Once extended to a sufficiently large number of indices, the Downside Capture Ratio (DCR) identifies the sensitivity of an asset to various stressed events, not only confined to equity. It may also become a valid alternative to historical stress tests.

The simplicity of the computation has many advantages, and one of them is certainly the ability of comparing different types of risk, extracting information from asset track records.

A visual comparison helps more than a thousand words.

In the chart below, funds are plotted with DCR on the x-axis and annualized performance on the y-axis. The top-right quadrant contains funds which show an exceptional feature: they make money when one or more indices sell off. Beware, we are not talking of Pearson of Spearman correlations: a negative correlation with the S&P 500, for instance, does not mean automatically that an asset is likely to grow in price during a drawdown.

On the contrary, a negative DCR has exactly that meaning, and it gives substantial more information to investors.



We have adopted DCR in our analyses in combination with traditional risk measures, and we found the unorthodox approach much more effective in managing a portfolio of financial assets.

author

Andrea Luzzi

CEO, Ayaltis AG

Andrea started his financial career in 2001 working in the Risk Management department of large asset managers. In 2006 he switched to the hedge fund industry working for Mangart, one of the biggest European global macro funds, in charge of Risk Management and Operations. In 2009 he joined OneInvestments, manager of the long/short equity fund Antares and in the same year, he founded Quantyx, a service provider of external risk management.

Andrea has a Master's degree in Economics, a Master in Quantitative Finance from the Bocconi University in Milan and he is a PRM and a CAIA charter holder.

Single Counterparty Credit Limit (SCCL Rule) rule overview and resulting challenges & opportunities

by **Shamoun** Afram

SCCL rule – overview

In June 2018, the Federal Reserve Board adopted regulations to implement SCCL mandated by the Dodd-Frank Wall Street Reform and Consumer Protection Act. The rule's intent is to limit "net credit exposures" of a covered firm to a single counterparty to a specified percentage of the firm's eligible capital base. Unlike bank-level lending limits, which focus solely on a bank's exposures, SCCL limits the exposures of the entire consolidated institution to its counterparties. The link between large banking organizations and their counterparties is a concern SCCL aims to address which in turn helps reduce the threat to financial stability at times of stress.

SCCL applies to the two categories of US banks: Major covered companies – i.e. GSIBs (Globally Systemically Important Banks), and Non-major covered companies – i.e. non-GSIBs. SCCL also applies to major Foreign Banking Organizations (FBOs) and Intermediate Holding Companies (IHCs) as well as non-major FBOs and IHCs. This translates to 10+ US banks and 75+ FBOs. SCCL takes effect for major banks Jan 2020, while non-major banks have 6 additional months. Although implementing SCCL can be costly, the industry should benefit from having consistent exposure reporting per counterparty across banking organizations.

SCCL allows for what is called "rule equivalency" for covered FBO. Accordingly, a Covered Foreign Entity does not need to comply with SCCL's limits on the aggregate net credit exposure of combined U.S. operations if the FBO certifies on behalf of its combined U.S. operations to the FRB that it meets large exposure standards on a consolidated basis established by its home-country supervisor that are consistent with the large exposures framework published by the Basel Committee on Banking Supervision. In June 2019, CRR2 (Capital Requirements Regulation) under Basel III was published inclusive of revised large exposure rules/ guidelines which mainly take effect for European banks June 2021. The misalignment of effective dates between the FRB, the European regulators and other regulators have caused uncertainty among the impacted banks.

Under SCCL, net exposure is calculated across a group of counterparties where their financial statements are consolidated for financial reporting purposes. Net exposure is measured against the bank's tier 1 capital. Once net exposure exceeds 5% of tier 1 capital, additional counterparties are required to be grouped based on economic interdependence and control relationships. The additional control and economic tests are in line with other existing regulations such as the FRB's Regulation K and the EBA's Connected Counterparties regulation.

The SCCL Rule requires continuous compliance through daily monitoring and quarterly reporting. The proposed form FR 2590 requires granular information on the covered company/foreign entity's exposures to its 50 largest counterparties. Schedules are required to be provided to the FRB 40 to 45 days after each quarter end. The covered company/foreign entity's Chief Financial Officer is requested to attest to the company's compliance to the SCCL rule. "Daily compliance" is required under SCCL, but there is no prescribed daily reporting format. In theory, and based on the rule, the FRB can request a covered bank to demonstrate compliance by the rule for any particular business day of the year. The method of demonstrating daily compliance can vary vastly per bank and has been a source of debate in the industry on how to effectively but efficiently address.

SCCL rule – challenges/opportunities

Banks are likely to encounter challenges across one or many dimensions when implementing SCCL. The first dimension being whether the bank is US based, an FBO with an IHC, or an FBO without an IHC. Here are 3 challenges chosen as example based on first-hand experience of implementing the rule.

Calculating exposures for derivatives and secured financing transactions (SFTs) under SCCL

- SCCL allows exposure for derivatives and SFTs to be calculated using a bank's internal methodology if already approved by the FRB. If not approved by the FRB (which is the case for most – if not all- non-IHC FBOs) the exposure should be calculated using the "Exposure At Default" formula per the US BIII standard approach.
- This creates the challenge of implementing a regulatory exposure calculation that may not be aligned with the management's view of exposure for the same product set
- This in turn creates the opportunity to have an aligned exposure calculation for regulatory and management reporting purposes. Or at least creates the opportunity to streamlining multiple calculations off of the same data set and engine.

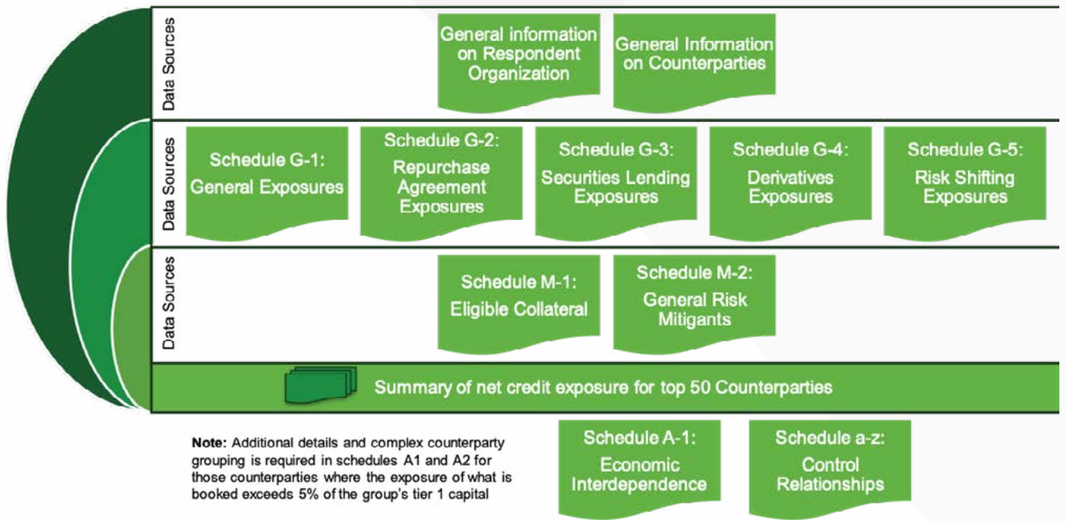
Treatment of master netting agreements and collateral agreements

- Treatment of trades (mainly derivatives and SFTs) that fall under "master netting agreements" and collateral agreements (e.g. CSAs) which have a scope larger than the booking entities that fall under the scope of SCCL reporting. (This is a common issue for IHCs and/or FBOs).
- This creates the challenge of having to decide on what to account for when applying trade netting which may not align with the legal agreement. Same applies for how collateral is used to reduce exposure when collateral covers trades in booking entities that are broader than the scope of SCCL reporting.
- This creates the opportunity to standardize how such scenarios are treated when exposure is calculated for a counterparty based on trades booked in booking entities that fall under a specific jurisdiction.

Solutioning for and ownership of quarterly reporting vs. daily compliance

- In short, SCCL challenges us in rethinking the lines that have been drawn between risk and finance on who owns what and for what reason.
- As a result, SCCL creates the opportunity to streamline certain reporting and monitoring functions which in turn can result in higher efficiency and lower cost.

This article by no means provides a comprehensive view of the SCCL rule, its challenges and opportunities. But it touches upon the main aspects of the rule providing relevant examples. In closing, this diagram illustrates the quarterly reporting schedules as per FR 2590. Schedules continue to be in DRAFT form as of Oct 2019. The FRB is expected to issue the final version anytime now.



references

1. https://www.federalregister.gov/documents/2018/08/06/2018-16133/single-counterparty-credit-limits-for-bank-holding-companies-and-foreign-banking-organizations
2. Single-Counterparty Credit Limits Reporting Form - https://www.federalreserve.gov/reportforms/formsreview/FR2590_20180620_i_draft.pdf
3. https://www.davispolk.com/files/2016-03-22_Single_Counterparty_Credit_Limits_Proposed_Rule.pdf

author

Shamoun Afram

Shamoun is a global Finance and Risk Transformation/Change Executive with proven track record of managing large-scale transformation and regulatory programs in Finance/ Treasury/Risk functions of Investment Bank and Wealth Management organizations.

Shamoun began his career in management consulting responsible for programs with large-scale system design, development, testing, and implementation. He delivered benefits as the global lead for a liquidity risk program at a foreign bank. He implemented BCBS239 principles in the liquidity space for the US operations of a foreign bank.

Currently, he is leading a team that defined and is in the process of delivering the optimal solution for addressing the FRB's "Single Counterparty Credit Limit" reporting capability at the US operations of a foreign bank.

pillar 2 liquidity risk management

by **Moorad** Choudhry

Banks have been managing liquidity risk in line with the Basel III liquidity coverage ratio (LCR) for some years now. The requirement to address the concept of "Pillar 2 liquidity" is more recent, with regulators worldwide pronouncing on this subject in the years following the crash. The publication of the United Kingdom Prudential Regulation Authority (PRA) Policy Statement 13/19 earlier this year affords a good opportunity for banks to finalize their approach to meeting the needs of Pillar 2 liquidity, and to ensure that their risk management framework in this space represents best practice. This article distils some key messages concerning Pillar 2 liquidity and what it means for the minimum size of a bank's high-quality liquid assets buffer (HQLA).

pillar 2 liquidity framework

The basic premise of "Pillar 2" liquidity is the requirement for banks to consider liquidity risk exposures beyond those described under the LCR ("Pillar 1"), and which are deemed not covered by LCR. In the UK the subject was described in a PRA Statement of Policy (SoP) Pillar 2 Liquidity, and updated in PS13/19. Its aim is to ensure that firms retain sufficient available liquidity to cover risks that are not covered or only partially covered by the LCR.

These additional risks include the following:

- Franchise viability risks (such as debt buyback: a non-contractual request by debt holders to buy back issued debt);
- Intraday liquidity risk;
- Funding risks, including "cliff" risk (risk that outflows beyond the 30-day LCR horizon exceed inflows);
- Cash flow mismatch risk (the risk generated by using a "point-in-time" approach in the LCR against the maximum net cumulative outflow);
- Liquid asset management risk, generated potentially by widening the definition of "liquid assets" to include assets that in reality cannot be monetized as quickly as cash;
- Funding concentration risks, arising from over-reliance on a single or restricted sources of funding;
- Inadequate systems and controls for managing liquidity risk;

- Inadequate systems and controls for managing liquidity risk;
- Risks relating to derivative outflows not included under the LCR standard;
- Risks relating to securities financing margin requirements;
- Risks relating to intragroup flows.

In practice Pillar 2 means that most banks will have a liquidity risk mitigation add-on, most commonly in the form of a higher minimum HQLA requirement than that given by LCR.

enhanced monitoring framework

A close reading of the text in PRA CP6/19 and PS13/19 provides a template for the enhanced liquidity risk monitoring framework that banks will be implementing. The key point about Pillar 2 liquidity is the emphasis on stress testing over a 90-day minimum period as opposed to a 30-day one. Other notable pointers include:

Paragraph 3.7: the PRA will set guidance or monitor the stress scenario or stress tools at consolidated and/or single currency level using the granular LCR scenario. This confirms that this does not preclude use of additional stress scenarios or tools to set guidance, for example in temporary and targeted ways; it also implies emphasis on firm-specific stress tests;

Paragraph 3.13: the PRA will monitor over a 90-day horizon retail-only and wholesale-only stress scenarios. This extends the respective LCR inflow and outflow rates to contractual flows scheduled between 31-90 days;

Paragraph 3.16: Retail-only and wholesale-only stress scenarios are considered separately and jointly as a combined stress scenario. Available liquidity derived from the firm's HQLA as described within days 1 to 90 will be used to complete the calculation of net liquidity profiles under the benchmark scenarios;

Paragraphs 3.21, 3.22: the PRA assesses vulnerability to an acute retail run (90-day horizon) at levels informed by certain severe stress episodes observed during the financial crisis. It assesses reliance on wholesale markets and their vulnerability to a market shutdown through an enhanced wholesale stress. (Note that this assumes complete closure of unsecured wholesale markets for 90 days. Hence a "market lockout" stress test is virtually compulsory. Note also that seeking to raise funds from this market cannot therefore be a "management action" in the firm's liquidity adequacy assessment (ILAAP) for days 1-90 of the stress).

The exhibit below, an extract from PS13/19, summarizes the basic approach.

Stress scenarios and stress tools			Consolidated currency		Single currency	
			Monitoring only	Setting guidance	Monitoring only	Setting guidance
Stress scenario	Granular LCR		✔	✔	✔	
	Benchmark	Retail	✔		✔	
		Wholesale	✔			
Stress tool	Enhanced Retail		✔			
	Enhanced Wholesale		✔		✔	

The PRA will use the output from the benchmark stress analysis to calculate survival period

Pillar 2 liquidity framework

impact on HQLA and overall liquidity adequacy rule (OLAR)

The requirements of Pillar 2 liquidity make it incumbent upon banks to assess liquidity risk exposure beyond the 30-day horizon of the LCR and ensure that their risk management framework is compliant. The questions for a bank's asset-liability committee (ALCO) to address therefore include:

- What is the bank's appetite for liquidity and funding risk?
- How does this translate into a "Survival Days" horizon under foreseeable firm-specific stresses?
- Where should one set the minimum level for number of survival days in a stress?

A bank's formal risk appetite statement (RAS) will inform the impact of the stress test output, as the overall liquidity adequacy driver (OLAR) is driven partly by the bank's appetite for how long it wishes to remain survivable in a specified stress scenario. Regulators focus on the OLAR, which in practice is a function of the bank's RAS as well as informed by the worst-case ILAAP stress scenario, to determine how much HQLA the bank should have, and also what this amount implies for the number of days the bank is survivable as a going concern in a stress environment.

Implementing a 90-day "monitoring" horizon suggests that banks should adopt a "Stressed Liquidity Ratio" (SLR) as an internal metric in their RAS, this being calculated over a 90-day horizon compared to the 30-day LCR. The calculation is identical, but is simply over a 90-day period (or alternatively, over the time horizon of the bank's choice that aligns with its RAS).

$$SLR(\%) = \frac{HQLA}{\sum(Liquidity\ Outflows - Liquidity\ Inflows)}$$

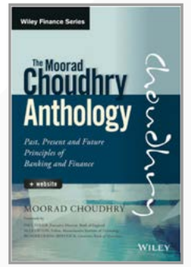
conclusion

Pillar 2 liquidity is understood as addressing liquidity risk exposure that is not addressed by Pillar 1 (LCR). But its application, analogous with capital adequacy, is not uniform across banks in the way Pillar 1 is. The bank's own Board-approved risk appetite will inform the answer to the question, *For how long does the bank wish to be standalone survivable during a liquidity stress event?* The answer to this will in turn inform the minimum floor for its HQLA.

author

Moorad Choudhry

Professor Moorad Choudhry is a Non-Executive Director on the board of Recognise Financial Services Ltd. He is author of The Principles of Banking (John Wiley & Sons 2012). Pillar 2 liquidity is discussed in the author's book The Moorad Choudhry Anthology, published by John Wiley & Sons Ltd (2018).



innovating to the core - how organizations must create an A.C.T.I.O.N plan

by **Nagaraja** Kumar Deevi & **Eric** Lui

Innovating to the Core is a concept which holds that organizations, whether great or small, must possess a transformational belief of change at their very core – strategy, mission, values, organizational capabilities, etc. Disruptive change in recent years has exploded through digitization, customer experience, emergent technology, and social impact. Companies and even entire industries are being turned upside down and those who are not willing to adapt or foresee the trends are being left behind, like Kodak, Sears and Blockbuster. We are at a juncture where traditional industries do not exist in silos within their strategic groups any longer. Companies and organizations now have the ability to cross sectors, industries and challenge incumbents in various ways. We now see large technology companies like Apple and Amazon in the United States, and Tencent and Alibaba in China, using their competitive advantages to disrupt multiple industries. At the other end of the spectrum, smaller, innovative startups such as those in the Financial Services (Fintech, RegTech, InsureTech) space are disrupting pockets of the supply chain in Wealth Management and Insurance. So, how do organizations prepare themselves and not succumb to the same fate as those companies who failed to "Innovate to the Core"? We examined a host of companies in various industries and formulated the core areas to succeed in innovating to the core - A.C.T.I.O.N.

A - adaptive

Organizations must be able to follow trends and not only foresee, but quickly adapt to, the changing landscapes of their industries. Companies should have dedicated research or competitive intelligence teams structured around trends not only from their own strategic groups, but outside, divergent industries as well, in order to adapt to change. This can only happen where organizations are structured in a way that is flexible, agile, unstructured and barrier-free, in order to be able to seize the moment and shift if necessary.

C – collaborative culture

The culture of a firm consists of the core beliefs, purpose, values and ideas shaping how its employees operate, interact, communicate, and work. It can be built and nurtured through time. It can also only be transformed through an environment that is open and collaborative. Companies must institute what we call "collaborative culture" - a culture which fosters an environment where ideas, problems and interactions can take place, in order to share, resolve and innovate. The idea of "Innovation hours" is tied to how a company's organizational structure needs to embed Innovation as a core key performance indicator, alongside day to day responsibilities. We have seen a company like Google which encourages its employees to dedicate 20% of their time to side projects, in order to help Google innovate. This type of structure allows their employees to innovate freely using their creativity and not be impeded by their core day to day duties.

T – tone from the top

Incorporating innovation hours

- Every employee in the organization must devote a few hours of their time to THINK, INNOVATE in a day/week/month/year
- Management and Senior Leaders must allow all employees to count innovation hours toward their billable targeted hours of time, in order to develop their ideas outside of their regular work, and align this practice within the organization's overall strategy. Encouraged to submit ideas in a firmwide centralized knowledge base, tied back to employee performance (innovation KPI)
- A Chief Knowledge Officer must be identified and nominated

I – inclusive innovation

In today's paradigm, we take for granted that innovation has to be for all and not just for the privileged few. Innovation should also be inclusive through the use of feedback, and not only for the purpose of making things easier, but also to solve problems of the greater good. Innovation should be both inclusive and diverse. Innovation comes from the diversity of the workplace, where previous challenges, experiences and ideas are brought to the forefront of discussions and problem-solving. A more diverse organization can generate inclusive innovations in areas such as gender equality, financial inclusion and poverty, overlooked segments in industry, equal opportunities, etc. This may mean opening up with new opportunities, customer bases and revenue streams. For example, Fintechs in the financial services space have emerged to cater to neglected customer segments such as those in the unbanked and underbanked (such as those in the least developed countries, the gig economy, etc.). According to the World Bank and their 2020 goal for Universal Financial Access, there are still 2 billion people in the world that are currently "unbanked".

Financial inclusion creates businesses opportunities and can have a societal impact contributing to income spikes, food, access to social services, etc. In the technology space, Microsoft is instituting “inclusive design” in their products to make software applications and hardware easier for disabilities and a more diverse population. The objective is to learn from various angles and look at uses of their products from different perspectives, so they can build better products which recognize that we are all after all – human.

O – organizational capabilities & training

An organization’s capabilities – its abilities and competitive advantages (resources, talent, customer base, geography, etc.) are vital to its success. For organizations embarking on an innovation journey, this may mean innovating by using the capabilities they currently have, or formulating a strategy based on these strengths and weaknesses. Management direction in setting a strategy for these capabilities and aligning these agendas to performance and skill building can help organizations succeed. A recent study by IBM (September 2019) discussed the trends of the future of work and how robotics and intelligent automation will displace 120 million workers in the next three years who will need to be upskilled and retrained. Leadership must integrate training into performance measures, so organizations can prepare this talent shift bridging humans and emergent technology.

N – next generation technologies

Innovation and technology are in a way synonymous but also symbiotic. Without one you cannot lead to another and vice versa. Organizations must embrace new technologies into their everyday processes and longer term strategies. Emergent technologies such as Blockchain and Quantum Computing are closer to solving certain cases but require investments in resources, technology, people and time. Some firms are reluctant to be pioneers in these emergent technologies simply because they cannot either afford to or venture into new ways without such capabilities.

conclusion

Innovating to the core requires a combination not only of people and technology but also a culture that is willing to accept, upskill and obtain these types of know-how as part of their everyday environment. We have seen organizations implement with great success a combination of these bets to improve on both existing processes to solve rather big problems with small investments and also to have “skin in the game” with larger initiatives in order to keep up with innovation trends. There is no one-size-fits-all or an “all-in” strategy.

authors

Nagaraja Kumar Deevi

Nagaraja Kumar Deevi is a senior strategic executive with over two decades of Leadership experience in Finance, Risk, Regulatory, Digital, Analytics and Technology enabled solutions advising Global Banking & Financial Institutions. He is currently Managing Partner & Senior Advisor at DEEVI Advisory & Research Studies. NAG is specialized in Digital Transformation, Banking regulations, Regulatory Policy & Affairs and Enterprise wide Strategic Risk initiatives. Designed and developed Enterprise Risk Governance Framework aligned with firm-wide Corporate strategy, setting high level Regulatory Policy, Risk Appetite Statement, Recovery, and Resolution Planning (RRP)/Living Wills, Culture, Conduct & Reputational Risk. Effective utilization of Tools &Techniques addressing Risk Assessment, Risk Identification, Risk Measurement, Prioritize Risk & Risk Mitigation & Risk Response processes. NAG works closely with Academia and Research studies on Risk & Analytics and AI based startup companies through knowledge sharing, Solution Approach & Go-to Market strategy, and has advanced management studies from Columbia, NYU, Kellogg & MIT.

Eric Lui

Eric Lui is the Managing Partner at HCG Global Partners. He is a senior advisor, executive, and speaker with over 20 years of experience in the investment, management consulting, financial services, technology, risk management, innovations startups space. He holds a MBA from Northeastern University and is a Professor at NYU and Baruch College teaching Business Strategy, Enterprise Project Management, and Innovation. Eric was also awarded the 2019 Outstanding 50 Global Asian Americans in Business.

trade wars and financial risks

by **Alex** Marinov

what is a trade war?

Trade wars have a long history, since countries began imposing tariffs and levies on imports and exports, either as a retaliation on a political topic or to protect manufacturers and farmers from unfair competition.

When the terms “trade” and “war” are combined, they imply actions both military and/or economic to undermine particular industry sectors or countries in their trade dealings.

The most recent example is the current trade war between the USA and China.

what effect is the current trade war having on companies and businesses?

This can be summed up in one word: Severe.

There are several examples of past trade wars, such as the famous Opium Wars and the restrictions that followed the Cold War.

Currently, we are in the midst of the biggest and most hard fought trade war yet fought - China vs USA. This trade war has had severe implications, not just for the countries themselves but also around the globe.

The dispute started at the end of 2017, when $200bn worth of Chinese products were targeted by the USA for tariffs, which most recently have increased to 25%. China reacted and also imposed tariffs on $110bn worth of US goods. In theory, this made Chinese products more expensive for Americans which should prompt them to buy US-made equivalents; the same goes for Chinese consumers. However, given the way global supply chains have been built, the outcome is not always straightforward. In fact, the effect was not only felt by companies based in the USA and China.

far-reaching consequences

This dispute has had far-reaching consequences on companies which are not directly involved in these tactics. For example, Jaguar Land Rover’s largest market is China, but the recent trade dispute has pushed the company to a loss of £264m. It has also caused chaos in both US and Chinese stock markets, where the Dow went down to about 1,200 points and some companies experienced severe volatility in their stock prices due to their significant exposure to the Chinese market. It is also affecting other countries such as Japan. For example, Japan Display Inc. reported losses of ¥109.4bn (approximately $992 m) due to sluggish sales of iPhones caused by a slowdown in the Chinese market. Meanwhile Intel, one of the largest chip manufacturers, has 25% of its sales coming from China.

A major effect has also been felt by US farmers who export heavily to the Chinese market, where the severe tariffs are causing declining interest in their products.

Another aspect where companies are being hurt is in their procurement of highly qualified specialists such as those in advanced engineering. Technology companies such as Intel and Qualcomm have been hit especially hard, as they rely heavily on nationals from China to fill highly specialized roles, which require regulatory vetting beforehand, as reported in a recent article by the Wall Street Journal[1].

China is also severely impacted as the majority of the economy is run by small and mid-sized enterprises, which have stopped hiring because of the ongoing uncertainty. This is a big issue for a dynamic job market where new positions are needed to keep the economy from slowing down.

strategic measures taken to mitigate the effects of trade wars

Trade war events are very difficult to predict and overcome, wreaking havoc to existing supply chains.

If firms see their sales slow down significantly, they are forced to revise their growth targets as well as investment decisions, even though the majority of the growth in trade and commerce is coming from Asia. This is also scaring off potential investors, who are staying away from companies with significant exposure to the Chinese market, creating a ripple effect through the wider economy.

In addition, both China and USA have announced various measures to mitigate the effects on each side of the border. For example, US farmers received subsidies worth $12bn for last year, and this year they are poised to receive close to $15bn.

Manufacturers have started moving their factories abroad and some of the countries poised to benefit from this are Taiwan, Cambodia, Thailand and Malaysia. One company helped close to 300 manufacturers move production lines and equipment to other countries.

Another example is Vietnam, which has enjoyed 7% growth year-on-year and significant FDI of around $10.8 billion just in the first quarter of 2019, thanks to the fact that it is considered a sanctuary amidst the deepening escalation between the USA and China. But such logistics take time, are costly, and require a very dedicated team.

enhanced monitoring framework

Trade wars cause significant financial risks not only for the countries' respective political establishments but also for the wider economy, putting a serious wedge in the sales, investment and growth perspectives that are the driving forces behind economic growth and prosperity.

So how can one prepare in such an environment and tackle such significant effects?

One avenue is to have a robust strategy risk framework within the organization that monitors the largest clients, their country of origin, potential political/economical risks and diversification. In business it is never a good idea to have just one big client, but rather to have many medium/small ones, as one big client no matter how robust it might seem, could always go under. In addition, we all know that even the best of plans fail, but what never fails is having the resources in both people and team spirit to overcome such challenges and find suitable avenues to mitigate such effects. Usually, smaller companies are nimbler than big corporations as they have less constraints on their supply chain (it's easier to move 50 people compared to 2000 to another location or country). Finally, a dedicated and decisive management team can make an informed choice, but nobody can predict all the outcomes and all the risks which need to be taken.

Even the best strategy is dependent on political and economic developments, and the best resolution for a trade war is an amicable solution that leaves both countries satisfied with the outcome.

author

Alex Marinov

Alexander Marinov is a Market Risk Associate at Barclays Investment Bank. Mr. Marinov has been working in the financial services industry since 2013. Prior to joining Barclays he worked at BNY Mellon. Mr. Marinov has a MSc in Economics and International Financial Economics from the University of Warwick and Bachelor's in Economic and Social Studies from the University of Manchester. He is a PRM holder since 2015.

1 / WSJ May 19 - U.S. Slows Hiring of Chinese Nationals by Chip Makers - Link

operational risk governance - myths and facts

by **Rita** Previtali

governance drift

Industry players are drifting towards viewing operational risk management as part of either Internal Audit or Compliance. In fact, it is neither. Folding operational risk management under the umbrella of Audit or Compliance impedes the discipline's ability to effectively help organizations confidently avoid disastrous economic shocks, achieve desired cost reductions, and realize growth objectives.

Historically, operational risk control emerged from the Sarbanes-Oxley Act of 2002, SOX, brought into law after two major company financial reporting fiascos, Enron and WorldCom. The market and regulators determined that the control gaps that led to their demise resided in operational risk control, or better, the lack thereof. Although the Audit and Compliance functions existed, these two functions' goals did not cover oversight of the complete operational processes for the entire organization.

evolution of operational risk governance

The genesis of operational risk control is SOX Section 404: Assessment for Internal Control, which requires that a firm's annual company reports must "contain an assessment, …, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting".

To comply, companies generally adopted an internal operational risk control framework, following what is known as the "COSO" components, which are guidelines issued by the Committee of Sponsoring Organizations of the Treadway Commission.

Establishment and implementation of the internal control framework generated an innovative mind-set based on objective and independent assessments not only of financial statement processes but also of all operational processes throughout the organization that could directly or indirectly affect a company's financial performance.

Now, however, recent industry publications, risk management training documents, chats, and blogs put forward by respectable but, perhaps misinformed, individuals within the risk management community at large and/or by trade organizations show an overall impetus to fold operational risk management under other fields of organizational control[1].

1 / The Institute of Internal Auditors has modified its International Professional Practice Framework, effective Jan 2017, to include operational risk management activities under their responsibilities. Presentation: Internal Audit Standards, IIA, Australia. Pg.4 - Link

This has created confusing myths that beg examination. Myths must be flushed out and facts need to be cemented so that the essence of operational risk management and its importance as a necessary independent, stand-alone, discipline is fully recognized. This will allow organizations to confidently rely on the intended benefits of operational risk management.

myth 1

"Operational Risk is part of the Internal Audit organization."

Fact: Audit's goal is to attest the veracity of a company's financial statements by verifying that the data presented on these statements faithfully reflects the actual financial situation of a company and its continuous viability. Audit also advises financial/product control and financial reporting on the most accurate ways of presenting the financial statements.

If operational risk is folded under Audit's umbrella, this would risk overlooking/missing critical operational controls that might not be sufficiently consequential to auditors at the moment of detection.

myth 2

"Operational Risk is part of the Compliance organization."

Fact 1: Compliance's main focus is to ensure that a company conforms with regulatory mandates by recommending governance and guidelines and their implementation. Compliance also ensures that a company is legally protected by clarifying regulations, old and new, and guiding it to the correct regulatory interpretation by constantly verifying the path of action with the regulatory bodies.

Folding operational risk under Compliance would compel it into a legal compliance angle. It could miss/overlook operational risks that would not necessarily be the immediate concern of a compliance department. A resulting oversight could later impact the organization if the risk control gap were not adequately addressed.

Fact 2: Operational risk events (ORE) occur frequently during daily activities. ORE findings need to be protected from countervailing management interests if the OREs compromise the division's good standings.

Fact 3: Procedurally, the operational risk framework establishes that a sound review must verify processes in the field, depicting process or data flows and their corresponding control points when warranted. Some schools of thought, however, recommend starting a process review by asking the manager(s) where they believe is their operational risk gap. Abiding to these recommendations would cause operational risk control to lose its effectiveness. Operational risk detection relies on strict on-the-field review of processes and their abiding to approved procedures.

conclusion

In order for operational risk management to effectively protect an organization and facilitate its growth, it must be an independent entity, reporting to the Board.

references

i. https://en.wikipedia.org/wiki/Sarbanes%E2%80%93Oxley_Act - Sarbanes–Oxley Section 404: Assessment of internal control

ii. "if the (Risk Management) Committee (of the Board), identifies issues concerning operational risk, it typically refers these to the audit committee for review"- Market Liquidity and Asset Liability Management, (MLARM), PRMIA Risk Management Handbook. Page 35.

iii. What Is The Role of The Audit Function – MLARM, PRMIA Risk Management Handbook. Page 47. Box 2.- Example Statement of Audit Findings.

author

Rita Previtali

Rita Previtali is a Certified Risk Management Executive with over 15 years of experience in operational and market risk control across investment banking, fund management, and broker/dealer segments, information technology and consulting firms.

She has deep knowledge of global capital markets, financial products including derivatives, market risk valuations, operational risk assessment, credit risk, and global financial regulations with extensive program/project management experience; former Big 4 risk management, IT/automation, and financial consultancy.

She has an MBA and MIM from the Thunderbird School of Global Management; a PRMIA Market, Liquidity and Asset Liability Management Risk Manager certificate; is a RIM Institution Assessor; and certifications from Columbia University in Comprehensive Risk Management and MIT in Artificial Intelligence, Implications for Business Strategies.

taming the “known unknowns”

by **Mark** D. Trembacki

Expect the unexpected. Reflect on any ten-year period from a geo-political, economic, social, climate, or technological perspective – unexpected events do occur. Here is a quick review of select unexpected events of the 2000’s: (Decade Timeline: The Last 10 Years - 2000-2009, 2009)

- Terrorist attacks on the World Trade Centre and the Pentagon kill nearly 3,000 people.
- Enron goes bust at a cost of $17b; WorldCom collapses after fraud investigation of $3.8b.
- The Euro is introduced into 12 countries within the Euro-zone.
- First cases of a new respiratory disease, SARS, emerges in Hong Kong.
- Facebook is founded; YouTube and Twitter launch; the verb “to google” enters the Oxford English Dictionary.
- Hurricane Katrina hits New Orleans, causing major flooding and loss of life.
- “Black Monday” - Lehman Brothers goes bankrupt; Fannie Mae and Freddie Mac are bailed out by the U.S. government; U.S. announces a $700b bailout package.

Clearly these events were unknown, but not entirely unanticipated; deadly weather, extreme economic swings and new diseases do occur. Our desire to better manage overall risk outcomes should be bolstered by the fact that we can anticipate the occurrence of unexpected risk catalysts.

In his remarks in February 2002, Donald Rumsfeld referenced “known unknowns” (DoD News Briefing - Secretary Rumsfeld and Gen. Myers, 2002):

> *“As we know, there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns—the ones we don’t know we don’t know.”*

Although Rumsfeld was ridiculed by pundits at the time, the underpinnings of his remarks do enjoy relevance in multiple disciplines, including science, sociology, philosophy and project management.

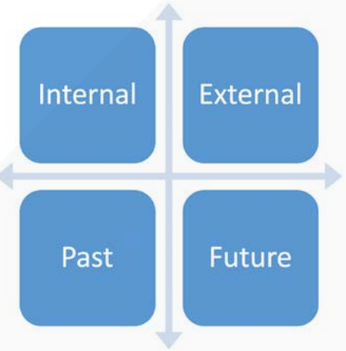
The most fundamental risk management framework effectively deals with the “known knowns,” concrete items that are predictable and therefore quantifiable. When we look at events we can expect, but not predict, our ability to quantify is reduced; however, we can work towards productively managing the outcome.

A straightforward and powerful framework to deal with a vast array of “known unknowns” and their potential outcomes contains three steps:

These events are, by definition, impossible to specify; however, they are not impossible to anticipate. One way to project the types of occurrences (and their related impact) is to look within and outside of the organization using past and future filters:

Internal: What sort of unexpected events have hit the organization and what was the impact to operations and financial outcomes? What keeps us up at night relative to our own vulnerabilities?

External: What have other companies experienced in the past, both in our peer group and in other sectors? What are prognosticators saying about possible future disruptive events and trends?



Although defining the potential event is interesting (and, dare I say, fun), a more critical step is assessing and estimating the impact arising from a catalytic event. At the end of the day, what actually happens is less important than the event’s potential to destabilize the organization. Here is where high-quality business continuity plans can come into play. Although most plans are predicated on certain events, the true driving force behind a plan is tackling how those events may impact the organization.

In the final part of the framework, it is essential to articulate a range of responses to the event outcomes. At this point the “known unknown” converts to a “known known.” Although business continuity plans can inform the discussion, unexpected events often cause deeper disruption or greater loss because they are outside our normal paradigms in terms of potential impact. Consequently, scenario planning should be amped up to include how certain risk factors may conspire to simultaneously work against us. The response may need to be equally integrated.

Rumsfeld also referenced “unknown unknowns” – the most dangerous risks as we cannot manage a risk of which we are unaware. These events are not expected because there has been no prior experience or other basis for expecting them. Becoming aware of these risks over time occurs through discovery, a process supported by a strong risk management framework. In turn, this conversion to either “known unknowns” or “known knowns” allows for risk management through the corresponding analytical and response frameworks.

A solid risk management framework and a comprehensive business continuity plan are essential to building organizational readiness and resilience. Think about what can happen, project how it can impact your organization, and focus on how you will respond to ensure your preparedness for that next unexpected event – whether known or unknown.

references

1. Decade Timeline: The Last 10 Years - 2000-2009. (2009, October 19). The Guardian.
2. DoD News Briefing - Secretary Rumsfeld and Gen. Myers. (2002, February 12). Retrieved from U.S. Department of Defense: https://archive.defense.gov/Transcripts/Transcript.aspx?TranscriptID=2636

author

Mark Trembacki

As Managing Principal of Risk Management Levers, Mark Trembacki provides organizations with practical value-added solutions in strategy development and execution, enterprise risk management, acquisition integration and governance. He teaches Enterprise Risk Management in the Masters of Finance program at the University of Illinois, Urbana-Champaign. Mark enjoyed a diverse career at BMO Financial Group, holding a variety of executive risk management and business leadership roles.

Mark graduated from the University of Illinois, earned an MBA in Finance from The University of Chicago Booth School of Business, and is a CPA. He earned a Cyber Security Management Graduate Certificate from the University of Virginia and is recognized as a National Association of Corporate Directors (NACD) Governance Fellow. Mark serves as Board Chair of the DuPage Children’s Museum and Treasurer of the Chicago History Museum.

fintech horizons 2019 review

FinTech Horizons was a compelling event designed to look at the intersection of Financial Services innovation and Risk. This inaugural event had over 130 registrations and attracted a very diverse delegate background ranging from banking and asset management to FinTech. The presenters shared experiences and ideas from the trenches of co-opetition. For a full look at what was covered, please listen to the recordings at https://soundcloud.com/prmia/sets/fintech-horizons-2019 and view the entire agenda at: https://2019.fthorizon.app/.

The conference kicked off with Menekse Gencer, SVP of Digital Transformation at Wells Fargo, who talked about the principles of digital transformation and the risk principles used when digitizing processes and the entire enterprise. Devin Banerjee, the senior editor from LinkedIn, asked punchy questions on the digital transformation roadmap and balance between risk and reward.

We jumped straight into Machine Learning Applications in the Financial Services area, doing an in-depth review with Prof. Sanjiv Das from Santa Clara University of current projects applied in the VC labs supported by the banks. Bob Mark, PRMIA San Francisco Chapter Regional Director and Founder of Black Diamond Risk, moderated this as well as the next session looking at Augmented Intelligence: Turning Humans into Computational Superheroes. Sanjiv was joined by Moody Hadi, Senior Financial Engineer for S&P Global, and Jack Kim, CRO of Data Capital Management. This session had interesting observations on the complexity of tuning the algorithms in your favor, data management and data cleansing.

The Future of Capital Markets conversation followed and featured individuals who build or fund Capital Markets Infrastructure (CMI) as they discussed the current state of the industry and what the path of least resistance looks like in their view. Distributed Ledgers had many tailwinds for infrastructure, and tokenization was heavily discussed.

After lunch, Marc Barrachin, Head of Product Research and Innovation at S&P Global, joined Torbjorn Jacobsson, CRO of Avida Finans from Sweden, and Michael Warner, a Senior Strategist at the SF Fed, to discuss how digitalization is creating new dimensions in risk management. Like many developments, this is a double-edged sword, but the conclusion was that technology is generally an enabler and minimizes risk. Listen to the fascinating conversation, moderated by the Chair of PRMIA Institute, Justin McCarthy.

Adrien Vanderlinden, a Systemic Risk Executive from the DTCC, discussed his research findings on the systemic exposures the FinTech sectors converges, looking at regulatory issues, bundling and unbundling, concentration risk, interconnectedness and AI model risk.

The next session featured Jos Gheerardyn, CEO at Yields, who showed how firms can implement a real time model risk management framework and automate a big chunk of the model risk process. Hersh Shefrin, Professor at Santa Clara University, discussed the opportunities and dangers that AI has for our society at large, from assisting humans in complicated decisions and tasks, to causing disasters. Krishna Gade, CEO of Fiddler.ai, followed with a brief presentation on how to build auditable and explainable AI. Jos, Hersh and Krishna then discussed the strategic considerations when applying Machine Learning in the financial services space and the data management landscape in a conversation moderated by Bob Mark.

Our last panel covered the regulatory roadmap for FinTech and tokenization which was covered by Harriet Britt, Chief Compliance Officer for Union Square Advisors; Laxmi Ramanath, Founder of LaMeer; Torbjorn Jacobsson, CRO for Avida in Sweden; and Hardy Callcott, a Partner at Sidley Austin LLP. You may listen to the recordings at https://soundcloud.com/prmia/sets/fintech-horizons-2019.

The date for the 2020 FinTech Horizons is being finalized for April and will be announced soon. If you have ideas on topics or speakers, please reach out to Alex Voicu at alexvoicu@prmia.org.

external risks and the challenge of two cultures[1]

by **David** M. Rowe, Ph.D.

two cultures

Detailed distributional models are very useful tools for assessing the impact of most typical market changes. Nevertheless, blind mechanical use of such models will fail if it ignores critical judgmental inputs and geopolitical analysis of what makes any given situation unique. Often this is not advice that is easily implemented by risk managers whose background is narrowly technical. Effective provision of such judgmental inputs is the work of a lifetime, not a short-term change in focus for those without the appropriate background.

One implication of all this is that we need a significant shift in risk management personnel away from highly skilled specialists in current mathematical techniques and toward professionals with a broader and richer background in the social sciences. Even this, however, will not be an easy transition. The reason why is reflected in C.P. Snow's 1959 essay entitled The Two Cultures and the Scientific Revolution[2]. In this essay, Snow highlighted the often willful lack of communication between scientists and literary intellectuals.[3] In all too many cases, Snow argued, formal training compounded inherently different mindsets to produce a nearly complete lack of understanding and communication across these two cultures.

black boxes

Snow's essay comes to mind when considering a similar problem that afflicts the practice of modern finance, namely the split between "quants" and the larger community of traditional financial managers. Quantitative pricing techniques and statistical risk management are little more than opaque black boxes for all too many general financial executives. What is more, those who do understand the technical details often have limited insight into broader structural and behavioral issues. They also have little incentive to make their work more transparent to outsiders since this would undermine the "mystique" that surrounds their skill set. In some situations, a lack of technical insight has little or no serious consequences. After all, few of us can understand the technical mechanics of a modern automobile but that does not inhibit our ability to drive. In the case of financial management, however, the impact of Two Cultures can be serious indeed. This is primarily because running a financial institution demands a constant series of large and small decisions under uncertainty. Such decisions can never be effective if they are made mechanically.

1 / This essay is a slightly edited excerpt from the author's book An Insider's Guide to Risk Management – Relearning the Lessons of the Global Financial Crisis. The printed book is available from both www.amazon.com and www.barnesandnoble.com. It also is available as an iBook from the Apple App Store and on the Amazon Kindle.

2 / Snow, C.P., The Two Cultures and the Scientific Revolution, Cambridge University Press, 1959.

3 / Snow was a trained scientist who also wrote imaginative literature. As such, he was uniquely qualified to assess the problem of The Two Cultures.

Effective decisions must reflect experience and judgment conditioned by the available empirical evidence. As finance has become ever more complex and quantitative, the communications gap between finance's Two Cultures has become ever more consequential. Most senior bank managers are unable to weigh the subtle details of modern finance and few state-of-the-art quants are well equipped to assist them (even if they were motivated to do so.)

closing the gap

Snow says, "Closing the gap between our cultures is a necessity in the most abstract intellectual sense, as well as in the most practical. When those two senses have grown apart, then no society is going to be able to think with wisdom." The same is true of financial institutions. If they are going to be able to "think with wisdom", it is necessary to broaden the range of skills actively engaged in risk management. Accomplishing this requires that we begin to close the gap between the cultures of quantitative finance and general financial management.

For several years I was a permanent attendee at the Market Risk Committee of a major bank. The two-hour agenda typically started with a scheduled ten-minute briefing by the bank's economics department. Often, however, the committee chairman would begin with a statement like, "Let's make this first item quick, we have many important issues on today's agenda." In retrospect, I think this experience illustrates an important weakness in the way financial risk management evolved prior to 2008. Analysis tended to be too narrowly focused. We concentrated on specific markets and estimated volatilities and correlations across markets using comparatively short data histories. In brief, the models we used in financial risk management were radically reduced form constructs. They were effectively descriptive not structural. We paid too little attention to the pervasive reality that social systems embody unstable random processes. Merely examining price volatility and correlation in a reduced form fashion does not give us meaningful insight into structural stresses that may result in radical and sudden shifts.

In December of 2009, with the effects of the Global Financial Crisis still very much in evidence, Roger Bootle of Capital Economics was asked what risk managers should do differently in the future. After a moment of thought he replied, "I think they should read less mathematics and more history and literature." That was wise advice that we all should take seriously today.

author

David M. Rowe

wrote the monthly Risk Analysis column in Risk magazine from 1999 through late 2015. He has over 40 years of experience at the interface between economic forecasting, finance, and risk management with the rapidly changing world of information technology. His professional career included years spent at Wharton Econometric Forecasting Associates, Townsend-Greenspan & Co., Security Pacific Bank, Bank of America, SunGard and Misys as well as his own small consulting firm. Dr. Rowe is also a former board member of PRMIA.

PRMIA nominating committee profile

2019 Board Elections

by **Andrew** Auslander and **Bonita** Dorland

Nominating committee co-chairs

the nominating committee

A new election season has begun. Your nominating committee continues to focus on maintaining a high caliber board and build on our mission and strategic objectives. To these objectives, over the years we have introduced new procedures as well as considerations for changing the by-laws. Recognizing the importance of continuity of leadership, the bylaws were amended by instituting a “daisy chain.” This provides for the sequencing of board positions on a rotational basis.

The Committee’s Terms of Reference states the purpose of the committee is to “support the Board in fulfilling the Board’s responsibility to identity candidates to serve as Directors of the Association.” To support our work, we have developed a worksheet/scorecard comprising elements considered important to be an effective Board member. While this is an objective standard, a key consideration is the qualitative components that include interviews with nominees and feedback from other members.

Over the recent years we have focused on continuity, quality and diversity of leadership. While these are still pillars of our work, the 2020 year will add more attention to: building focus on adjusting our strategic objective to the fast changing world, ensuring financial strength to support being a member-driven organization, and building our brand.

fast changing world

With the fast growth of technology, burgeoning rules and regulations, and the always important risk-reward trade-off, we understand the necessity to be at the cutting edge. PRMIA has been successful in this through our many conferences, affiliations with universities, risk competitions, etc. This year the Nominating Committee is introducing a new expertise to its worksheet/scorecard with the label Fin-Tech. This label calls attention to technology which is a key driver for the future of risk while also identifying our recognition to stay at the cutting edge.

financial resources

Our organization is wonderful and unique as a by-members, for-members volunteer organization. As such, we rely on our membership for financial support. It is imperative we stay removed from the influences of financial sponsorship that require attachment or wavering of our independence. PRMIA does aspire to have more financial resources in order to better reach the global financial community and accomplish the important work of our mission. We have increased the weight the Nomination Committee gives to nominees who have demonstrated a track record of “Industry Connections/Financial Support/Sponsorship”.

building PRMIA brand

PRMIA will continue to focus on building its brand encompassing the numerous elements of a successful board, including diversity, leadership, volunteer experience, and collaborative abilities. A successful board is a sum of its parts combining to generate solid, committed and forward looking leadership. Our Brand is a direct result of the work and outreach of PRMIA’s members. This includes growing our affiliations through individuals and institutions that recognize the value of risk management and independence. This will include not only a global focus but also industries such as mutual funds, insurance, etc.

Appreciation to the PRMIA Nominating committee of 2020 who are: Mark Abbott, Dr. Nasreen Al Qaseer, Marc Grande, Robert Iommazzo, and Susan Ma.

Special thanks to the outstanding PRMIA personnel Ken Radigan and Kristin Lucas.

author

Andrew Auslander and **Bonita** Dorland

PRMIA member profile

by **Adam** Lindquist

PRMIA Director of Membership

When Gift Moonga began his career in banking, risk management was the farthest thing from where he imagined he would be 25 years later. “I was working for a commercial bank on the sales side and decided I was interested in earning a Masters in International Banking and Finance.” His degree pursuit found him in England, which required a course in risk management as part of the master’s program. He stated:

> “My instructor noticed how interested I was in the topic and suggested I explore risk as a career and recommended the Professional Risk Managers’ International Association (PRMIA) and the Professional Risk Manager (PRM) designation. It was challenging and interesting to me and seemed like a great way to set myself apart professionally,”

When you first meet Gift you realize that he has an enthusiasm that is almost contagious. That’s probably why his initial bank employer started him in customer relations but advanced him to head up their small and medium enterprise client businesses. His name describes what makes him special, he has a special gift for pushing and challenging himself. “I came back from the master’s program with an interest in pursuing the PRM with an understanding that part of the reason I wanted to do it was the challenge that it was going to be hard. In fact, halfway through, I realized I needed more foundation and stepped back to take the Associate Professional Risk Manager Certificate to give me the foundation for the PRM.”

While the PRM proved challenging, he discovered quickly that what he was learning had relevancy. “My boss came to me with a problem he was trying to solve, so I pulled out my course notes and showed him how to solve it. He looked at me with a blank stare and asked me where I had learned my skills and I told him about PRMIA.”

His boss was impressed, and soon his opportunities within the bank began to develop more broadly but the true value of his PRM proved itself when his boss was asked to speak at an annual Chartered Accountant event about risk management in banks, and immediately recruited Gift. “I was excited to have the opportunity, and the audience responded extremely well to my talk. Soon my professional network was much larger.” He smiled.

“There is a lot of information within the PRM, and it exposes you to things that frankly we are just starting to explore where I work in Africa.

Gift has grown into the Head of Risk Management in ERM at his firm and is a strong proponent of leveraging PRMIA to train his team. “I like the specialty certificates for helping my people find and enhance their areas of expertise. The PRM is always part of the recommendation, as I feel it truly provides the best foundation on risk there is. I don’t care what role a person has in risk, the PRM will help them advance.”

Through PRMIA, he came across the NYU – Stern Business School advert for the Masters in Risk Management which he was impressed to pursue and immediately requested his employer to help sponsor which they did.

“Association with PRMIA, has been truly a ‘cradle to the pinnacle’ experience,” he says. Gift certainly is personally motivated to advance in his career, and with his energy and commitment his team is adding to his success as well.

PRMIA member

Gift Moonga

author

Adam Lindquist

Adam Lindquist is the Director of Membership for PRMIA. His career background includes vertical integration disruption as a regional manager in banking, business development resulting in a 5-year run as fastest growing specialty retailer, and many entrepreneurial ventures.

PRMIA Montréal spotlight

Montreal is home to one of the most active chapters of PRMIA. Vibrant and diverse like the city itself, the Montreal chapter demonstrates its commitment to developing the next generation of risk leaders through the organization of many educational events, including the 7th Annual Canadian Risk Forum in 2019. Blessed with four world-class universities at its doorstep, the Montréal chapter has launched several other initiatives to promote risk management education and awareness with practitioners, researchers, and students including its Career Day & Bursary Program, participation in the PRMIA Risk Management Challenge (PRMC) and, most recently, its unique Mentorship Program.

canadian risk forum

PRMIA Montreal is proud to host the 7th Annual Canadian Risk Forum, November 12-13. Senior risk professionals, industry experts, and scholars will share their thought leadership insight on Risk Management: Trending Practices Versus Practical Trends. Join us as we take an in depth look at this topic. Montreal welcomes PRMIA members from the entire PRMIA community to join us at this Forum.

Learn more about the 2019 Canadian Risk Forum.

mentorship program

Launched in September 2014, the Mentorship Program pairs emerging leaders with experienced leaders recognizing that people continually learn from others and mentoring is an innovative way to encourage this process. The PRMIA Montreal Mentorship program targets members who have 5 – 7 years of experience and are looking to further develop their leadership skills with a unique one-on-one mentorship experience geared at enhancing personal and professional growth. While the PRM™ and other designations help provide the robust technical skills that can lead to a successful career, the mentorship program complements these competencies with a focus on developing soft skills such as relationship management and leadership. Candidates for the program must be either Contributing Members or Sustaining Members of PRMIA. The recruitment process and training sessions for both mentors and candidates take place from September to December of each year, with the program occurring from January to December of the following year.

Learn more about the PRMIA Montreal Mentor Program.

bursary program and career day

In its 2019 edition, the PRMIA Montreal Career Day provides an opportunity for students from the different universities from Quebec and Ontario to discover the various professional career paths available in finance and risk management. Seasoned professionals share their experiences, describe their roles and career paths, and answer students' questions through a combination of discussions and presentations. The Career Day is attended by companies who are available to meet with students to discuss potential jobs or internship opportunities.

In conjunction with its Career Day, PRMIA Montreal also offers a bursary award program. Every year, students from universities across Quebec are invited to submit their applications to be awarded the PRM bursary. With a monetary value of $1,430 USD, the bursary provides recipients with all the necessary funding for their studies towards achieving the PRM designation. Over the years, the Montreal chapter has awarded more than 60 bursaries.

PRMIA risk management challenge

As a proud member of the PRMIA community, the Montreal chapter organizes a local event for the PRMIA Risk Management Challenge where graduate and undergraduate students from all over the world compete to solve business cases with a risk management focus.

On March 29, 2019, ten international team finalists met in Montréal QC at PSP Investments to participate in the final championship round of the PRMIA Risk Management Challenge (PRMC). The ten teams represented undergraduate and graduate students from universities/colleges across Chicago, Edmonton, Egypt, Hungary, London, Montreal, New York, Toronto, and Vancouver.

Congratulations to Desautels Capital Management Team from McGill University – Ludovic Van den Bergen, Emilie Granger, Ian Jiang, and Roy Chen Zhang. The champions took home the $10,000 in prize money for the team and were offered fee waivers for the Professional Risk Manager (PRM™) Designation.

All finalists advanced through their local regional round challenges by solving the MATLAB Modelling Challenge and solving risk management issues from a case study of United Grain Growers, a Toronto-listed grain trading company. At the international challenge finalists convened at PSP Investments, where each team presented their recommendations about the evolving risk profile coming out of the digitalization of ING Bank, using a Harvard Business Review case study.

All teams attended a lunch panel discussion about their career in risk management and practical aspects of their jobs with Stuart Kozola, Francois Pouliot, Jean-Charles Bouvrette, Badye Essid, Oscar McCarthy and Ken Radigan. They shared their evolving experience on how they grew, and what are their personal principles for success and ethics.

Through sponsorship, all the participants' expenses for both the local finals and the international championship (i.e. registration, travel, room and board) are covered. We were able to do so thanks to our generous sponsors, most notably Desjardins.

Learn more about the PRMIA Risk Management Challenge.

Thank you to the PRMIA Montreal Regional Directors and Steering Committee Members for delivering these exciting opportunities and for their incredible dedication and commitment to PRMIA Montreal and the Risk Management community.

Regional Directors

- Kabil Jaa, Total Fund Investment Risk and Restructuring, PSP Investments
- Linda El Ghordaf, Partner, Financial Risk Management, KPMG

Steering Committee

- Badye Essid, Senior Manager, Deloitte
- David Latour, Advisory Vice President, Caisse de dépôt et placement
- David Streliski, Senior Vice-President and Chief Risk Officer, Fiera Capital Corporation
- David Whittall, Chief Risk Officer, Pembroke Management Ltd
- Francesco Faiola, Educational Events Committee, Executive Director, Client Coverage, MSCI
- France Panneton, PRMC Quebec Committee, Educational Events Committee, Mentor Program Committee, Freelance Advisor
- Jean-Charles Bouvrette, PRMC Committee, Director, Integrated Risk Management Modelling, Desjardins
- Jeff d'Avignon, Educational Events Committee, Senior Sales Executive, IBM Canada Ltd.
- Pascal Francois, Co-chair Mentor Program Committee, Co-chair Career Day Committee, Director, IFSID
- Ron Cheshire, Co-chair Mentor Program Committee, Educational Events Committee, Vice President, Foyston, Gordon & Payne
- Ryan Kastner, Co-chair PRMC Committee, Senior Associate, Financial Strategy Group, Mercer
- Simon Beaulieu, Educational Events Committee, Partner, Ernst & Young, Financial Services Advisory
- Stéphane Thomas-Simonpoli, Director, Global Research & Analytics North America, Chappuis Halder & Co.
- Steven Rinaldi, Co-chair PRM Bursary Program, Educational Events Committee, Advisor, Project Integration and Optimization, Caisse centrale Desjardins

calendar of events

Please join us for an upcoming training course, regional event, or chapter event, offered in locations around the world or virtually for your convenience.

PRM™ SCHEDULING WINDOW

September 14 – December 20

ERM 2.0 – STRESS TESTING, CAPITAL PLANNING & SCENARIO ANALYSIS

November 5 – December 10 – Virtual Training

EMEA RISK LEADER SUMMIT

November 5 – 6 – London

NACHHALTIGKEITSRISIKEN

November 7 - Frankfurt

CANADIAN RISK FORUM

November 12 – 13 - Montreal

FRTB AND THE COMPUTE BOTTLENECK

November 13 – Webinar

PRM™ TESTING WINDOW

November 18 – December 20

INTRODUCTION TO THE MONTE CARLO METHOD

November 20 – Webinar

WHAT THE BOARD NEEDS TO KNOW ABOUT THIRD PARTY RISK MANAGEMENT

December 4 – Webinar

TECHNOLOGY RISK MANAGEMENT IN THE DIGITAL TRANSFORMATION ERA

December 11 - Webinar

PRMIA RISK MANAGEMENT CHALLENGE

January 10 – April 2020

INTELLIGENT RISK

knowledge for the PRMIA community

PRMIA
Professional Risk Managers'
International Association