INTELLIGENT RISK

knowledge for the PRMIA community

April 2019

PRMIA
Professional Risk Managers'
International Association

PROFESSIONAL RISK MANAGERS' INTERNATIONAL ASSOCIATION

CONTENT EDITORS

Steve Lindo
Principal, SRL Advisory Services and
Lecturer at Columbia University

Dr. **David** Veen
Director, Evaluation Services - IT
at Western Governors University

Nagaraja Kumar Deevi
Managing Partner | Senior Advisor
DEEVI | Advisory | Research Studies
Finance | Risk | Regulations | Digital

INSIDE THIS ISSUE

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

editor introduction

Steve Lindo
Editor, PRMIA

Dr. **David** Veen
Editor, PRMIA

Nagaraja Kumar Deevi
Editor, PRMIA

The April 2019 issue of Intelligent Risk features articles on Managing Preventable Risks, which are risks arising within an organization that are controllable and, therefore, avoidable. While a small amount of these risks may be tolerated due to the inevitability of human failings and considerations of operational costs and flexibility, preventable risks are inherently undesirable, because taking these risks produces no strategic benefit to an organization.

The articles submitted by PRMIA members for this issue of Intelligent Risk cover a broad set of perspectives on this topic, ranging from controls, monitoring, governance and training to data quality, IT integrity and advanced technology. Several articles focus on methods to avoid failures in the area of regulatory compliance, which has been a source of heavy losses for banks.

The next issue of Intelligent Risk will feature articles on Managing Strategic Risks, which is the second of our 2019 topics. In the meantime, we hope that you enjoy reading the articles published in this issue as much as we did editing them.

sponsor

DataRobot

DataRobot is the category creator and leading provider of automated machine learning. Organizations worldwide use DataRobot to empower the teams they already have in place to rapidly build and deploy machine learning models and create advanced AI applications. With a library of hundreds of the most powerful open source machine learning algorithms, the DataRobot platform encapsulates every best practice and safeguard to accelerate and scale data science capabilities while maximizing transparency, accuracy and collaboration.

By making data scientists more productive and enabling the democratization of data science, DataRobot helps organizations transform into AI-driven enterprises. For more information, visit www.datarobot.com.

letter from leadership

Ken Radigan
CEO, PRMIA

Welcome to the April 2019 issue of Intelligent Risk!

I was privileged to serve as both a panelist and judge at the recent PRMIA Risk Management Challenge international competition in Montreal, where the top ten teams from the regional rounds gathered at PSP Investments to present their recommendations about the evolving risk profile coming out of the digitalization of ING Bank, using a Harvard Business Review case study.

Congratulations to this year's champions, Desautels Capital Management Team from McGill University – Ludovic Van den Bergen, Emilie Granger, Ian Jiang, and Roy Chen Zhang. The champions took home $10,000 in prize money for the team and were offered fee waivers for the Professional Risk Manager (PRM™) Designation. Congratulations also to the runners-up, Team Riskcoders from the Beedie School of Business, Simon Fraser University - Tunc Utku, Lingyun (Iris) Fan, Jingxaun (Jessie) Wu, and Priyaadarshini Elango. The runners-up were also awarded fee waivers for the PRM™ Designation. Each team that qualified for the final received PRMIA Sustaining memberships for each team member.

Thank you to my fellow panelists and judges who volunteered their time for this important annual competition that helps to build leadership and career development opportunities for graduate and undergraduate students around the world looking to enter the world of risk management. Based on the skills, talent, and leadership skills I saw displayed at this year's challenge, the future is looking bright for risk management!

Ken Radigan
PRMIA CEO

Thank you to our international sponsor

MathWorks
Accelerating the pace of engineering and science

Thank you to our local sponsors

RBC

Scotiabank

Congratulations to the 2019 PRMIA Risk Management Challenge champions, Desautels Capital Management Team from McGill University.

5 AI solutions every chief risk officer needs

by **Seph** Mard

For the risk manager, AI means greater efficiency, lower costs, and less risk. This article focuses on five key solutions with huge potential ROI that every chief risk officer can begin building immediately. Representing foundational capabilities for risk management, these five solutions have the potential to substantially impact financial results, and an automated machine learning platform represents the most efficient and effective method of delivering on the promise of these AI use cases.

1. Anti-money laundering

Every year organizations spend millions of dollars on detecting, investigating, and reporting potential money laundering – and for good reason. It's not uncommon for regulators to levy fines for inadequate or lax anti-money laundering (AML) monitoring that exceed one billion dollars.

Transaction monitoring systems (TMS) are (mostly) rule-based systems that are designed to identify transactions that might be indicative of money laundering. These systems, which are designed to avoid missing potential money laundering (false negatives) at any cost, generate reams of alerts, forcing banks to set up large investigative teams to handle all of them.

Machine learning models can be used to score alerts according to how likely they are to actually result in a Suspicious Activity Report filing. The bank has complete control over how conservatively this system performs so that the number of false negatives can be reduced to near zero.

2. Fraud detection/prevention

Losses due to fraud increase every year, with some estimates claiming worldwide losses to fraud as high as $200B in 2017. Despite the cost, many banks are either fighting fraud with antiquated, rules-based systems or with expensive, black-box vendor models.

Running a successful fraud solution means not only minimizing losses due to fraud, but also minimizing irritation and impact to existing customers. For example, blocking a legitimate transaction or placing excessive holds on a deposit may not result in a direct loss to a bank, but they still have a substantial impact in terms of customer satisfaction, retention, and churn.

Machine learning is the ideal solution for fighting fraud. By the very nature of the business, banks record mountains of relevant information about all types of transactions and their counterparties, and whether or not these transactions are fraudulent. This historical data is the foundation of the machine learning approach.

Machine learning models can predict which checks are likely to be bad, which loan applications are likely to be based on identity fraud, or which point-of-sale transactions are likely to be fraudulent. Implementing these models can prevent millions of dollars in losses to fraudsters.

3. Streamlining model risk management

Part of the reason that model validation is so difficult is that most models today are custom-built by hand. Data science teams—and validation teams—don't have the well-established testing and quality control measures in place that software development teams have built over the past several decades.

Another reason for the challenge is documentation. A recent survey conducted by McKinsey & Company found that of the leading financial institutions, 76 percent of respondents identified documentation that is incomplete or of poor quality as the largest barrier for their validation timelines.

Following a systematic and unbiased approach to model building is key to a sustainable model risk management practice. Model developers must be disciplined in the way models are developed and must utilize tools to make the process more reliable and consistent. These same tools should also make the documentation tasks easier, providing interpretability and insights that speed documentation for regulators. These new technologies make safely developing highly-accurate models quicker and easier.

4. Credit risk & loss forecasting

New financial accounting standards are based on an "expected loss" method. Unlike the incurred loss method that is based on backward-looking loss rates, the expected loss method applies when the loss has not yet occurred, but its occurrence is probable. In other words, the loss of future-flow is expected with some probability and must be estimated. Machine learning provides the most robust framework for producing highly accurate and transparent expected loss predictions.

The new expected loss standards require that organizations use historical data and "reasonable and supportable" forecasts when estimating expected credit losses. Although this is a huge change to the current incurred loss standards, it also provides a unique opportunity because the new standards do not prescribe how lenders choose to make the estimate, but only that the forecasts must be "reasonable and supportable." This gives banks the flexibility to implement the best models and methodologies to forecast expected loss.

Accurate and transparent models for predicting expected losses should be at the core of successful compliance programs. Machine learning models detect patterns in historical data to accurately estimate credit losses, and these models are no longer black boxes. Modern tools allow stakeholders to understand how these models work in a detailed way, including why individual predictions were made. Not only is this useful from a compliance perspective, but also from an underwriting and portfolio management perspective.

Granular credit loss models are also the foundation of good risk adjusted pricing. Pricing inefficiencies — overpricing or underpricing risk—can easily be spotted by predicting the expected loss at a given price. Overpricing may indicate potential for volume growth, and underpricing may indicate the need for adjustment in policy or risk selection. Superior pricing analytics may also identify market pricing inefficiencies, including opportunities to acquire portfolios where risk is overpriced or opportunities to originate and sell portfolios where risk is underpriced.

5. Targeted risk review

Risk review functions have moved beyond their traditional "loan review" scope and are now looking at risk holistically:

- **Operational Risk:** Identify potential control weaknesses using error rates, historical operational data, and client complaints as well as new business volumes, employee turnover, client attrition rates, etc.
- **Compliance Risk:** Predict policy exception levels based on historical trends, product mix, control self-assessments, audit findings.
- **Credit Risk:** Predict risk levels across a lending unit and identify pockets of higher or rising risk using delinquency, collections data, and external risk indicators.

Very few risk review teams, though, are leveraging machine learning to improve the quality and efficiency of their work - but they should. Machine learning can guide field work based on business mix, risk metrics, and past reviews of similar areas.

Risk review management uses the historical findings of their teams, along with risk metrics of all kinds, to identify significant or escalating risks, plan their reviews, and allocate their resources optimally. Risk review teams constitute a key part of the third line of defense – assuring that no significant risks go unnoticed, unmitigated, and unmanaged. By utilizing machine learning, these functions can be made smarter, faster, more effective, and more efficient.

More information: Download the full eBook at **datarobot.com/risk.**

author

Seph Mard

Head of Model Risk Management at DataRobot

As the head of Model Risk Management at DataRobot, Seph Mard is responsible for model risk management, model validation, and model governance products, as well as services. Seph is leading the initiative to bring AI-driven solutions into the model risk management industry by leveraging DataRobot's superior automated machine learning technology and product offering. Seph has more than 10 years of experience working across different banking and risk management teams and organizations. He started his career as a behavioral economist with a focus on modeling microeconomic choices under uncertainty and risk, then transitioned into the financial services industry. Seph is a subject matter expert in model risk management and model validation.

even preventable risks have a return

by **Ariane** Chapelle, PhD

abstract

This paper argues that all risks have a return, sometimes negligible, sometimes non-financial, but always existent. Categorizing the trade-offs between risk and return, the author proposes 4 essential types of decision-making for firms and individual alike.

returns of operational risks

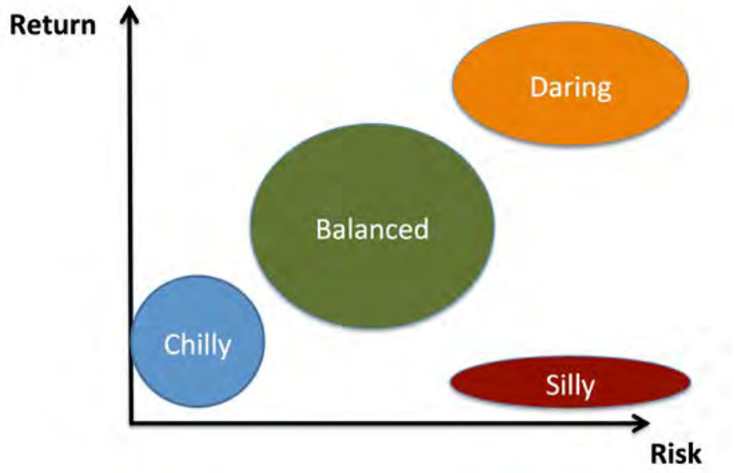
In the financial industry lies the common idea that operational risk, unlike financial risks, has only downside; "you make no money for taking operational risk". Credit margins, insurance margins, and trading revenue are all visible counterpart of financial risks. Can we observe returns of operational risks? Arguable, fee income in financial firms is the visible counterparty of operational risk taking in financial companies.

Industrial or technological companies get very little revenues from financial activities; most of their income is generated by operational activities. Risk management is called operational risk management only in the financial sector, to distinguish it from credit and market risks. Operational risks, even preventable risk, must have a return, since the surest way to eliminate all risks is to halt every business operation, shutting down both the revenues and risks at the same time. Is there an optimum between business requirements and safety? This article highlights four categories of risk-taking decisions.

risk/return trade-off

Arguably, all risk-based decision-making can be assessed from risk/return trade-off perspective. Risks and returns must not be restricted to financial outcomes. While taking risks allows uncertainty of outcome, the return of those risks are the benefits brought by letting the possibility of the risk to materialize: in case of a two-sided risk, it is to capture the upside; in case of one-sided risk, it is simply the convenience, or the cost-saving, of not having a control in place. To convert the concept into practicable actions, this article suggests a typology of four risk decisions: silly, chilly, daring and balanced (Fig. 1).

Figure 1. A typology of risk-return decisions



neither silly nor chilly

Reckless risk taking of easily preventable risks can be qualified as silly risk decisions, those actions where risk-taking can bring only downside and when the cost of avoiding the risk is so negligible compared to the potential damage, that it is quite unforgivable to expose oneself: not wearing a car seat belt, texting behind the wheel, not locking your working station in public places, letting a stranger tail gate you into sensitive work areas. Examples are numerous. How many of those silly decisions do we make in our personal and our professional lives?

In the same vein, neglecting a key control in place (a deal confirmation, a reconciliation, a test) on critical processes are silly risk decisions: the upside is limited to the seconds of time saved or the minor convenience enjoyed, but the possible downside can be a significant fraud or a major disruption. For those obvious preventions, either easy or key, what needs to be done is clear. But how far to push the process? How preventative does an organization need to be, and do all non-financial risks have only downside?

At the other end of the spectrum lies the chilly risk decisions: fear-driven, leading to excessive protection, destroying the possibly of capturing an upside, or misallocating limited resources. Chilly decisions fail to consider the downside risk of immobilism, the cost of not taking risks. Examples include shying away from important transformation projects by fear of complications and change management burden, or applying redundant layers controls on non-critical processes, consuming more resources in mitigation than the income of operations themselves.

Chilly decisions disregard the "money left on the table" through low productivity and poor performance and by not engaging in promising development and changes. The opportunity costs of non-action, like the opportunity costs of inefficiencies, are typically greatly underestimated in firms, because they are much less visible that money outflows and sheer loss events. However, they are possibly much larger.

High-risk-high-return strategies are daring risk decisions. In many regulated sectors, they are largely forbidden. They exist nonetheless, originating mainly from violations to the rules, either under the pressure of profit objectives or fear of retributions. Both individuals and institutions may take daring decisions, such as breaching external compliance or internal rules for financial motives, gambling on the fact that the sanctions will not exceed the profits generated, or that it will not get caught. Subprimes misselling, VW emission fraud and Wells Fargo conduct scandal are all examples of daring decisions gone wrong.

Taking risk can be good, but blowing up should not be part of the possibilities. Thriving companies are those who seek from risk management the opportunities to capture the upside while efficiently limiting downside, just like the payoff of a financial call option, or of an insurance policy. Business operations are full of real options; good risk managers ought to recognize them.

Valuable risk management relate to balanced risk decisions, resulting from conscious, well-informed trade-off between target returns and necessary controls. Examples include all careful investments decisions, commercial initiatives, entrepreneurial projects or other business operations where risk is mitigated to an extent that makes economical sense and accepted when fairly compensated by expected returns. It requires avoiding prone-to-error processes and poor control design, moving unnecessary rework and forgone revenues due to inefficiencies, but up to a point that increases, not decreases, a risk-adjusted efficiency.

Even airlines and high-speed trains accept some level of residual risk for the necessary returns of transport and mobility, but these risks are mitigated down to an ALARP level: As Low As Reasonably Practicable.

non preventable risks: fat tails, surprises and external events – the case for resilience

Besides preventable risk and the mass of small, usually acceptable incidents in well-controlled firms, there are the tail risks events, these surprises, colossal internal failures or critical external events leading to catastrophic consequences to the unprepared: frauds, fires and floods, terror and cyber attacks, political events, crises and disruptions. To all these predictable or unpredictable surprises, resilience is key. No matter the cause or the likelihood of a possible crisis, critical sectors and systemic organizations have the regulatory obligation to demonstrate sufficient operational resilience and ensure the continuity of all its critical processes even in the face of extreme adverse events.

author

Ariane Chapelle, PhD

Associate Professor (Honorary Reader) at University College London

Ariane Chapelle, PhD, is Associate Professor (Honorary Reader) at University College London, a Fellow of the Institute of Operational Risk, and she runs her own training and consulting practice in risk management. She has been a long-time trainer for PRMIA Learning and Development programs.

Ariane's new book Operational Risk Management: Best Practices in the Financial Industry forms the basis for the new PRMIA Certificate of Team Leadership in Advanced Operational Risk.

interview with Massimo Vita, Chair of the RIM Steering Committee

by **Adam** Lindquist, Director of Membership, PRMIA

The Professional Risk Managers' International Association (PRMIA) and The Risk Management Initiative in Microfinance (RIM) merged in July 2018 to meet the growing needs of the risk management community and elevate the mission to set standards and serve the full financial risk management profession.

The merger allows PRMIA and RIM to increase the reach of their institution assessment trainings, expand the RIM membership base, and create a certificate program for the microfinance industry. Combined, RIM and PRMIA increase responsiveness to industry needs and trends in support of its mission. The merger gives PRMIA the full spectrum of financial risk training, from the very beginning journey of an institution's risk awareness, to the fully operational risk department implementing best practices.

We asked Massimo Vita, Chair of the RIM Steering Committee, to share with us insights into the microfinance sector and the future of financial inclusion.

Adam Thank you for your time, Massimo. We have been hearing about microfinance for a while now. What is it, and where does risk management play into the industry?

Massimo Microfinance refers to the provision of financial services to low-income clients, including the self-employed in both urban and rural areas (clients are often traders, street vendors, service providers, artisans, and small producers. Although the clients are poor, they have activities providing a stable source of income). Financial services generally include credit but also savings, insurance, and payment services. In addition to financial services, many Microfinance Institutions (MFIs) provide social services such as group formation, development of self-confidence and financial education.

In general, the most important business and asset in the B/S of an MFI has always been the loan portfolio composed of small loans typically for working capital. The typical activities for micro-lending are usually informal appraisal of borrowers, use of collateral substitutes (e.g., group joint-liability, compulsory cash collateral), or loans renewal based on repayment performance. Therefore, the major risks to be managed have always been credit and operational risk because, especially in their initial stages, MFIs focus on the processes required to administer their loan portfolio.

Massimo However, quoting Karla Brom in our RIM Position Paper (and I could not say it better), "During the past decade, MFIs worldwide have begun a transformation from their status as NGOs (micro-lending only institution) to becoming non-banks and ultimately MFI banks. Each stage of growth represents not only an increase in the number of clients served or types of loan products offered, but also, typically, a greater access to commercial funding sources in the forms of debt, equity, or deposits. This transformation may also feature more sophisticated front offices or payment systems, while back offices often lag behind in sophistication. Therefore, operational risk management extends beyond the credit process and as MFIs grow other areas of risk management require attention as well. With greater access to commercial funding sources has come increased focus on risk management in MFIs, mainly to ensure that investors' funds are protected (i.e., the impetus for risk management has been coming from the investor, more than from the MFI)."

In the last years there have been increased requirements—from regulators, investors, and microfinance networks and associations—for formalized risk management. The Risk Management Initiative in Microfinance (RIM) was created to facilitate the understanding of how a risk management function works and how a formal risk management culture is integrated throughout an MFI. RIM's mission is to contribute to the global development of awareness, best practices, and appropriate standards for risk management in microfinance.

Adam How is risk usually measured today in microfinance?

Massimo This depends on the size and phase of development of the MFIs. We must recognize that smaller and simpler MFIs do not require the same degree of formal risk management as larger and more complex MFIs. To address this priority, RIM developed the Risk Management Graduation Model approach, which is a pathways-based, best-practice framework for risk management in the microfinance sector. The Graduation Model tries to explain how risk management for MFIs is similar to that of banks, and how it is different. This is a very valuable approach since MFIs are often bombarded with requirements, yet don't understand how they can integrate those requirements into their existing framework.

Adam Where is microfinance most prevalent? Who is the primary customer?

Massimo The majority of microfinance operations occur in developing nations (Asia, Latin America and Africa). For the past decade, the microfinance sector has been growing and expanding rapidly in a variety of ways—in geographic reach, the number of clients served, the number and size of loans, the types of products and services offered, and funding sources (including deposits).

Adam What is your and your organization's role in the industry?

Massimo Since 2016 I have been working for CreditAccess Asia (CAA).

Massimo Established in 2008, CAA provides suitable financial services to Micro and Small Enterprises (MSE) in India and Southeast Asia to unlock their potential. CAA attracts funds globally and provides working capital loans and other basic financial services to our customers in our countries of operation. Our service model seeks to create long term relationships with our customers through a `doorstep´ approach, underpinned by innovative technologies, to deliver efficient and customer-centric financial products catering to their entire business lifecycle. Asia is often identified as having the highest potential for strong financial sector development. Around 70% of the lower income population in South and Southeast Asia does not have access to formal financial services. The unmet credit needs of a significant number of MSEs further emphasizes the potential for development of the financial sector in the region. The largely untapped market in South and Southeast Asia forecasts solid economic growth and houses around one third of the world's population, thus providing an exciting potential business opportunity. By utilizing funds sourced from our investors and lenders, who seek financial and social returns, we are able to create and implement suitable financial services for MSEs. Some key figures for CAA as of last audited financial year (March 2018) are: Figures: € 726 million Assets, € 651 million Outstanding Loan Portfolio, > 2.6 million Customers, 945 Branches, 10,500+ Employees

In CAA (headquartered in Amsterdam), I personally set up in 2017 the Regional Business Support Office in Bangkok and my actual Role in the Group is Chief Risk Officer (CRO). I report to the Group CEO and the Group Risk and Audit Committee in Amsterdam. To fulfill my responsibilities I am also a Director in the BoD of our companies in India, Indonesia and Philippines and I am a member of the Risk Committee and Audit Committee in all our companies. Basically, I lead the Risk and Audit team in Bangkok focusing on: A) Risk management oversight and support and B) Internal audit oversight and support to the operating companies in Asia.

Risk Management: The broad objective is to ensure oversight regarding the effectiveness of the risk management framework and process performed across the operating subsidiaries of the Company and at the Group level.

Internal Audit: To ensure the oversight regarding the effectiveness of the internal audit processes and systems, performed across the operating companies.

Before CAA, I worked for Microfinanza Srl, a consulting company specialized in providing qualified services and technical support to the microfinance sector worldwide. I used to provide consulting services to MFIs in corporate governance, risk management and business planning. Also, I worked as Partner and Operations Director for MicroFinanza Rating, a specialized rating agency in microfinance which has the role to provide the microfinance and responsible finance industry with independent, high quality ratings and information services, aiming at enhancing transparency, facilitating investments and promoting best practices worldwide.

Adam What skills are important for risk managers who wish to work in microfinance?

Massimo The need of a dedicated risk manager depends on the size and stage of development (besides the legal form/regulation requirements) of a microfinance institution.

In smaller or early stage Institutions, risk management is usually done by the business line only with the addition of an audit function to ensure that policies and procedures are being followed.

As the MFI grows, the risk management function should formalize and specialize accordingly. However, of course, the business line still remains primarily responsible for risk management.

Second we need to distinguish between credit-only MFIs and deposit-taking MFIs.

In a Credit-Only Institution the major risks for an MFI are:

- Credit (transaction and concentration risk)
- Operational risk (staff selection, staff turnover, MIS/IT, processes efficiency)
- Growth and expansion risk (e.g., geographical dispersion, branch selection)
- Funding (concentration) risk

Therefore, the main skills needed for a risk manager are on credit and operational risk management.

In a Deposit-Taking Institution, financial risk management (especially liquidity risk management and market risk) becomes important like in a bank.

Then, in general, for most growing MFIs we can observe emerging risks and increasing existing ones in most of the markets (e.g., IT changes/innovation, new products, aggressive competition) which require more advanced skills and competencies for the risk management function, such as:

a. Statistics, modelling (e.g., stress testing)
b. New products development and possibly IT and tech products/services
c. Local context knowledge and access to relevant information (including products/services offered by competitors) in order to monitor the business development of new emerging strategic, operational and external risks.

Eventually, in mature MFIs, the risk management function should have the ability to effectively challenge the business lines regarding all aspects of risk arising from actual and future company's activities. Therefore, the CRO and the risk team should be strong in all aspects of risk theory (e.g., economics, finance, mathematics, statistics, and possibly MIS and IT).

Adam What challenges or opportunities do you see on the horizon with microfinance?

Massimo Challenges and in a way opportunities as well (just to mention some of them):

1. Entry of new players with the intent to disrupt the market while not having necessarily the mindset for responsible practices (e.g., Fintech companies, large banking institutions, pension funds, consumer leasing companies, telecoms (e.ge. Telenor in Pakistan) etc, to name a few.

2. Customer needs going beyond traditional microfinance model--Current group of microfinance companies' inability to meet them.

3. Adoption of technology, as data analytics is still very limited in this space. Alternative credit scoring and algorithm based lending is increasingly being explored by MFIs and represents a huge opportunity to make the credit appraisal process more efficient. Digitalization and the rise of the mobile phone.

Adam Why have so many large institutions embraced micro finance?

Massimo There are several reasons, including:

1. Track record of stable returns from existing players
2. New models of partnerships making entry to the segment viable
3. There is money to be made at the bottom of the pyramid - large market size and potential future customer prospect

Adam What are the pitfalls to microfinance to be aware of if your organization is considering investment in microfinance?

Massimo Although there is a proven record of investments in MFIs which yielded important returns both from social and profitability angles, the risks and possible issues which characterize this industry need to be carefully assessed. Compared to mainstream finance, microfinance presents a better diversification of assets, due to the very small average loan size, which mitigates the credit risk stemming from the lack of collateral. At the same time, MFIs generally only lend to microenterprises which are not linked to the mainstream financial market and therefore less affected by a major financial crisis. It has, therefore, happened in many cases that while a country's financial sector was suffering from a recession due to external or internal factors, there was little to no impact on the microfinance industry. These and several other elements ensure that MFIs have on average lower levels of NPL than banks and other mainstream financial institutions.

On the other end, MFIs are generally more vulnerable to political interference. As MFIs have usually a large number of clients who are characterized by low education and can be easily influenced, they often become the target of politicians trying to get votes, especially during elections. There have been many cases of local politicians waiving loans of MFIs or forbidding loan officers to collect installments in villages in exchange for votes or consensus. In some cases, such as in Andhra Pradesh in India, such initiatives have led to the collapse of the microfinance industry in entire states or in a country, creating huge damage to MFIs, clients and investors.

At the same time, the microfinance industry suffers in many countries from a chronic lack of proper regulation. In fact, often the governments do not have a proper understanding of how MFIs operate and especially of their cost/revenues structure which, because of the small size of their loans and labor intensive operations, entails higher rates of interest. Because of this lack of understanding, MFIs are often overly regulated with laws which include tight caps on interest rates or on margins. This forces MFIs to gradually lend higher amounts and drift away from the micro to the SME segment. There are also cases in which the MF sector is instead very poorly regulated and supervised, and informal MFIs are allowed to expand with no rules, charging overly high interest rates or offering loans without restriction. Although in the short term this is conducive to fast growth of the industry, in the long term it can cause overlending, high delinquency rate, and eventually the intervention of the regulator or the government to curb the sector.

In order to mitigate the political and regulatory risks mentioned above, it is important that the sector invests in a strong microfinance association which self-regulates MFIs and pushes them to adopt best practices in terms of client protection, avoidance of overlending, and lobbying with supervisors and the government for the adoption of well-balanced regulation.

Another major issue is related to the investors themselves. Often, as investors are convinced to pay high valuations to hold a participation in MFIs, once invested they push for short term growth and profitability objectives to quickly recover the investment made and start generating returns. This forces MFIs to cut corners in order to achieve unrealistic targets and in turn triggers a worsening of the portfolio quality not only of the invested MFI but of all the sector. Hence, investors need to take an important part in the process of making the MF industry virtuous, ensuring the price they pay and returns they expect are well balanced and requesting their investees to seek long term double bottom line objectives.

Adam Are there disruptors in microfinance that you or the industry are monitoring?

Massimo Just to mention some of them:

- Companies offering credit based on mobile phone data (digital lending model)
- Tech / ecommerce companies entering this space (e.g., in Asia Go-Jek, Grab, Ola) and P2P (peer to peer) / online lenders
- SME focused FinTech leveraging data analytics to assess and underwrite customers

Adam Thank you for your time, Massimo.

Massimo Vita

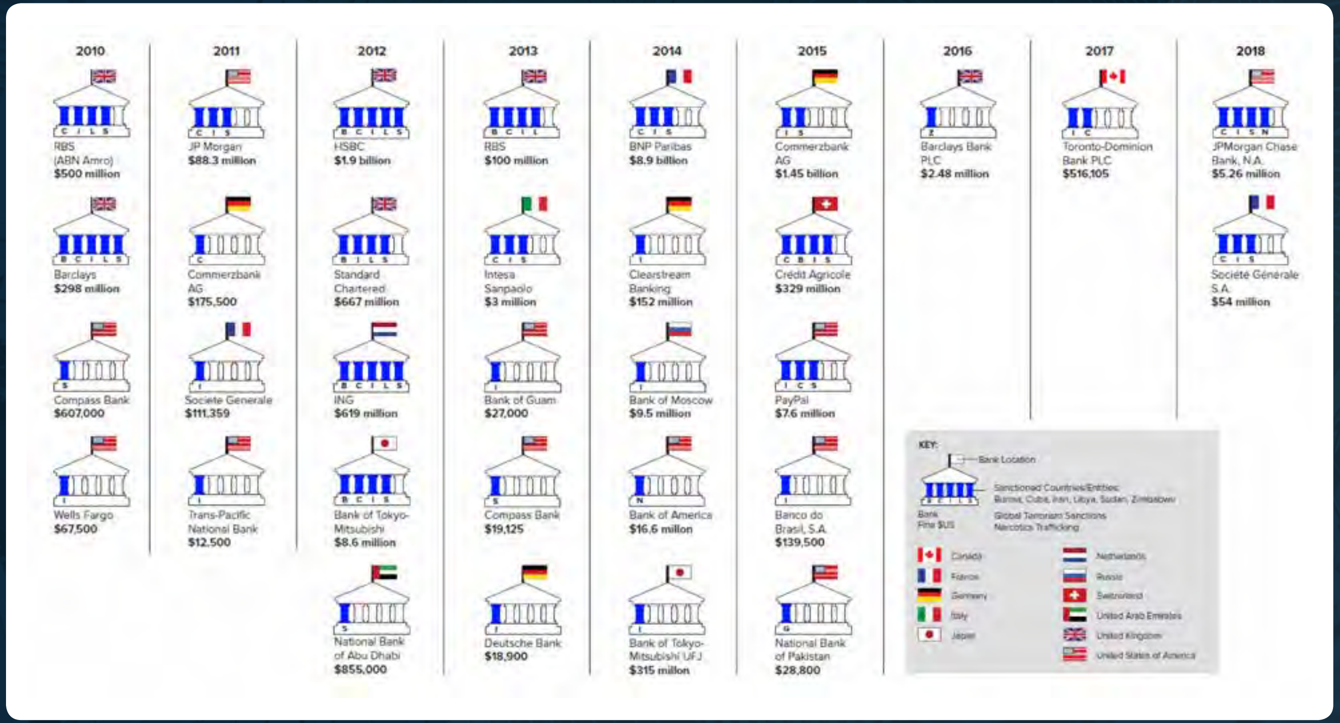
Chair of the RIM Steering Committee

the low hanging fruits to mitigate regulatory risks for banks

by **Vikram** Nath

A 2018 study[1] conducted by Fenergo, a provider of Client Lifecycle Management solutions, estimated that a staggering $26 billion in fines has been imposed for non-compliance with Anti-Money Laundering ("AML"), Know Your Customer ("KYC") and sanctions regulations in the past 10 years. The US accounts for about 44% of all global regulatory AML/KYC fines translating to over 90% of the total value. Another study[2] conducted by REFINITV (Financial & Risk business of Thomson Reuters) found that there were 32 instances (see the infographics below) of fines imposed on various global financial institutions between 2010 and 2018. The fines ranged between several thousand dollars to $8.9 billion (BNP Paribas in 2014[3]).

Fines for banks that breached U.S. OFAC sanctions



Source: Thomson Reuters – https://www.refinitiv.com/en/resources/infographics/fines-banks-breached-us-sanctions/

While the above challenges pertaining to KYC/AML regulations is enough to cause a dent in the viability of a bank, they are but one of the many other challenges banks face in current times. In the aftermath of the financial crisis, regulators all over the world (more so in developed countries) have come up with a plethora of regulations to avoid a repeat of the crisis in the future e.g. Dodd-Frank Act, Volcker Rule, European Markets and Infrastructure Regulation ("EMIR") and last but not the least – Basel III and Basel IV Accords. Readers looking for a summary and impact of Basel III/IV changes can refer to an article[4] - Basel IV – Profound Changes in Banking Regulations on the Horizon.

An obvious pathway for banks facing so many regulatory challenges is to invest deeply in its workforce and hire more control and compliance staff. Additionally, huge IT infrastructure investments should be made to make sure that the banks systems are in-sync with the current demands from the regulators. This would help demonstrate the regulators about an organizations' commitment to meet the regulatory obligations during an audit. While it is undeniable that an organization would need to incur these costs, there are some low cost and easy to monitor ways to mitigate the regulatory burden and avoid monetary penalties. This article discusses some of these preventable and employable measures below:

1. **Monitoring of all regulatory trainings and ensuring that the employees complete their assigned trainings before the deadline**

   During an audit, the regulators may seek a log of the organization wide trainings and the rate of compliance (i.e. whether its employees completed the training prior to the prescribed deadline). Needless to say a high level of compliance would indicate a high level of motivation from the employees to meet current regulatory requirements. A high level of compliance would also mean that a bank is committed to enforce a strict training program on its employees.

2. **Clearly documented policy and procedures that are easily accessible by all employees**

   A review of banks policy and procedures is one of the first evidence that a regulator may ask during an audit. Besides, these documents must be placed preferably on corporate intranet so that they are easily accessible by the banks employees. For each of those documents, a strict versioning log must be included in the document reflecting the date of any change and which team or individual performed that change.

3. **Regular updates to policy and procedures while keeping employees informed about such updates:**

   In the current regulatory environment, change is constant. As such, the policies and procedures should be updated on a regular basis to keep them current with the applicable regulations. In addition, adequate communications must be made to let employees know of these updates.

4. **Timeliness in completing Periodic Reviews of Bank's customers (read Borrowers) including collateral appraisal and revaluation:**

   Another easy way for banks to curb an unwanted increase in its cost of capital is to ensure that all the periodic reviews of ratings and LGD (Loss Given Default) so that these don't get defaulted to a penalty rate. The ratings represent the probability of default and higher probability of default results in a bank incurring higher capital charges. Likewise, LGDs determine a banks loss if the borrower defaults. A higher LGD would always result in a higher cost of capital. Typically both the rating and LGD should be reviewed once a year at the least. If these are not reviewed in time, these then default to more penalizing values thereby resulting the bank to incur higher capital charges.

5. **Supporting IT infrastructure to ensure compliance with internal procedures and processes. Making sure that systems talk to each other as isolated systems are risk vulnerabilities:**

   The banks should make sure that the IT infrastructure of the banks are state-of-the-art and are up-to-date with applicable processes and procedures. The banks systems should be able to communicate to each other for a good risk monitoring. For example, the ratings system of the bank should be able to communicate directly with the trading platform as well as the loan servicing platform. This would alert a trader or a loan servicer if he or she should not trade due to an expired rating or an LGD. At the very least, such communications would prompt the trader or loan servicer to request the respective team to update such rating and LGDs.

references

1. https://www.fenergo.com/lookbook/webinar-on-demand-global-aml-and-sanctions-fines.html?alild=5121997

2. https://www.refinitiv.com/en/resources/infographics/fines-banks-breached-us-sanctions

3. https://www.reuters.com/article/us-bnp-paribas-settlement-sentencing/bnp-paribas-sentenced-in-8-9-billion-accord-over-sanctions-violations-idUSKBN0NM41K20150501

4. https://issuu.com/prmia/docs/irisk_-_jan_2019_-_issuu

author

Vikram Nath

Works in the Houston, Texas, office of Natixis. Natixis is the corporate & investment banking ("CIB") arm of Group BPCE, one of the largest banking franchise in Europe. In Houston, Vikram supervises the oil and gas portfolio team that is responsible for managing a multi-billion dollar loan and commodity derivatives portfolio. Apart from portfolio management, Vikram specializes in Reserve Based Loan (RBL) financing in the energy upstream sector, midstream financing and acquisition financing within the energy space. Vikram has an MBA from Rice University, Houston as well as an engineering degree from Indian Institute of Technology (IIT) Delhi. Vikram is an avid golfer and loves to watch movies and TV shows in his free time. This article represents author's personal views and analysis and not that of his employer's views or positions on the subject.

strategic risk management and new digital tools are key to managing preventable compliance risks in financial institutions

by **Paul** van Warmelo

financial institutions care about preventable compliance risk management

Organizations classify risks as preventable risks when they are seen to provide no strategic benefit if accepted, like the compliance risk of financial crime, and tend to be mitigated or avoided. Strategic risks are those which offer a reward when taken on, like credit risk, which tend to be mitigated or accepted. External risks, as a third category, are those which an organisation tries to identify early to manage as they occur, like natural disasters, which tend to be accepted or transferred to insurers.

Financial Institutions face an increasing burden of compliance requirements, both locally and from globalization of business. This article will discuss why classification of compliance risks into strategic and preventable is in itself a risky decision, and how to address this risk with data management and smart analytics.

financial institutions apply a preventable risk approach to their complex and evolving compliance risk

Corporations operate under multiple obligations, including the legislation of the countries they operate in, regulatory requirements, social expectations and others. Clearly, the risk of not complying with obligations is a preventable risk, whether by avoiding risky operations or products, or by mitigating the risk through controls. However, recent financial institution scandals might show that the risk of not complying was treated as a risk to accept, a strategic risk. It is apparent that in some cases, organizations chose to accept the risk of non-compliance, without clear evidence of a mitigation control.

Perhaps this is because obligations change over time, within geographic or regulatory environments, as Financial Institutions enter new regions, or as they change their product mix and processes. Change is costly and takes time, and compliance controls are not always well understood or implemented.

why is compliance risk not managed well?

From a risk manager’s view, complete elimination of compliance risks may not be possible, owing to the operational risks inherent in the processes conceived to eliminate the risks, where operational risks include the risks of losses caused by people, processes or systems or from external events. So instead of managing the compliance risk itself, the author has seen that the management of compliance becomes the management of the controls used to ensure compliance. Because compliance risk is then not managed directly, senior management lacks the tools to mitigate compliance risk effectively.

Controls are evaluated as effective in design or effective in operation. Ineffective controls are then tolerated as long as there is a time-bound action plan to make them effective. And so, compliance risk is mitigated or accepted.

Other approaches include culturally reinforcing the social value of good corporate citizenship. Perhaps the recent fines and exposure of corporate greed, such as in the Australian Royal Commission into misconduct of banks and financial institutions shows that the “tone from the top” is more impactful than any corporate citizenship, vision statement or training. Addressing preventable compliance risks maybe needs a different or complementary approach.

financial institutions can learn to manage preventable compliance risks better from managing strategic risks

Compliance risks can evolve over time between Preventable Risks and Strategic Risks, for example customer best interests requirements. It is worth learning from the approaches used to manage strategic risks when managing preventable risks.

Extensive bodies of knowledge exist in support of strategic risk management, with well-understood ways to understand and test residual risks (the remaining risk after applying controls). These methods should be applied to compliance obligations, to understand the actual risk of non-compliance, in order to better match up the business’ risk tolerance and capability with the risk of non-compliance. Organizations are then able to proactively understand their risk of non-compliance and the pathways to compliance.

Senior leadership are then able to own this risk, and understand their organisation’s exposure to their compliance environment. This is valuable in Australia, for example, where senior leadership are being held personally responsible for compliance under the Banking Executive Accountability Regime (BEAR).

use new data, digital and analytics approaches

Basic compliance is achieved through the appropriate organisation of people implementing an adequate compliance governance framework. To retain and manage knowledge, larger and more complex organisations must systematise their compliance using data, metrics, dashboards and information management. By reflecting the real organisation in the virtual environment of systematised information, they are now able to take advantage of new digital tools and approaches to manage noncompliance.

Smart digital tools can now be used to digitally understand compliance obligations as they evolve, for example in Anti-Money Laundering (AML) and taxation. These tools can digitally evaluate not only the degree of compliance, but also the effectiveness of the compliance management framework and the risks of noncompliance.

As these tools improve over time, and become more commoditized, organizations will be expected by their regulators and shareholders to use their data flexibly and effectively to pre-empt noncompliance. They will expect sufficient digital control of preventable compliance risks, and formalised processes and knowledge management to address compliance obligations.

Senior management in financial institutions will be expected to make conscious active decisions on how they meet compliance obligations by the way that:

- Skilled personnel are strongly supported by smart software systems
- Data clearly supports the presentation of insights, which drive actions
- Data quality management is systematised and automated

author

Paul van Warmelo

Paul is responsible for leading the Risk Data and Analytics practice for Genpact consulting, Australia. Paul has 12+ years' experience in Financial Services and 20+ years in Risk Management. Paul is also a Reporting, Risk, Risk Capital and Financial Model expert in Banking, Financial Services, Corporate Treasury and Insurance. Paul has extensive experience in wealth management, banking and corporate treasury risk management – operational, interest rate, and foreign exchange risk. Paul also has process transformation experience and customer contact in a range of industries. He holds the PRM and FRM certifications, and the CFA and Professional Engineer charters.

the new European overnight rate – a complicated transition

by **Maximilian** Beckmann & **Andreas** Hock

the current situation

According to EU Benchmark Regulation (EU BMR 2016/1011), which has been in effect since 2018, only approved reference interest rates may be used for new business starting in 2020. Consequently EONIA, the current European overnight benchmark, will not be reformed since EMMI, its administrator, concluded that its compliance with the EU Benchmark Regulation could not be achieved under current market conditions.

In order to find an adequate successor rate, the ECB established a working group. In September 2018, the Euro Working Group recommended ESTER as the alternative, risk free interest rate (RFR) and replacement for EONIA. ESTER will be published beginning in October 2019.

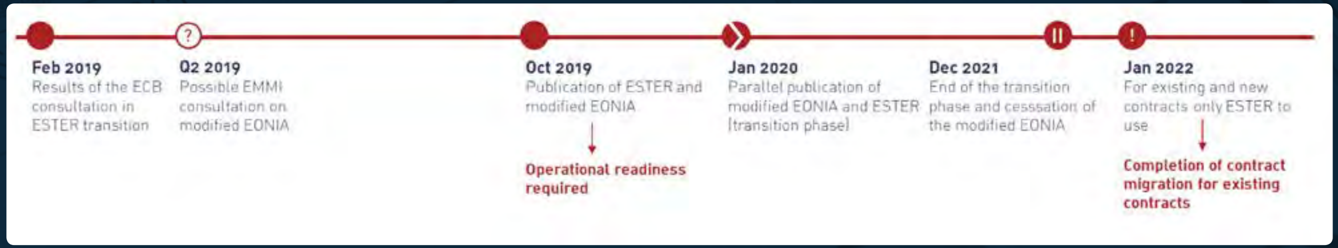
Due to the high relevance of EONIA, the objectives are to ensure a coordinated transition, prevent a market fragmentation and contribute to the creation of a liquid market for ESTER derivatives.

For a successful transition, compliance with regulatory deadlines is necessary. Moreover, the current liquidity from EONIA derivatives must be effectively transferred to ESTER, and users – especially those that are the least sophisticated – must be protected by reducing potential value transfers in the system. In addition, legal risks have to be avoided. Finally, transactions have to be operationally feasible and all accounting and risk management processing requirements have to be considered.

In late February, the Euro Working Group recommended the following approach: as of October 2019, EONIA will be redefined as ESTER plus a fixed spread (expected to be <10 bps) and be published until the end of 2021. Thus, EONIA will then comply with EU BMR and be eligible for new business

EMMI, as the benchmark administrator, now has to start the process of developing EONIA according to the Working Group's plan. A first step would be to have a public consultation on the "evolved" EONIA.

On February 25, 2019, in order to ensure financial stability, EU regulatory bodies agreed to grant administrators of "critical benchmarks" (e.g. EONIA, EURIBOR) two extra years until 31 December 2021 to comply with EU BMR. Even though this extension theoretically reduces implementation pressure, market participants expect that the Working Group's original plan will be carried out nevertheless.


Feb 2019
Results of the ECB consultation in ESTER transition
Q2 2019
Possible EMMI consultation on modified EONIA
Oct 2019
Publication of ESTER and modified EONIA
Operational readiness required
Jan 2020
Parallel publication of modified EONIA and ESTER [transition phase]
Dec 2021
End of the transition phase and cessation of the modified EONIA
Jan 2022
For existing and new contracts only ESTER to use
Completion of contract migration for existing contracts

challenges of implementing a parallel system

ESTER readiness will be required by October 2019. On the go-live date, banks' internal systems need to be able to process both curves simultaneously. In addition to that, ESTER is being quoted as T+1, whereas EONIA is being quoted T+0. Whether the new EONIA will be based on the preceding day-ESTER or also converted to T+1 is yet unclear, but very likely, which will affect the entire process chain.

In terms of IT systems, EONIA and ESTER contracts will coexist, which alleviates time pressure with respect to the transition. A basis risk between EONIA and ESTER will not be present due to the fixed spread. With the ESTER implementation, EONIA and ESTER curves will be connected by a deterministic spread. Therefore, all (algorithmic) valuation calculations can continue to take place. However, they need to be converted to ESTER at a suitable point in time. Thus, a validation of model parameters (market data and system configuration) will be necessary after the ESTER implementation.

EONIA transactions will still be able to be evaluated and processed. The desired implementation eases the situation in terms of fallback management and contract conversion. However, this approach also implies that transactions with regard to EONIA and ESTER have to be supported by the system in parallel, unless banks can reach an agreement beforehand in terms of a "big bang," meaning the simultaneous conversion of CSAs, cleared derivatives and EONIA-based products. However, most market participants consider this very unlikely.

Whether a single / dual discounting regime is sought is also still uncertain. For a substantial part, this will depend on the decision of the central counterparty (CCP). Nevertheless, a conversion of the CSAs should be sought as soon as possible, even if EONIA discounting / price aligning interest (PAI) is temporarily possible. As first calculations show, effects on the amount of the required collateral will be marginal. Once more, it is clear that an approach to CSAs needs to be identified.

conclusion

With the conversion of the reference interest rates, there is a need for action by every financial market participant. The expected transition from EONIA to ESTER at the beginning of October 2019 will stress the entire process chain. The challenges for the entire banking industry are substantial and intertwined. Action should start as soon as possible to cope with the major challenges.

authors

Maximilian Beckmann

Maximilian Beckmann is Managing Consultant at Lucht Probst Associates (LPA) GmbH. As a member of LPA's Consulting practice, he focuses on the intersection of regulation and technology, currently working on IBOR transition and KYC transformation. Prior to that Maximilian worked for a risk and capital management consulting boutique in Frankfurt and London.

Andreas Hock

Andreas Hock has been with LPA for more than 3 years and is part of LPA's IBOR Transition Practice Group. As a Managing Consultant in LPA's team Risk & Quant consulting team, he focuses on regulatory topics for market and counterparty risk as well as the valuation of financial instruments.

COP24 advances ESG commitments for EU banks and regulators

by Anna Reitman

In tackling climate change as a long-term risk, EU finance ministers are advancing European Banking Authority studies on mandatory ESG (Environmental, Social, Governance) disclosures for banks in three years and regulatory reporting requirements as part of "greening" financial flows in Europe at the 24th session of the Conference of the Parties, taking place in Poland.

Where is the financial industry at right now in being ready for this?

ETF and ETP flows help paint a picture of the market size: it's a growing area but small overall: net inflows were at almost $1.1 billion in October with total assets invested sitting at $21.9 billion, according to ETFGI research.

Small but mighty, however: year-to-date, ESG ETFs/ETPs assets have increased 25.9% compared to 2.5% for all ETFs/ETPs listed globally. BlackRock iShares, UBS, and BNP Paribas have the three largest by AuM in the market.

Results are also promising: research from Barclays going back nine years claims that high-ESG portfolios have outperformed in both US and euro investment grade credit markets. This was the case for two sources of ESG ratings considered, despite their differences in methodology and the relatively low correlations between their ratings. (The Financial Times has a fun, cynical take on this).

Principles for green bonds have been clarified by the International Capital Market Association, and some of the most vulnerable global regions are innovating: like the Seychelles Islands, which have launched sovereign"blue" bonds to protect oceans. There are of course numerous examples.

under pressure

COP24 is starting this week after a particularly bad year for climate change realities. The IPCC released a special report on what seems like the globe's inevitable path to 1.5 degree warming, having already passed 1 degree. The impacts are: greater intensity and frequency of extreme events on resources, ecosystems, biodiversity, food security, cities, tourism and carbon removal.

There's a good deal of pressure from society as people become sensitive to the ethical quality of a company, and it is impacting how investment works, said Bruno Dupire, head of Quantitative Research at Bloomberg L.P., speaking at Hebrew University on a panel about the future of options.

Speaking to Fintech Capital Markets on the sidelines of the conference, he clarified that the generation known as Millennials (ages 22 to 37) is backing a major push for ethical investment, and fund managers, as well as sovereign wealth funds, are ready to be activist.

This also impacts the future of derivatives, Dupire said on the panel, which is to stop creating complicated products and instead create products that apply to realities more relevant for corporations' and an individual's "longevity".

As an example, he discussed the risk faced by individuals of living past their savings: "What financing should generally do is create products that are adapted to the situations…like annuities (that) have payments that really accompany your needs. It should be an alignment of asset-liabilities," he said.

insuring doom

There's a well-worn adage that climate is what you expect, and weather is what you get. And while insurers have been covering weather since time immemorial, the industry is paying a lot more attention to climate.

The economic impact of weather is profound and ubiquitous at a time when the insurance business is barely past its annus horribilis in 2017, said a panelist speaking at a recent PRMIA (Professional Risk Managers' International Association) event.*

2017 tallied up the highest insured losses ever, according to data from MunichRe, when a series of hurricanes put the final insurance bill for those and other natural catastrophes, including a severe earthquake in Mexico, at some $135 billion. And overall losses – including uninsured losses – amounted to $330 billion, the second-highest figure ever recorded for natural disasters. The only costlier year so far was 2011, when the Tohoku earthquake in Japan contributed to overall losses of $354 billion in today's dollars.

Meanwhile, there's no end in sight: "Insured events are going off the scale…so it matters to sellers of protection for that risk." What this means is that insurers have had to figure out what resilience is required for "tail climate risk", and this experience is what they bring to the table now: the metrics, measuring and modeling of such risks.

Still, while the insurance industry is great at managing liability-side risks, there is a disconnect from the asset side: "Where the knowledge, skill, data and modeling exist for the very immediate purposes of the liability side of the business, it is not necessarily conveying itself in the same format in the same way to the asset management side of the business," said one panelist.

It should be noted, however, that the financial industry is facing a reporting burden.

*Event held under Chatham House Rule

who's reporting now?

Sustainability reporting has reached the Financial Stability Board as part of the TCFD (Taskforce on Climate-Related Financial Disclosures), which encourages companies to disclose specific metrics used to assess "risks and opportunities in line with its strategy and risk management process", according to TCFD.

This is not just to make the world a better place, global supervisors and authorities are recognizing that climate change poses systemic risk. The latest status report showed that hundreds of companies are trying to make it work, while in France, it is a legal requirement.

In that report's opening comments to FSB chair and Bank of England governor Mark Carney, Michael Bloomberg, founder of the eponymous firm, said that more than 500 public and private sector organizations have indicated support, including global companies, banks, insurers, asset managers, stock exchanges, and governments, while acknowledging that there's yet much work ahead.

Some of that has to do with mindset: some 60% of banks identified climate change as a short-term risk, and only 10% view it from a strategic, long-term perspective, said a panelist referencing FSB data.

It seems that only a handful of banks have started their first TCFD disclosures, with UBS being noted for providing a view of carbon assets in their exposure and looking to develop metrics, and there are indications that many banks will consider climate stress tests. But for the majority, disclosures are qualitative rather than quantitative, for now. And ESG standard audits don't exist.

So, where does FinTech fit in? One example provided by a panelist had to do with a fintech figuring out how to provide invoice financing for sustainable tea farming in Malawi, while also tracking products to ensure a sustainable supply chain. Blockchain was mentioned as part of that model.

FinTech was also noted for its contribution to data gathering in general, while other mentions were all data-driven: included artificial intelligence, wearable technology, drones, advanced sentiment technology, and satellites.

At the same time, it was pointed out that FinTech itself is under the gun: "The FinTech of sustainability is not the same as the sustainability of FinTech."

Originally published on Fintech Capital Markets, a Finadium publication.

Fintech Capital Markets

author

Anna Reitman

Anna Reitman is the editor of Fintech Capital Markets, a publication by research and consulting firm Finadium. Finadium's core practices relate to securities finance, collateral and derivatives, and the application of emerging technologies in capital markets.

2019 PRM™ program design

by **Mary** Rehm

Over the last year, the Professional Risk Manager (PRM™) Designation program has been in a redesign effort based on the findings from the 2017 job analysis study[1]. From the study results, the Education Committee approved the inclusion of several new topics to the PRM syllabus and a redesign of the exam program.

how were topics identified for inclusion into the 2019 syllabus?

In order for a professional certification program to be valid, there must be evidence that what is being assessed by its examination program is critical to the job or role the credential represents. The examination program must measure those topics that are important for the professional to possess in order to be successful and there must be evidence that those skills are consistently applied in that role.

Respondents to the job analysis survey were asked to rate each major topic within the PRM Designation program on the importance of the topic in the person's role as a risk manager and how frequently knowledge of that topic is applied in that role.

The following questions were posed to the respondents:

How important are the following topics in your current role?

(1) Not important
(2) Somewhat important
(3) Important
(4) Very important
(5) Critical

How frequently do you use knowledge of that topic in this role?

(1) Never
(2) Annually
(3) Monthly
(4) Weekly
(5) Daily

Average ratings were compared to a benchmark rating to determine whether the topic should be included in the updated syllabus. Any topic with an average rating greater than 2.49 (important and used monthly) was included in the syllabus. Topics with an average rating between 1.49 and 2.49 were discussed for inclusion by the test specifications committee. Topics in this range may be somewhat important to respondents or seldomly applied, but the committee may determine that the topic is very important to the role of the risk manager and justify the inclusion in the syllabus.

[1] / For more information on the job analysis study and its initial findings, see the May and October 2017 Intelligent Risk publications.

Any topic with an average rating below 1.49 was not included because when these topics are marked as "not important" or "never" used by respondents, there is evidence that these are not critical to the success of that person in their role as a professional risk manager.

how were demographics used to identify core PRM experience requirements?

The job analysis survey included several demographic survey items intended to provide input into the current population of PRM Holders and their level of competency, work experience and job role, and educational levels. These data were used to validate the current set of experience requirements.

- 75% of respondents completed a Master's degree level education or higher
- 19% of respondents have worked in the risk profession for 3-5 years and 36% for 6-10 years
- 84% of respondents work as regular, full-time employees
- 56% of respondents describe their current career track as a risk manager as "experienced" or "advanced"

Given the demographics, the test specifications committee found that it was not necessary to adjust the application requirements for the program – applicants to the PRM Designation are required to hold a Master's degree, or a Bachelor's degree with two years of full-time work experience. If the applicant does not hold a degree, four years of full-time work experience is required.

how were the new PRM syllabus statements crafted?

The test specifications participants spent a lot of time re-organizing the topics for the syllabus and re-crafting the syllabus statements to make the objectives clear for candidates. Unlike the prior syllabus which listed the topics, the 2019 syllabus describes the knowledge or skill that will be assessed for the core competencies of the Professional Risk Manager.

The syllabus statements in the 2019 program are written using Bloom's 2001 Taxonomy for Learning[2] where specific verbs indicate the level of knowledge and skill expected of candidates for that area of the syllabus. Download the PRM Candidate Guidebook from www.prmia.org/PRM to learn more about how this taxonomy can be used to better understand the competencies assessed in the exam program.

[2] / Anderson, Lorin W.; Krathwohl, David R.; Bloom, Benjamin S. (2001) A taxonomy for learning, teaching, and assessing: a revision of Bloom's taxonomy of educational objectives. New York: Longman. ISBN 0321084055; 080131903X

how was the PRM examination program redesigned?

The 2019 PRM exam program includes two required examinations, versus the four exams required with the 2015 exam program. After examining test time data and the number of questions included in the new exam program structure, the test specifications committee agreed that the testing process could be made more efficient by combining topics into a common exam.

The 2019 PRM Exam 1 assesses knowledge of the domains related to finance theory, instruments, markets, and the application of mathematical foundations of risk measurement. These topics were tested before in the 2015 PRM exams I and II.

The 2019 PRM Exam 2 assesses the knowledge of the domains related to risk management frameworks, asset liability management, funds transfer pricing, the specific risk areas of operational risk, credit risk, counterparty credit risk, and market risk, as well as the PRMIA Standards and Governance. These topics were tested before in the 2015 PRM exams III and IV.

The 2019 PRM Exam 2 includes a practicum assessment that assesses the ability to apply lessons learned from the PRMIA case studies using knowledge from across the PRM syllabus. The practicum portion of the exam will include 4 sets of 5 multiple choice questions, each set related to a specific scenario from a PRMIA case study.

For complete details on how the exam structure will change and how each of the domains in the 2019 syllabus will be assessed, download the PRM Candidate Guidebook from www.prmia.org/PRM.

what comes next?

The PRMIA Education Committee will now turn their attention to developing a new edition of the Professional Risk Managers' Handbook and further developing the PRMIA case study library. The next edition of the PRM Handbook volume set will first be published digitally, with print versions becoming available later.

You can expect to see new case studies published beginning in July 2019 and published each quarter over the next few years. Individuals studying for the 2019 PRM exams will be provided ample time to read and review the content of the case studies before these cases are included in the formal examination.

what impact can current PRM Designation candidates expect for their path to certification?

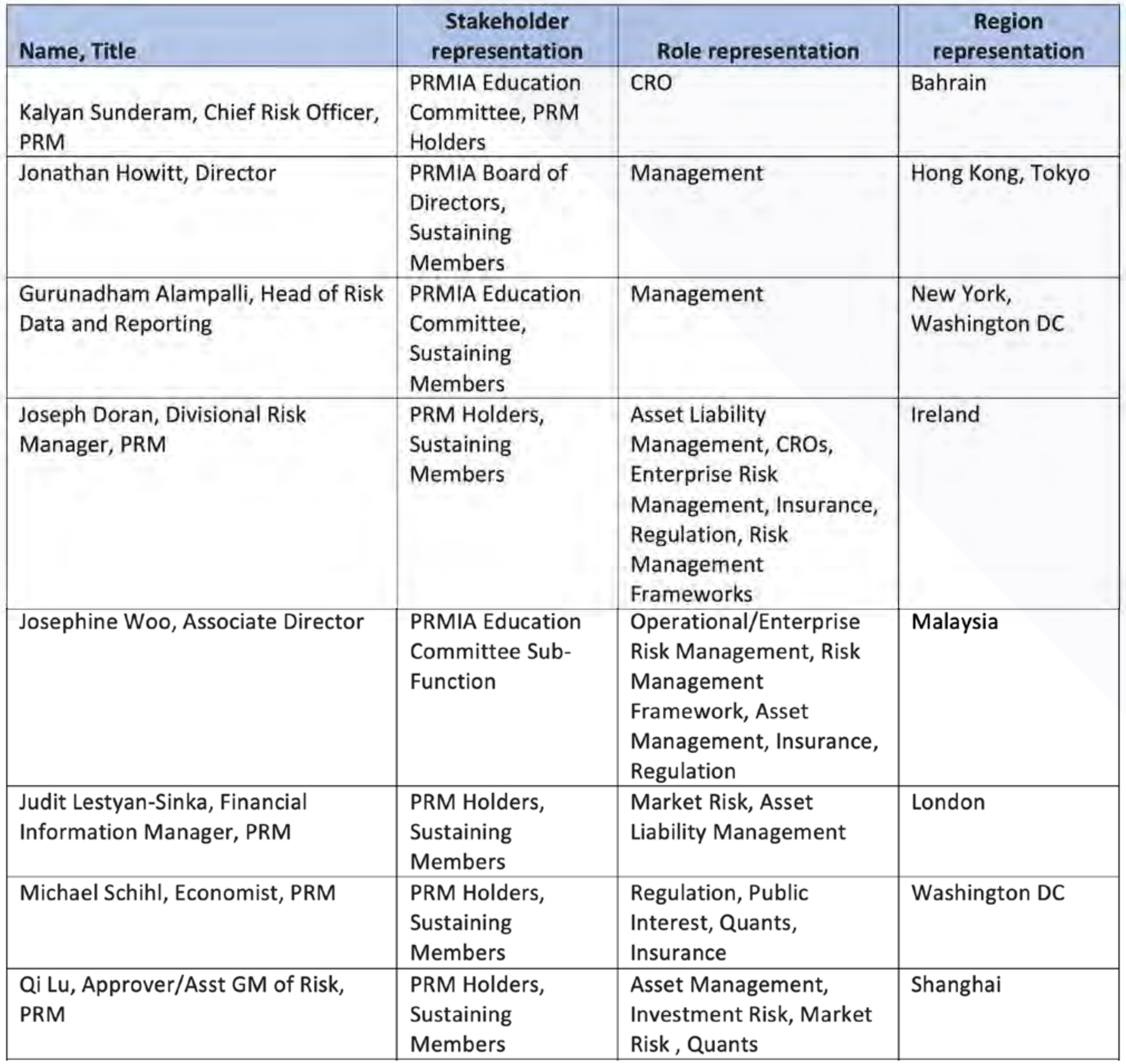
Candidates currently working to achieve certification should continue. The 2015 exam program will remain available for testing through June 2020. Any individual who still needs to meet their exam requirements will be transitioned into the 2019 exam program after June 2020.

For complete details on the transition period and the impact for current PRM candidates, please visit the PRM Transition webpage at www.prmia.org/PRM

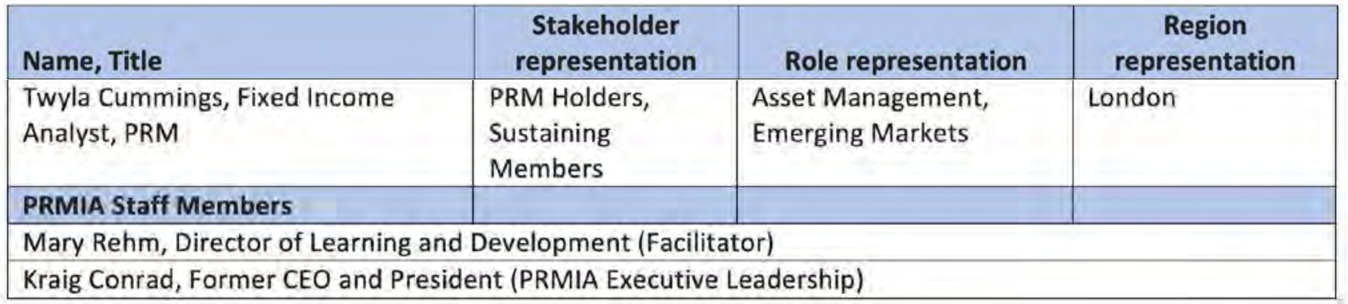
thank you to the PRM Test Specifications Working Group

The following individuals participated in the test specifications working group. These professionals were recruited to participate as representatives of specific roles, regions, and stakeholder groups within the PRMIA membership.

Their time and expertise were invaluable in the success of this study of the PRM Designation.



Name, Title	Stakeholder representation	Role representation	Region representation
Kalyan Sunderam, Chief Risk Officer, PRM	PRMIA Education Committee, PRM Holders	CRO	Bahrain
Jonathan Howitt, Director	PRMIA Board of Directors, Sustaining Members	Management	Hong Kong, Tokyo
Gurunadham Alampalli, Head of Risk Data and Reporting	PRMIA Education Committee, Sustaining Members	Management	New York, Washington DC
Joseph Doran, Divisional Risk Manager, PRM	PRM Holders, Sustaining Members	Asset Liability Management, CROs, Enterprise Risk Management, Insurance, Regulation, Risk Management Frameworks	Ireland
Josephine Woo, Associate Director	PRMIA Education Committee Sub-Function	Operational/Enterprise Risk Management, Risk Management Framework, Asset Management, Insurance, Regulation	**Malaysia**
Judit Lestyan-Sinka, Financial Information Manager, PRM	PRM Holders, Sustaining Members	Market Risk, Asset Liability Management	London
Michael Schihl, Economist, PRM	PRM Holders, Sustaining Members	Regulation, Public Interest, Quants, Insurance	Washington DC
Qi Lu, Approver/Asst GM of Risk, PRM	PRM Holders, Sustaining Members	Asset Management, Investment Risk, Market Risk , Quants	Shanghai



Name, Title	Stakeholder representation	Role representation	Region representation
Twyla Cummings, Fixed Income Analyst, PRM	PRM Holders, Sustaining Members	Asset Management, Emerging Markets	London
PRMIA Staff Members			
Mary Rehm, Director of Learning and Development (Facilitator)			
Kraig Conrad, Former CEO and President (PRMIA Executive Leadership)			

author

Mary Rehm

PRMIA Director of Learning and Development

the riskiness of current IT security risk management

by **Frederick** R. Doyle

lots of solutions, little progress

Judging by the number of exhibitors – 592 – offering IT security services or products at the RSA 2018 security conference, there is no shortage of potential solutions to IT security. Similarly, there is no industry-wide shortage of funding for IT security solutions: Gartner projects that the 2019 IT security market will increase 12.4% to $124B, up from $114B in 2018. Yet there has not been a corresponding diminution in the frequency or magnitude of IT security breaches. Indeed, the influx of new security offerings has done little more than maintain the status quo, because the security industry is interested mostly in mitigating threats and not managing preventable risks.

it risk definitions lack units of measurement

As an IT professional with over 30 years of experience, I have watched the IT industry struggle with vulnerabilities and threats of all types. I have also witnessed IT professionals struggle with the concept of risk, much less a mathematical definition of risk.

The definition of risk in PRMIA's PRM Handbook is elegant in its simplicity, simultaneously capturing the mathematical essence of what risk is. While we calculate risk in many ways to leverage available data, we can always represent risk consistent with PRMIA's risk definition:

Risk is the probability of an adverse occurrence multiplied by the impact of that adverse occurrence.

Compare PRMIA's definition to just a few of the risk definitions used throughout IT security:

ISACA Enhanced Risk for Vulnerabilities[1]
Risk = Criticality (Likelihood × Vulnerability Scores [CVSS]) × Impact

Rapid 7[2]
Risk = (threat x vulnerability (exploit likelihood x exploit impact) x asset value) - security controls

FAIR[3]
Risk is the probable frequency and probable magnitude of future loss.

NSA and CIA (Hayden)[4]
Risk = threat x vulnerability x consequence

RMIA's definition captures the probability of a potential impact. As probability has no standard unit of measurement, risk must use the unit of measurement of the potential impact – dollars, records, lives, widgets, etc. But in most of the IT security risk definitions, respect for units of measurement is non-existent. Where is the unit of measurement for a threat, vulnerability, criticality, or vulnerability score? And in the case of the FAIR definition, it dilutes the calculation of risk by using two probabilities – the probable frequency and the probable loss – in its calculations. It is no wonder that most presentations of IT security risk are qualitative rather than quantitative.

heat maps – of questionable value

In IT security risk, "heat maps" rule. To obfuscate the fact that they have a deficient understanding of risk, IT security professionals typically use vaunted "heat maps" as their risk communication tool. For example, for each identified threat and impact pair, they identify the likelihood and impact based on an arbitrary scale (in this case minimal to extreme) and then plot the results on a color-coded grid to represent the intersection of the probability and impact. Figure 1 below is an example of a typical heat map with six arbitrary threat-impact pairs:

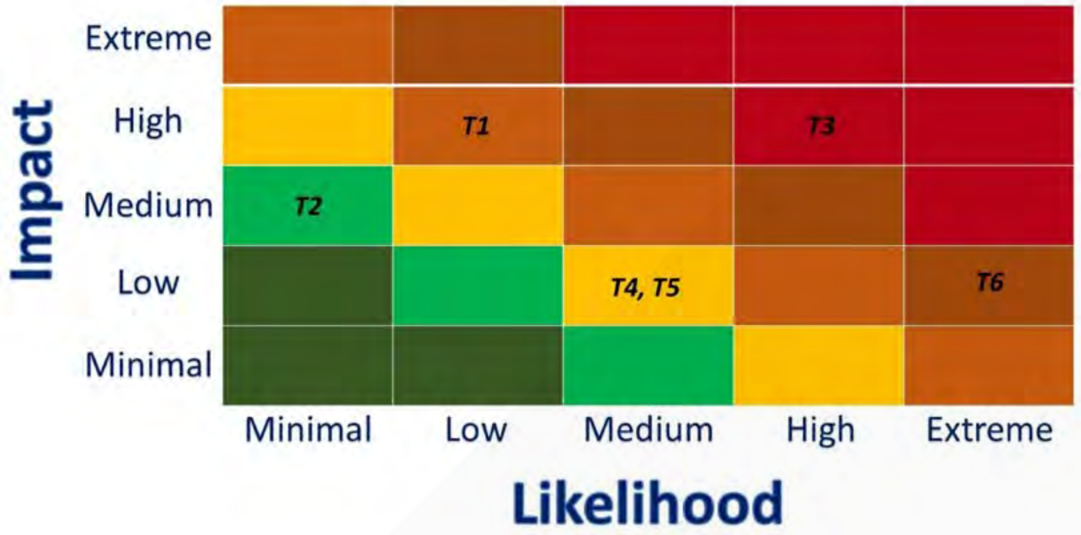


Figure 1 - Typical IT Security Risk Representation

From an IT Security perspective, it appears that the risk analysis is complete. But from a risk manager's view, the heat map is of questionable value. There are no quantitative elements to algorithmically model risk reduction. There is no way to obtain an aggregate risk from the data as displayed on the heat map. And, while it may serve to prioritize IT security actions, there is no way to measure whether those actions are indeed most effective to reduce overall IT security risk.

[1] / https://www.isaca.org/Journal/archives/2014/Volume-4/Pages/JOnline-An-Enhanced-Risk-Formula-for-Software-Security-Vulnerabilities.aspx

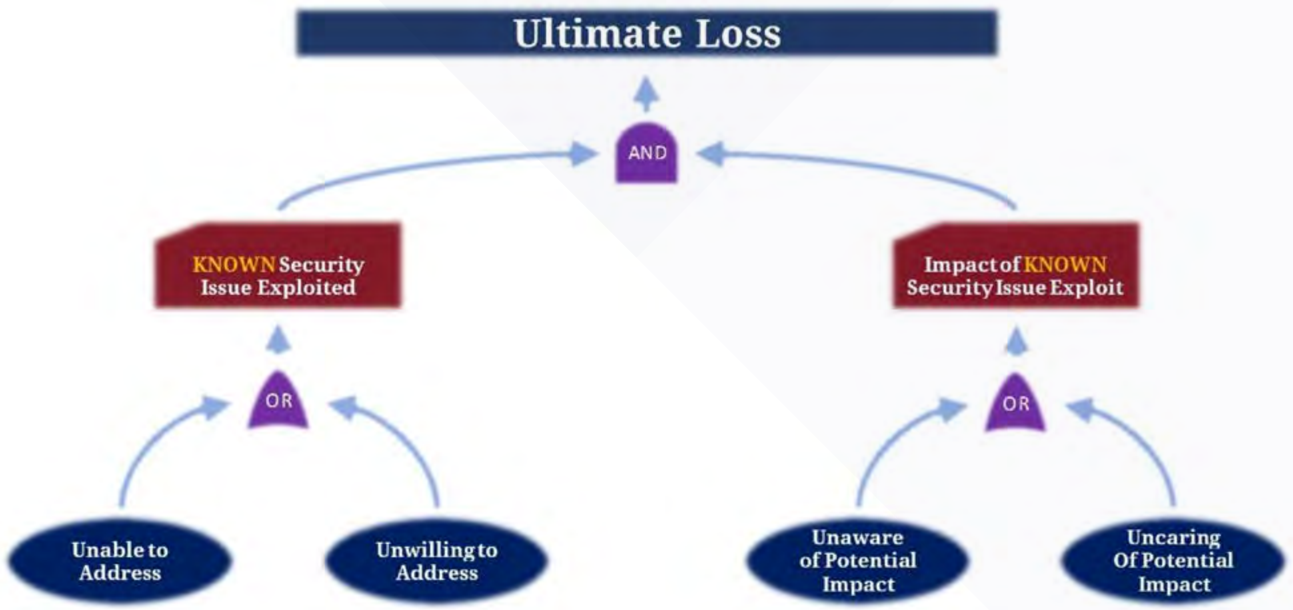
[2] / https://www.rapid7.com/fundamentals/information-security-risk-management/

[3] / http://pubs.opengroup.org/onlinepubs/9699919899/toc.pdf

[4] / https://www.isaca.org/Journal/archives/2014/Volume-4/Pages/JOnline-An-Enhanced-Risk-Formula-for-Software-Security-Vulnerabilities.aspx

fault-tree analysis of past breaches

Because IT security professionals focus on threats and not risks, they rarely consider the magnitude of the breach when conducting their root-cause analysis of a security breach. By applying Fault-tree Analysis (FTA) to several major IT security breaches over the last several years, I was able to show that all major breaches resulted from a failure of risk management, and not a failure of IT security. The FTAs of all the examined breaches, for example, take the form illustrated in Figure 2:



Ultimate Loss
AND
KNOWN Security Issue Exploited
Impact of KNOWN Security Issue Exploit
OR
OR
Unable to Address
Unwilling to Address
Unaware of Potential Impact
Uncaring Of Potential Impact

Figure 2 - Generic Fault-tree Analysis of Studied Breaches

In all studied breaches, a fundamental ignorance of the consequence of a successful breach led IT security professionals to apply resources to the wrong threat. A quantitative, risk-based approach to resource allocation would have prevented or minimized the extent of the breach.

conclusion

IT Security is a complex operational domain that requires an expertise in identifying and mitigating threats to information technology – the tools that are so vital to corporate operations and productivity. IT security expertise does not, however, include expertise in risk management – as evidenced by current IT approaches to risk – so it must fall upon risk management personnel to educate IT security professionals in extracting the risk elements required for true financial risk management from their operational data. The data is there, and until they are able to do that, IT security will remain a risky, non-preventable risk.

author

Frederick R. Doyle

Frederick R. Doyle is the Founder and CEO of CubicPrism Enterprises, an IT security and risk consulting firm. Frederick is also the inventor of risk-based decision support platform called RiskPrism®. Frederick was formerly the Director of Special Projects at iSIGHT Partners and FireEye from 2014 through 2016 and was Director of Technical Intelligence at iSIGHT Partners from 2008 through 2014. From 2006 through 2008, Frederick was the Director of the Verisign Vulnerability Research labs, and from 2002 to 2006, he was a malware analyst for iDefense. From 1994 to 2002, he ran a computer consulting firm and retail computer store.

preventing operational risks in organizations: a multi-faceted approach

by Vivek Seth

While Operational Risk is a broad risk discipline, it is essentially the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events.[1] Although such preventable risks should be avoided, these undesirable risks cannot be completely eliminated due to practical reasons such as human oversight, cost considerations and inherent risk of doing business. At the same time, organizations should always keep a close watch on Key Risk Indicators on its client engagement activities, business operations, and IT infrastructure to ensure that the impact of materialization of risks that can cause large scale strategic, financial, and reputational risk disruptions are limited.

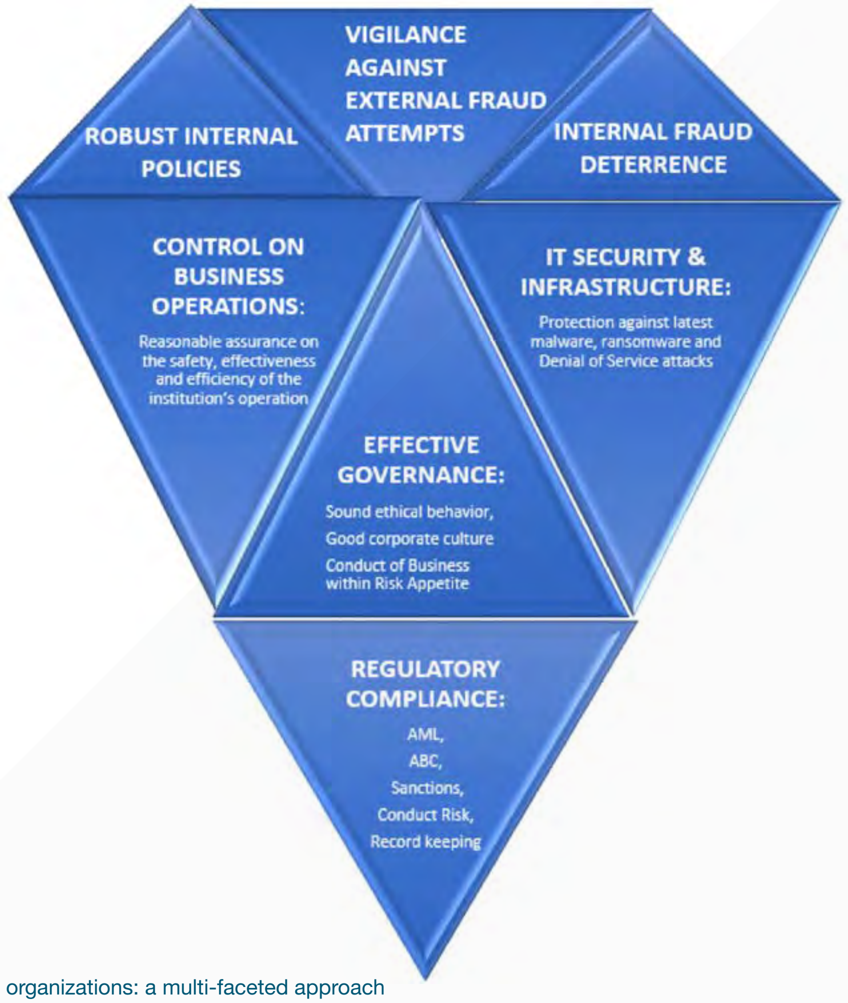
Over the years, corporations worldwide have witnessed the downside impacts when lapses occur in operational risk management. Such was the case observed in LIBOR scandal where control failures to timely detect fraudulent actions with regards to manipulation of London Interbank Offered Rate resulted in global banks being fined over $9 billion by regulators.[2] Toyota's global safety recalls in previous years affecting millions of cars have been estimated to cost $5 billion, taking into consideration lost opportunity, litigation costs and marketing efforts.[3] Such financial & reputation losses can also occur due to large scale internal collusion, fraudulent and unethical behaviors as observed in the case of Theranos, which made false claims of its revolutionary blood testing technology. With a $9 billion valuation at its peak in 2014, Theranos faced a string of legal and commercial challenges due to false statements made about the company's technology, business, and financial performance and finally ceased operations in September 2018.[4]

Managing operational risk is crucial to the firm's long-term viability to focus on their core business strategy, manage their prestige and avoid undesirable time spent in addressing regulators, customers and public media in the event of such risks. A key component of maintaining a robust Operational Risk Management Framework include having a vigilant oversight on following aspects:

Effective Governance: Ensuring sound risk management and ethical behavior in an organization is largely determined by how Board and Senior Management operate and emphasize good governance as they are entrusted to be the custodians of good corporate culture. The top executives should oversee that the design and operation of the institution's business processes are in line with long-term strategic objectives, financial soundness and firm's corporate values.

Such good governance should be implemented via periodic formal engagement forums to timely address issues on areas such as conflicts of interests, conduct risk management and excessive risk-taking behavior. While delegation on running institutions', day-to-day operations may be required, it should be understood that the Board & Senior Management set the tone on risk appetite framework and corporate risk profile and bear the overall responsibility for corporations' compliance with approved policies, regulations and industry's prudent practices.

Regulatory & Internal Policy Compliance: Corporations should ensure, as part of their daily operations and client engagement, applicable regulatory requirements are met with full adherence, including key obligations on complying with Anti-Money Laundering, Sanctions, Anti-Bribery & Corruption, Conduct Risk management and Record keeping requirements. The regulatory body should be notified in advance or upon discovery of any strategic changes in the institution's business activities, material adverse developments or breach of legal obligations that could negatively impact the firm's customers and shareholders. In addition, organization should stringently comply to regulatory periodic submissions including timely reporting of the institution's exposures such as credit, market, liquidity, country and interest rate reporting. Organization should also have independent functions like Compliance, Audit and Risk departments to implement internal policy framework and industry best practices.


VIGILANCE AGAINST EXTERNAL FRAUD ATTEMPTS
ROBUST INTERNAL POLICIES
INTERNAL FRAUD DETERRENCE
CONTROL ON BUSINESS OPERATIONS:
Reasonable assurance on the safety, effectiveness and efficiency of the institution's operation
IT SECURITY & INFRASTRUCTURE:
Protection against latest malware, ransomware and Denial of Service attacks
EFFECTIVE GOVERNANCE:
Sound ethical behavior,
Good corporate culture
Conduct of Business within Risk Appetite
REGULATORY COMPLIANCE:
AML,
ABC,
Sanctions,
Conduct Risk,
Record keeping

Preventing operational risk in organizations: a multi-faceted approach

[1] / Basel Committee on Banking Supervision, "Principles for the Sound Management of Operational Risk" (link)

[2] / The Council on Foreign Relations (CFR), "Understanding the Libor Scandal" (link)

[3] / The Wall Street Journal, "Toyota's Recall Costs Could Top $5 Billion"(link)

[4] / https://phys.org, "Theranos collapse offers three big lessons for companies", June 18, 2018 (link)

Controls on Business Operations: A system of strong internal controls is fundamental to the safe and sound management of institutions. Internal controls essentially provide reasonable assurance on the safety, effectiveness and efficiency of the institution's operation and reliability of financial and managerial reporting. Robust internal control framework keeps a check against risks associated with key processes such as Transactions Processing, Accounting & Record Keeping, Staff Recruitment & Training, Client Complaint Handling, Outsourcing, and Business Continuity activities. Effective internal controls help an institution to protect and enhance shareholders' value and reduce the possibility of unexpected losses or damage to its reputation.

Checks against Internal & External Fraud: As part of conducting business, firms need to proactively manage external fraud attempts by malicious attackers aimed at gaining financial, customer and internal information. Such attacks could include fraudulent email instructions requesting release of funds, forged documentations, social engineering attempts and cybersecurity attacks. Additionally, an organization needs to recognize that its confidential information, client data and personnel statistics can be misused by company staff, both accidentally and intentionally. In an age where job retrenchments and reorganization are becoming standard work phenomenon, the risk of disgruntled employees deliberately compromising the institution has become more probable than ever. Robust checks such as segregation of duties in IT Systems and Key Business Processes, enhanced due diligence on authenticating client instructions, internal policies such as mandatory block leave for internal staff and staff training and awareness on anti-fraudulent measures need to be in place for organizations to operate effectively against fraud attacks.

IT Security and Infrastructure: In the current business environment witnessing large scale digitalization, outsourcing of IT infrastructure capabilities and increasing cyber-attack incidents, organizations need to ensure their IT infrastructure capabilities are up-to-date with international standards. Corporations need to ensure they are protected against latest malware, ransomware and Denial of Service attacks and have in place adequate IT protection against system data compromises. Digitalization and outsourcing attempts should be carried out while keeping in mind the expectations of customers, business stakeholders and regulators. Periodic KPI reports on data security and service offering should be reviewed across governance forums in order to remain vigilant against cyber threats.

Bringing it all together: Operational Risk Management implies prevention of risks arising from inadequate internal processes, people, systems and external events, wherever feasible. While a small amount of these risks may be tolerated for practical reasons on conducting business, materialization of large-scale impact events such as breakdown of daily processes, fraudulent attempts, unethical business practices, regulatory breaches and cyber-attacks, need to be prevented for a corporation's long-term viability. A multi-faceted approach of enforcing good corporate governance, diligent adherence with regulatory and industry best practices, strong internal control framework, efficient checks against fraudulent attacks and sturdy IT security and infrastructure can greatly help an organization in managing a robust Operational Risk Framework.

author

Vivek Seth

Vivek Seth is a Singapore citizen with over 15 years of experience in Risk Management spread 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 data risks - taking data quality to the next level

by **Boyke** Baboelal

Too many financial services firms still have a reactive approach to data quality. Cleansing and analysis of incoming data is mainly done on a day-to-day basis before distributing to downstream systems.

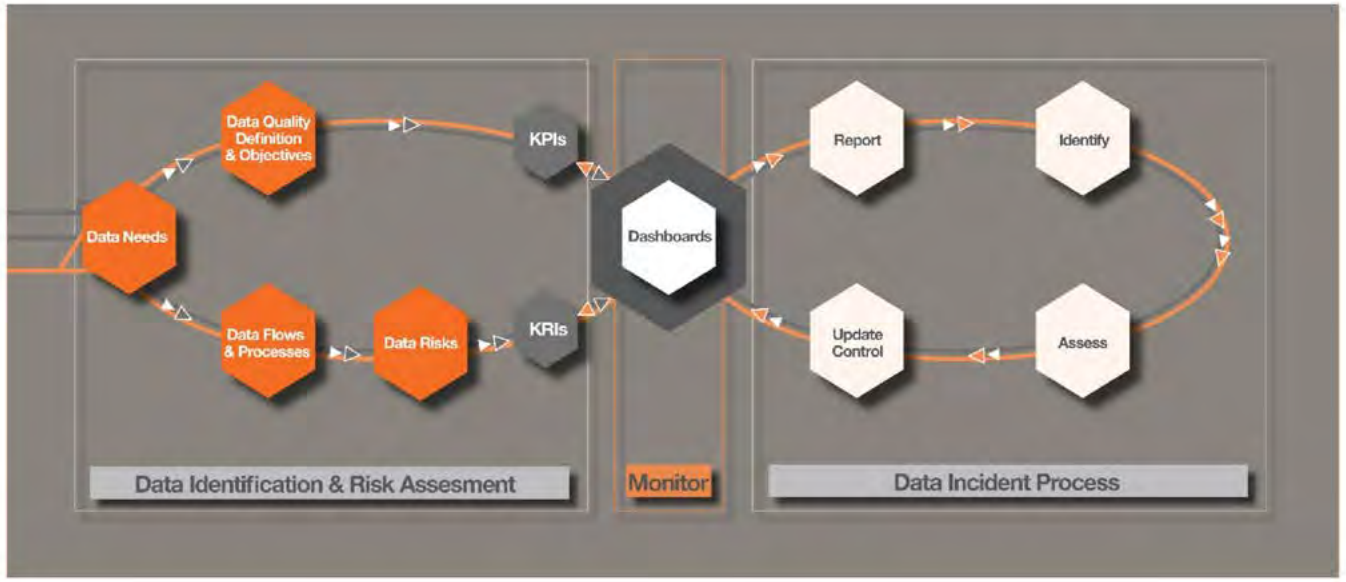
Unfortunately, by prioritizing ad-hoc incident resolution, organizations struggle to identify and address recurring data quality problems in a structural manner.

To rectify this issue, organizations must carry out continuous analysis, targeted at understanding their data quality and reporting on it over time. Not many are doing this, and that's a problem. After all, if firms fail to track what was done historically, they will not know how often specific data items contained completeness or accuracy issues, nor how often mistakes are made, or how frequently quick bulk validations replace more thorough analysis. More importantly they will not be able to measure and demonstrate their levels of data quality.

To address this, organizations need to put in place a data quality framework. Indeed, the latest regulations and guidelines increasingly require them to establish and implement this type of framework.

Organizations must outline a data quality policy that establishes clear data objectives, defines data quality and target levels, and puts in place data governance, including processes and procedures; responsibilities and data ownership. The next step is identifying the critical data elements, the risks and likely errors or gaps in that data, the flows needed to process and distribute risk factors, the data risks in the data flows, and the controls that are needed to mitigate risks identified. Organizations do not work according to this holistic approach, but most have some of the key controls in place such as exception handling and job monitoring.

The framework will guide organizations in establishing the dimensions of data quality. For instance, the framework will ensure data is accurate, complete, timely and appropriate. For all these areas, key performance indicators (KPIs) need to be implemented to enable the organization to measure what levels of data quality are achieved, while key risk indicators (KRIs) need to be implemented and monitored to ensure the organization knows that risks are at acceptable levels and controls are effectively mitigating those risks. Adverse changes in the KPIs and KRIs must be picked up using a clearly defined data incident process aimed to resolve data incidents in a structural manner and preventing them from occurring again, overall resulting in continuously improving data management.



The key question is, what is preventing organizations in implementing a data risk assessment process, and in general a data quality framework? The answer is data. Data needed to calculate these KPIs and KRIs has been transient or was scattered throughout the EDM solution as there was no direct use of this information. For example, how often did validation rules flag data as suspect and how often was it a True Positive? This is extremely hard for most organizations to assess but is key for evaluating the performance and effectiveness of one of the most important controls: exception handling.

Once put in place, a data quality framework will inevitably be focused on the operational aspects of an organization's data quality efforts. To further elevate data quality, businesses can employ a data quality intelligence approach which enables them to achieve a much broader level of insight, analysis, and reporting, also through analytics which can further reduce data risks, improve data quality, and increase operational efficiency.

Analytics are already being used for finding comparable instruments, notably for proxying, and the detection of outliers. However, with data quality information, for example a Data Quality Index, further optimizations can be made without user intervention, reducing the need for backtesting validation rules. Another example is assessing the effectiveness of controls by verifying the consistent application of rules across the universe of instruments using clustering algorithms.

Data quality intelligence effectively forms a further layer on top of the operational data quality functionality provided by the framework, which helps to visualize what it has achieved, making sure that all data controls are effective, and that the organization is achieving its KPIs and KRIs. Rather than being an operational tool, it is effectively a business intelligence solution, providing key insight into how the organization is performing against its key data quality goals and targets. CEOs and Chief Risk Officers (CROs) would benefit from this functionality as would compliance and operational risk departments, i.e. to assess compliance with internal data quality policies and relevant industry regulations.

In financial services with its significant regulatory burden, the consequences of poor data quality are even more severe. And so, it is a timely moment for the rollout of the multi-layered approach outlined above, which brings a range of benefits, helping firms demonstrate the accuracy, completeness and timeliness of their data, which in turn helps them meet relevant regulatory requirements, and assess compliance with their own data quality objectives. There has never been a better time for financial services organizations to take the plunge and start getting their data quality processes up to scratch.

author

Boyke Baboelal

Boyke Baboelal is Strategic Solutions Director Americas at Asset Control, where he ensures the company maintains its position as the industry's best-informed and most flexible partner for financial data management. Boyke brings 15 years of risk and data management knowledge to Asset Control. With his financial engineering background and hands-on experience, Boyke understands the importance and value of good data. Boyke holds a master's degree in Econometrics, a postgraduate degree in IT and an MBA from Rotterdam School of Management.

forward-looking bank steering – the move from the 'what-is' to the 'what-if'

by **Peter** Plochan

Over the last couple of years, banks around the globe have been swamped with increasing regulatory scrutiny and complexity. In particular, we have observed a shift from the traditional backward looking 'What Is' supervision focusing on "the observed" towards a more forward-looking 'What If' approach assessing both "the Expected and Unexpected future".

forward-looking regulations

Nowadays, satisfying regulatory requirements on historical performance (Pillar 1) is no longer sufficient. Banks now have to spend increasing effort to demonstrate to regulators that they can satisfy performance requirements and expectations on their financial KPIs & KRIs also in the future. Examples of the recent regulatory initiatives in this area from the last 12 months include:

- EBA's revised guidelines for SREP[1] and Supervisory Stress testing
- EBA's guidelines on Institution's Stress testing
- BIS's Stress Testing principles
- PRA's Model Risk Management principles for Stress Testing
- EBA's revised guidelines for ICAAP / ILAAP[2]
- EBA's updated requirements on Funding plans
- ECB's Recovery Plans submissions
- FED's increased transparency revision of the CCAR[3] program

A theme common to these regulatory changes is the demand for more transparency and granularity across the various forward-looking regulatory calculations. When forecasting their financial KPIs & KRIs, the banks have to perform more calculations, produce more reports and with higher frequency, while following more analytical approaches and less expert-judgment based forecasting.

[1] Supervisory Review and Evaluation Process

[2] Internal Capital Adequacy Assessment Procedure / Internal Liquidity Adequacy Assessment Procedure

[3] Comprehensive Capital Analysis and Review

In particular, European banks have been hit by a regulatory wave in this context where:

- EBA's EU wide stress testing 2018 for the first time required banks to incorporate the IFRS 9's forward-looking Expected Credit Loss calculations in their forecasting which introduced significant complexities into the process.
- ECB's liquidity risk Stress Test 2019 will for the first time require EU banks to stress their Basel liquidity measures and will put their liquidity risk forecasting capabilities to the test.
- In addition to the above, EBA has further expanded its Pillar 2 framework with additional capital requirement – Pillar 2 Capital Guidance (P2G, details on the right and below).

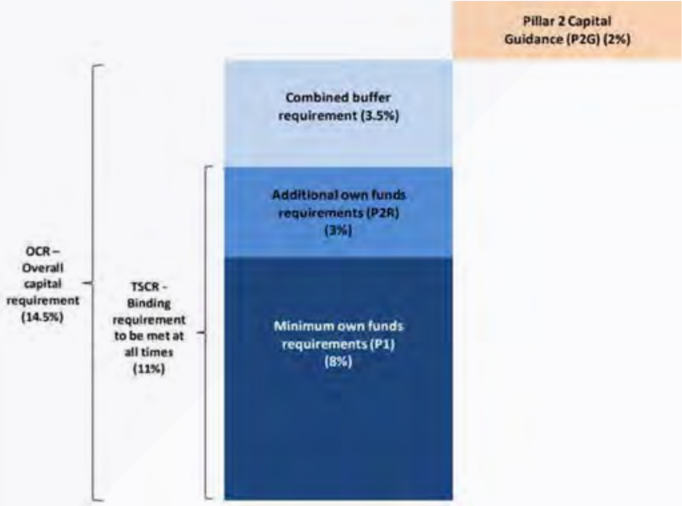


Figure 1: EBA's P2G Framework

P2G is a capital add-on that can be imposed on a bank on the top of its Pillar 2 capital requirement (P2R) as result of (1) the inability to meet the applicable own funds requirements (qualitative and quantitative) in stressed conditions; or (2) supervisory concerns over the (excessive) sensitivity of a bank toward scenarios assumed in supervisory stress testing.

In parallel to the above, the current geopolitical climate, macroeconomic environment of sub-zero interest rates combined with the emergence of the digital & FinTech era have put banks into a difficult situation. They now have to balance the need for more returns, better customer retention and lower costs with the drive to become more agile to flexibly and proactively respond to these recent regulatory and potentially unfavorable market trends.

forward-looking business processes and bank steering

The Budgeting, Financial (Capital) planning and ALM are the strategic business tools for each bank for determining its strategy, plan and future activities. Both the business as well as the regulatory driven forward-looking processes aim to forecast the bank's future balance sheet, P&L and the respective KPIs & KRIs under a particular macroeconomic or business scenario and assess the impact of any potential management action.

Senior executives at the banks use the information obtained during these processes for strategic decisioning and to steer the bank in the desired direction where performance goals are most likely to be achieved. .

While the business forecasting processes focus more on the expected financial KPIs and are typically driven from Finance, the ALM and regulatory driven initiatives on the other hand focus on a broader picture covering both the expected and the unexpected future and are often owned by Risk departments.

Due to the shared goals of these forward looking processes, typically they have also a number of overlapping and duplicate activities often running within Risk or a Finance silos and within the underlying system which then results in inconsistencies and reconciliation issues.

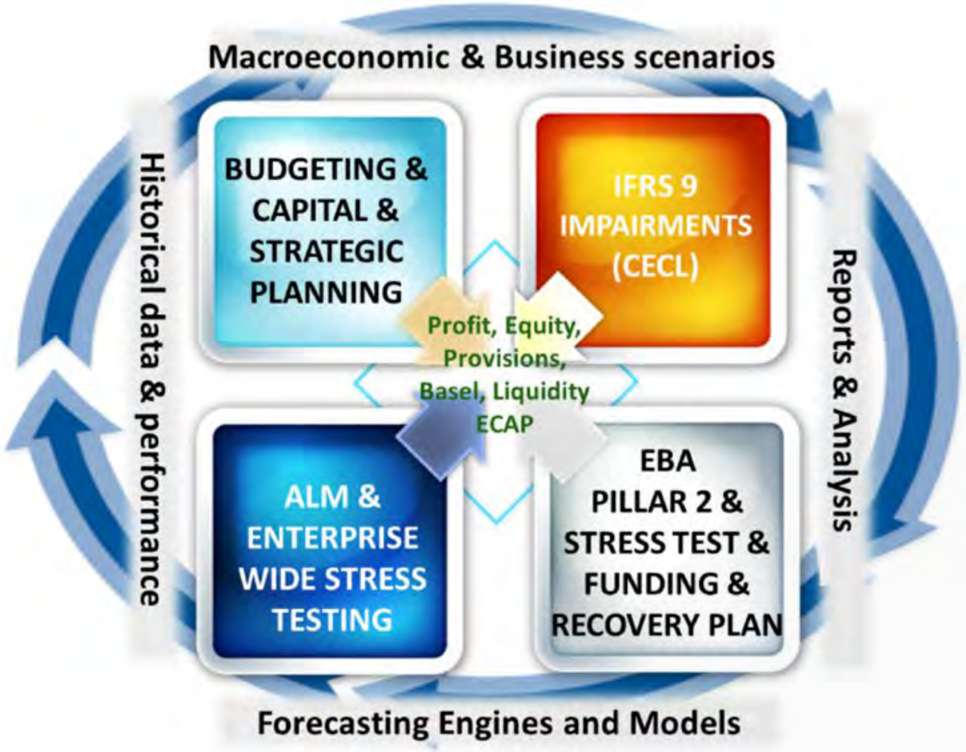

Macroeconomic & Business scenarios
Historical data & performance
Reports & Analysis
Forecasting Engines and Models
BUDGETING & CAPITAL & STRATEGIC PLANNING
IFRS 9 IMPAIRMENTS (CECL)
ALM & ENTERPRISE WIDE STRESS TESTING
EBA PILLAR 2 & STRESS TEST & FUNDING & RECOVERY PLAN
Profit, Equity, Provisions, Basel, Liquidity ECAP

Figure 2: Forward-looking performance management

However, to form a full view on each bank's future performance, both the finance and risk side are needed, which can be often very challenging, due to the complexities described above and the increasing business and regulatory requirements.

For example, the results of EBA's 2018 Stress Test (below) show that the key drivers behind the drop of aggregated Capital Adequacy (CET1) Ratio in times of stress have been the 1) Impairments; 2) P&L and only as nr; 3) RWA increase. The combined absolute capital impact of 1 and 2 on the CET 1 ratios were almost 5 times higher than the impact of RWA increase. Thus, the KPIs coming from Finance are crucial for determination of stress testing results, yet the exercise is driven by Risk.

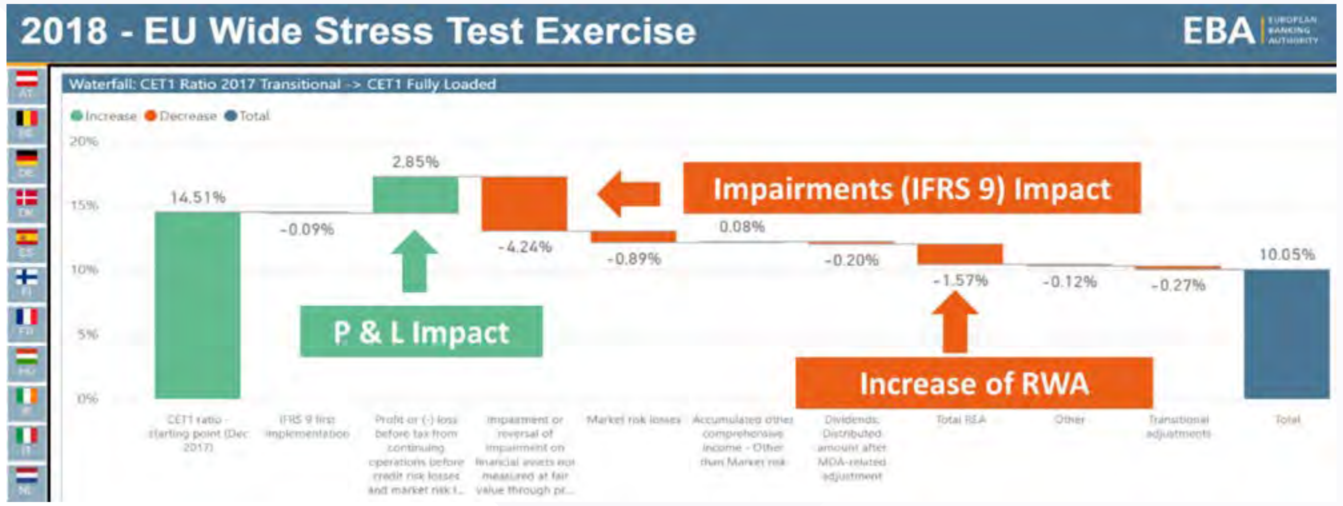


Figure 3: The Key drivers determining the Stress Test results

Source: EBA EU-Wide 2018 Stress Test - dashboard

impact of IFRS 9 & CECL

Generally, the credit risk provisions (or impairments) impact bank's performance along 3 dimensions:

- Balance Sheet – an increase of provisions decreases the Equity, the basis for regulatory capital
- Profit & Loss and Balance Sheet – generally an increase of provisions is recognized as credit loss (or bad debt expenses or impairment losses) which decreases the net profit and also decreases the gradual build-up of Balance Sheet Equity over time (Figure 3 example above)
- IRB shortfall – the pre-requisite of Basel Capital framework is that bank's expected credit losses are covered by bank's provisions and any shortfall will result in adjustment of the available capital.

With IFRS 9 ECL[4] being live since 2018, the complexity of the above interactions has significantly increased as the provisions became much more sensitive to the macroeconomic cycle. As a result, much more sophistication & resources are required to accurately estimate the future impact of provisions on banks KPI's and KRI's. A particular area of attention will be the level of (mis)alignment between the "through the cycle" Basel formula for expected credit loss calculation and the "point in time" ECL calculation required by IFRS 9.

While the overall impact of IFRS 9 adoption in 2018 on EU banks resulted only in a relatively minor increase of banks' provisions (5-10%)[5], it is in time of stress when the volatility and sensitivity of IFRS 9 ECL estimates and their impact on KPIs and KRIs really materialize (as shown in Figure 3). Therefore, it is reasonable to expect that banks will see much more volatility in their provisions as the economy slows down.

[4] / The Expected Credit Loss Impairment standard. In US it will be the CECL: The Current Expected Credit Loss accounting standard which is US GAAP version of the IFRS 9 applicable for US from 2020 onwards

As the baseline results of EBA 2018 Stress Test in Figure 4 below show, in the "good" times the future 1) P&L result; and, 2) Dividend policy have more impact than IFRS 9 provisions.

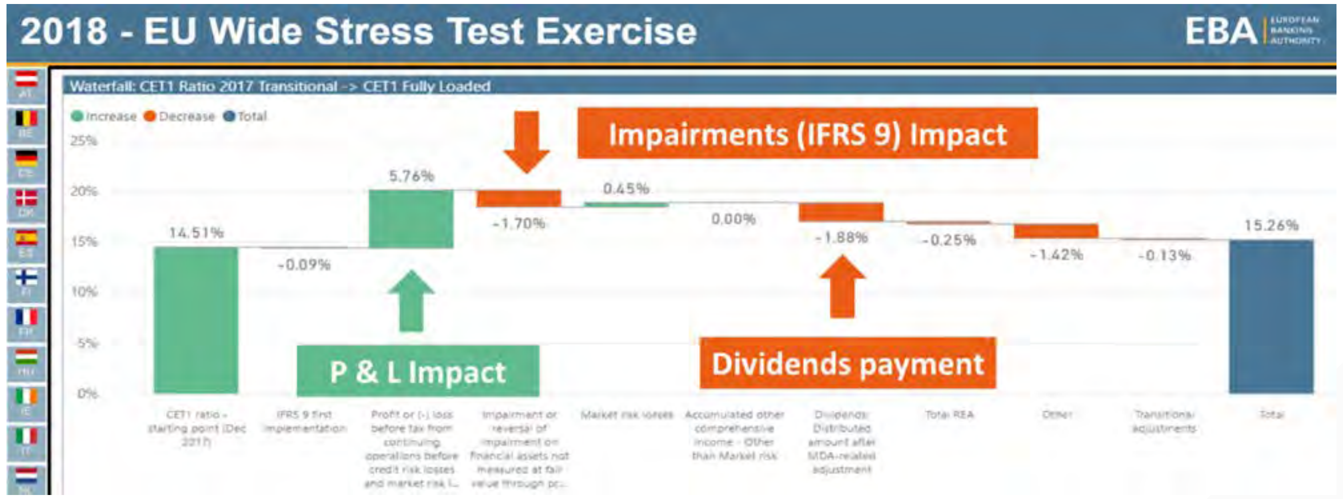


Figure 4: The Key drivers determining the KPIs & KRIs in "good" times

Source: EBA EU-Wide 2018 Stress Test - dashboard

the way forward

The new regulatory initiatives, market developments as well as the digital trends are demanding more forward-looking perspective on each bank's performance. Banks need to adapt in order to be able to pro-actively and much faster respond to sudden market developments, understand the impact of their decisions before making them and provide more forecasted information to both the external and internal stakeholders.

In order to efficiently address the above banks will have to align and automate their forecasting activities, bridge the gaps between various finance and risk processes, and consolidate their underlying systems. Those that succeed will be able to foresee the obstacles along their way, proactively take impact-aware actions and successfully steer their bank in the challenging and unstable geopolitical and economic waters.

[5] / EBA, Dec 2018, First observations on the impact and implementation of ifrs 9 by EU institutions

author

Peter Plochan

Peter Plochan is Senior Risk & Finance Specialist at SAS Institute assisting institutions in dealing with their challenges around finance and risk regulations, enterprise risk management, risk governance, risk analysis and modelling. Peter has a finance background (Master's degree in Banking) and is a certified Financial Risk Manager (FRM) with 10 years of experience in risk management in the financial sector. He has assisted various banking and insurance institutions with large-scale risk management implementations (Basel II, Solvency II) while working internally and also externally as a risk management advisor (PwC).

Interested in learning more from Peter? Join us for these upcoming opportunities:

- Thought Leadership Webinars (Complimentary for Sustaining members)

BALANCING THE TWO SIDES OF AI: BENEFITS VS. RISKS

Wednesday, May 15

ENTERPRISE RISK MANAGEMENT 2.0 – LOOKING TO THE FUTURE

Wednesday, May 22

- Virtual Learning Series (fee)

MODEL RISK MANAGEMENT

May 28-June 25

Five, 90-minute interactive lessons on the design and execution of robust MRM framework

managing preventable risks

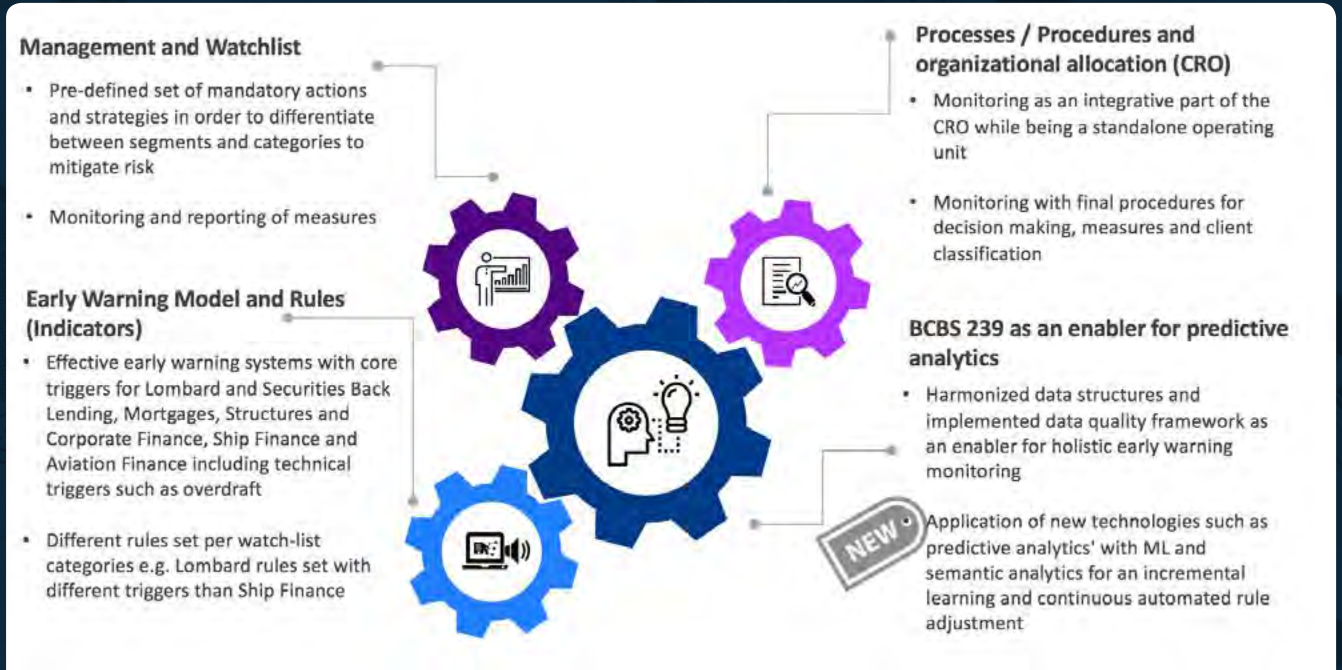
by **Elias** Loki

the opportunity for machine learning in credit risk early warning systems

Since the financial crisis of 2008, both Global Systemically Important Banks (G-SIB) and Domestic Systemically Important Banks (D-SIB) have been affected by regulations published by the Bank for International Settlements (BIS). The regulatory efforts of BCBS 239, in which financial institutions need to demonstrate transparency, completeness, accuracy and timely provisioning of risk data has enabled banks to free up synergies and leverage the revised infrastructure to apply better controls and open the capability to introduce, in a cost-efficient way, improved models and frameworks for an early warning system (EWS) in the area of credit risk management.

The banking industry is still, however, lacking behind in terms of leveraging freed up synergies. The opportunity of a methodology and technology re-launch for early warning systems could be used to replace traditional human rule-based approach. But why is this important? The decrease in the credit worthiness of a client or the potential increase of default reduces the opportunity of the bank and the client to navigate through a potentially difficult situation. The bank's first priority would be to keep the expected loss at a minimum. There are various possibilities to hedge potential loss situations, for example, through the use of credit default swaps. However, where clients are characterized as 'not listed corporates' or 'private individuals' an EWS provides a mechanism to better manage potential losses and which can lead to reduced loan-loss provisions, higher risk-bearing capacity and optimized regulatory capital requirements.

BCBS 239 infrastructure as an enabler



Management and Watchlist

- Pre-defined set of mandatory actions and strategies in order to differentiate between segments and categories to mitigate risk
- Monitoring and reporting of measures

Early Warning Model and Rules (Indicators)

- Effective early warning systems with core triggers for Lombard and Securities Back Lending, Mortgages, Structures and Corporate Finance, Ship Finance and Aviation Finance including technical triggers such as overdraft
- Different rules set per watch-list categories e.g. Lombard rules set with different triggers than Ship Finance

Processes / Procedures and organizational allocation (CRO)

- Monitoring as an integrative part of the CRO while being a standalone operating unit
- Monitoring with final procedures for decision making, measures and client classification

BCBS 239 as an enabler for predictive analytics

- Harmonized data structures and implemented data quality framework as an enabler for holistic early warning monitoring
- Application of new technologies such as predictive analytics' with ML and semantic analytics for an incremental learning and continuous automated rule adjustment

A mature EWS approach would consist of using statistical and qualitative indicators with a high predictive accuracy for default. Identifying these triggers, based on the released synergies raised from the Basel framework, provides Banks with an ideal opportunity to enhance their credit risk management (CRM) process. The relevant information technology infrastructure, human resources and data are available in such a highly sophisticated and educated manner than ever before. The question arises as to how to integrate these capabilities in order to manage preventable credit risk by a relaunch of methodology and technology. First, it is highly recommended to identify the relevant credit segments, which have a need for improvement and understand what governance processes are in place for an EWS and determine whether they are sufficiently robust and consider the data used in modelling.

Secondly, the questions of financial materiality and experienced shortcomings should be clarified. A strong alignment between the recovery team and portfolio management team would lead to expert and experience driven analysis. An analysis of defaults by credit volume and type, results in the assessment and re-calibration of given statistical and macro-economic triggers.

Thirdly, the validation of new technologies and methods needs to be considered. This includes the use of predictive analytics such as behavioral analytics, semantic analytics, and machine learning. The added value of behavioral analytics is characterized through data science and social network analysis combined with machine learning. Data feeds from external sources could be incorporated, in which major critical decisions are communicated earlier than in traditional news. Machine learning applies purely data driven rules for use in early warnings system based on various data sources (Big Data).

For example, the use of classical approaches e.g. Professor. Edward Altman Z-Score approach coupled with the use of more advanced mathematical algorithms e.g. in constructing Credit Risk Scorecard using the Mahalanobis-Distance approach to determine predictive clusters can be applied to identify the relevant clients in a shortfall position. This would help the first line of defense to proactively identify potential credit anomalies as opposed to reacting based on client-re-ratings as part of credit review process.

Data from the front-office can be integrated in the continuous improving machine learning algorithm. Further, a purely data driven rule-set generation enriched with the feedback of a risk manager incorporating the qualitative component, completes the full capability of a new auto-improved rule generation and indicator re-calibration. This supports the elimination of human error and increases the operational effectiveness.

Semantic analytics helps to transform unstructured data into actionable knowledge for a better comprehensive understanding and parameter calibration of the early warning models.

However, not every new technology or technical method is needed for every credit risk segment. More important would be the derived conclusions and benefit-based incorporation of new technologies and methods. The latest Basel frameworks have created added value and freed up new synergies in terms of data quality and re-calibration gains of existing credit risk systems.

references

1. https://www.bis.org/publ/bcbs239.pdf
2. http://pages.stern.nyu.edu/~ealtman/Zscores.pdf

author

Elias Loki

Elias Loki, Senior Business Consultant at BearingPoint, Switzerland, is a subject matter expert for BCBS239, market and credit risk management. He has been working with systemically important banks helping them in implementing regulatory change and giving them guidance and advise for several years. His educational background in business economics, mechanical engineering combined with an MBA has equipped him with a broad base from which to approach many topics in the area of Financial Risk Management.

managing systemic and preventable risks

by **Wilson** Fyffe

Although the focus of this article is ‘risks arising within an organization that are controllable and ought to be avoided or eliminated’, I wish to start from the top, dealing with human civilization itself as an organization.

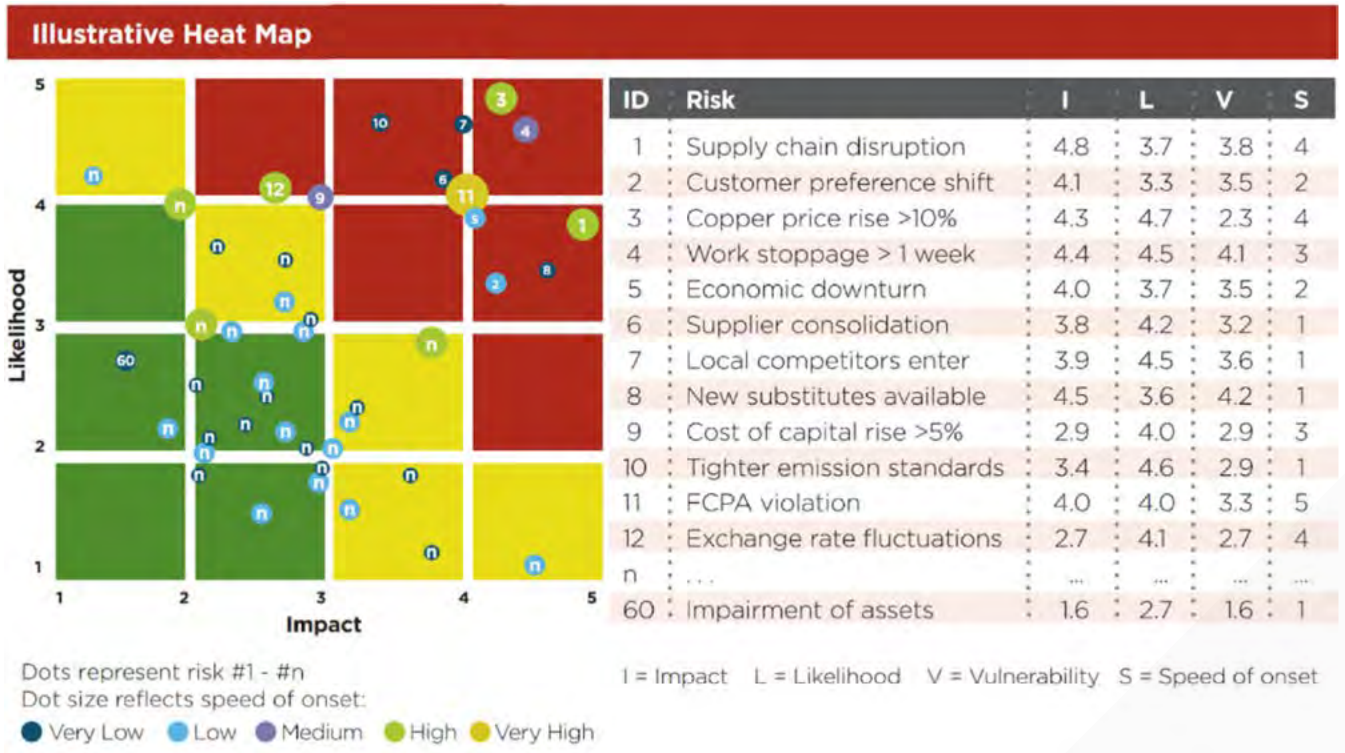
looking at preventable risks from an alternative viewpoint

The daily news and literature are replete with examples of realized and latent risks. Governments and industries are well aware of the consequences of inadequate risk management as required by ISO31000 and COSO. However, to a large extent, we still rely on common sense to make gradual improvements in our quality of life.

In that regard, the notion of ‘preventable risks’ engenders visions of safety fences and electrical voltage warnings. However, we may also consider such risks from a positive viewpoint regarding their potential to improve our quality of life, by the way we think about them. This latter area is rich with possibilities, mainly due to new technology developments.

organizational risk culture – prone to fatigue

The difficulties of maintaining an organizational risk-aware culture was brought home to me during an executive training exercise in the oil and gas industry in the Middle East. The client organization’s HR manager advised me that one of their issues was the fact that the company’s engineers became tired of preparing quarterly reports on the impact and probability of occurrence of process failures. In many cases, the failure scenarios required the preparation of comprehensive operational and financial models to place a monetary value on a contemplated failure. These values were then used in a conventional Failure Mode Effects & Analysis table to rank the various risks. Typically, the communication involved the use of ‘Heat Maps’, an example of which is shown below in Figure 1.



Illustrative Heat Map

ID	Risk	I	L	V	S
1	Supply chain disruption	4.8	3.7	3.8	4
2	Customer preference shift	4.1	3.3	3.5	2
3	Copper price rise >10%	4.3	4.7	2.3	4
4	Work stoppage > 1 week	4.4	4.5	4.1	3
5	Economic downturn	4.0	3.7	3.5	2
6	Supplier consolidation	3.8	4.2	3.2	1
7	Local competitors enter	3.9	4.5	3.6	1
8	New substitutes available	4.5	3.6	4.2	1
9	Cost of capital rise >5%	2.9	4.0	2.9	3
10	Tighter emission standards	3.4	4.6	2.9	1
11	FCPA violation	4.0	4.0	3.3	5
12	Exchange rate fluctuations	2.7	4.1	2.7	4
n	. . .	...	...	...	...
60	Impairment of assets	1.6	2.7	1.6	1

Dots represent risk #1 - #n
Dot size reflects speed of onset:
● Very Low ● Low ● Medium ● High ● Very High

I = Impact L = Likelihood V = Vulnerability S = Speed of onset

Figure 1: Heat Map

The above ‘Heat Map’ has been published on the Internet by Singapore-based Causal Capital.

managing systemic risks

Major geopolitical risk cases currently in the media include those described in the links below. While these risks are not preventable from an organizational perspective, their impact can be managed by using scenario stress testing.

- Future of Mining
- Future of BREXIT
- The US-Mexico Border Wall
- China Belt and Road

managing preventable risks

Preventable risk cases drawn from my personal experience include the following:

- Crowd control in large entertainment venues
- Driver fatigue in long-distance road transport
- Fraud in the banking system
- Inadequate assessment of investment opportunities

These examples illustrate four different preventable risk situations.

Crowd control in a large entertainment venue:

In this case, I was present in an exhibition at which there were more than 5,000 attendees. I attempted to go outside to the garden area but found that the emergency exit door was locked. The security guard did not speak English. I found the security manager, who explained that all emergency exits were locked to ensure that attendees could only exit via the front door, in order to ensure good traffic passing the prime exhibitors' stands.

Driver fatigue in long-distance road transport:

Truck and bus drivers are tempted to work long hours to make ends meet financially. In one case, my client requested that I assist by attending the site of a non-fatal highway accident where one of his company's trucks had rammed the rear of another truck. There were no skid marks, indicating that his driver had fallen asleep at the wheel.

In another case the driver of my sports team's bus could not stay awake during his 12-hour shift driving across Australia's Nullabor Plain. High speed heavy vehicle traffic was constant in the opposite direction. I was able to assist by keeping his hand-towel iced until the end of his shift.

Fraud in the banking system:

Sometimes banks assist clients to make multiple deposits to their many suppliers or partners. A typical facility is to instruct the bank's client to make one large payment by cheque, with the bank as the payee. The bank then distributes the money in accordance with a list of payees entered in a form provided by the bank. This involves risk to the bank if the form, which is an appendix to a contract (the cheque) is not signed by the approved cheque signatories (e.g. signed by the cheque drawer's staff member, who is not a cheque signatory).

Inadequate risk assessment of commercial property investments:

In one case, my client called for assistance when an investment in an operating riverbank-based small-scale shipbuilding facility ran into difficulties. The decision to acquire the facility was made without checking the plans of the local government for the region. These included the construction of a low-level highway fly-over of the river downstream from the facility, which limited all future construction in height above water level.

In another case, my client went ahead with construction of an ocean bay-based woodchip export ship loading facility without conducting long-term wind and wave studies. During an early ship-loading operation, once-in-5-year wave conditions rammed a loading ship against the facility, causing massive damage.

conclusion

Managing systemic and preventable risks requires not only thorough analysis but also different approaches. While both types of risk can result in catastrophic losses, the impact of systemic risks can be mitigated by scenario stress testing, while the occurrence of preventable risks can be avoided by common-sense business practices and controls.

author

Wilson Fyffe

Wilson Fyffe is a consulting futurist with a broad background in commerce globally, with particular emphasis on developing economies. He has direct experience in more than 30 industries over a period of 30 years. He has recently completed a 3-year term as a Global Director of the Professional Risk Management International Association (www.prmia.org) He is a member of the World Future Society (wfs.org), the Institute of Directors, India and of Parima. His works have been published by Wylie in the text 'Scenario Planning' (11changes.com) and by the KPI Institute. His research has included developments in Chaos Theory and its implications for business and government. Wilson holds a BA from Macquarie University with double major in philosophy, covering economics, statistics and the behavioral sciences.

confronting the bank technology challenge[1]

by **David** M. Rowe

Insurgent competition based on product innovations and application of new technology is an abiding threat to established firms in an ever-growing range of activities. This is certainly true for banks and other financial institutions.

This challenge is largely driven by technological advances with which they have failed to keep pace. To be fair, a complex web of banking regulations emerged in the mid-1980s and expanded dramatically after the Global Financial Crisis. Complying with these regulations involves a constant struggle to compile information from a maze of legacy information systems unsuited to meeting either these regulatory demands or multiple emerging competitive threats to banks' profitability.

In fact, I believe it is not overstating the case to assert that, late in the second decade of the 21st century, banks are facing an existential threat to their long-established place in society and the economy.

The compliance challenge has distracted bank management from focusing on a long-term transformation of their information infrastructure. With each passing year, the inflexibility, fragmentation and high maintenance cost of banks' information storage and processing systems has become a critical competitive handicap.

When Kohlberg Kravis Roberts bought RJR Nabisco in 1988, it inspired the book – later a movie – Barbarians at the Gates. This episode helped create the myth that financiers were the masters of the universe and became the stuff of nightmares for successive generations of corporate chief executives.

Now there has been something of a role reversal. Real engineers – rather than financial engineers – are suddenly the predators rather than the prey. Experts in technology, process and operations are stealthily plotting a thousand coups, small and large. Despite these warning signs, many bank managers remain unconvinced that a major architectural overhaul of their information systems is an urgent necessity.

The technological challenge has not come primarily in the form of de novo full-service banks. That would be what Silicon Valley types call a "full-stack financial services start-up". These interlopers are accustomed to thinking in terms of the individual components of a technology stack. They tend to seek disruptive innovations in selected areas that improve performance for one component of the stack, while fitting comfortably into the larger technology ecosystem. This mindset is directly reflected in the way FinTech is mounting its competitive challenge.

Domestic payment systems were the first area of attack with the founding of PayPal in the late 1990s. This first thrust was aimed at disrupting online payments at a time when many people hesitated to transmit credit card details over the internet. Later, Apple Pay extended the attack to the retail point-of-sale payment process. More recently Square, Shopify, Payline and others are offering a variety of hardware and processing rates to merchants of all sizes.

Peer-to-peer lending has evolved into what practitioners prefer to call market-place lending. It has moved beyond direct intermediation of savers and borrowers, instead attracting participation from hedge funds and other institutional investors. While still small, market-place lenders are growing rapidly. If this growth continues, they may well become a direct threat to banks' traditional role as the primary source of financing for individuals and small businesses once thought too small to tap public debt markets. At the very least, they will create pressure on banks' profit margins on this activity.

In the lucrative business of retail foreign exchange transfers, innovators such as TransferWise cut fees by 80–90% while still making money. In mid-2015, Mark Andreessen's venture capital firm, Andreessen Horowitz, invested $58 million in TransferWise. He had previously been widely quoted as saying, "We can reinvent the entire thing … We have a chance to rebuild the system … You would not today, starting from scratch, invent any of these financial businesses in the same way. To me, it's all about unbundling the banks." Bankers may think this is just Silicon Valley hype, but they ignore the challenge at their peril. The traditionally protected and profitable activities of banks will face growing competition from non-banks, powered by improving technology and shifting attitudes among members of the Millennial Generation.

Banks will not solve their technology problem by tinkering with marginal improvements in their existing applications. The problem lies in the fundamental characteristics of their information ecosystems rooted on outmoded 20th century system architecture. Only an orderly transition to the 21st century architecture that drives digital native companies like Google and Amazon will ultimately resolve banks' information systems dysfunction. This is a major multi-year undertaking, but tools and resources are increasingly available to support this transition.

Banks that fail to extract themselves from the burden and cost of their legacy technology will see more and more of their profitable business lines come under attack. Today it is no longer the Barbarians at the Gates that have all the leverage. The Geeks at the Gates are mounting a powerful challenge that will not go away.

author

David M. Rowe

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.

[1] / This essay is a slightly edited excerpt from David Rowe's new book An Insider's Guide to Risk Management – Relearning the Lessons of the Global Financial Crisis.

2018 EMEA Risk Leader Summit focused on future-proofing the organization

by **Alexandru** Voicu, PRMIA technical advisor

PRMIA was very pleased to partner with Bloomberg in hosting the 3rd and most successful edition of the EMEA Risk Leader Summit in November 2018. The event had 120 CROs and heads of risk gathered for an interactive summit. The dominant themes of the event were the influence of technology on the risk department and the business model in financial services, as well as geopolitical influences.

The event kicked off with a keynote by Prof. Charles Donovan from Imperial College Business School, talking about the geopolitical and financial influences of climate change -- How can the financial services industry take an active role in managing the climate transition by pricing climate risk? One of the key insights from polling our audience was that 78% of respondents said pricing climate risk in deals is a benefit to clients and is not pricing them out of the market. There are many actors that need to align for this framework to be successful, governments being in the lead here. But there was strong agreement that the industry can be an agent for change and is starting to do more than window-dress reports.

Climate risk was also the topic of conversation for a later panel. Our panelists, all leaders in the climate transitioning practice, discussed regulatory impacts, various carbon pricing schemes and their effectiveness, scenarios on various degrees of world heating, and incentives for climate resilience.

The second panel of the day looked at risks on the horizon, with more details discussed in David Croen's review of the panel he led. Key risks discussed included: cyber risk, decentralization and state fragility, business cycle risk coupled with trade headaches, talent and technology, climate change, demographic shifts and all things political. Plenty of things to juggle for risk managers and executives.

We then looked at Unleashing the Power of Digitalization in Finance with 3 disruptors in the mortgage FinTech space and blockchain. There are truly new digital innovations replacing legacy systems and gaining scale. The buy-side is able to take direct ownership of mortgages, completely avoiding the sell-side. Experimenting with tokenization might change asset structure ownership in the next couple of decades. Payments are undergoing significant disruption and cost reduction. All of these items pointed to our business model conversation.

The panel looking at the business model, comprised of corporate and independent VC investors, had a clear realization that the old ways of banking have to change. The closed banking environment is not the same, and regulators are taking steps to ease frictions on switching, a market reality which has to come with significant adjustments between the two competitively collaborative environments: banks and FinTechs. User experience and pricing are the key drivers of this transformation.

Where does risk fit into strategy was an important question we looked at from 4 angles: a large institution, one medium-sized, a nimble one, and a supranational. The key takeaways are that risk departments are a good reality check for deals and provide transparency in risk concentrating areas, and the Risk Appetite Statement has grown closer to the strategic planning process. There is a tendency of bringing the lines of defense closer together for better cooperation and deeper specialization.

Taming the Data, our panel on AI & machine learning had a very high level of engagement as these technologies are getting rolled out in the risk departments and beyond. The new technologies are fragmenting vendor relationships and are creating new dimensions of 3rd party risk which are harder to manage. Demystifying black box algos is another issue, but the panelists had convincing solutions in terms of apportioning principal drivers to models.

Adding a touch of Basel to the Market Structure issue and FRTB was the most fun and frank panel. We then concluded day 1 with a fun networking session in the Mithreaum.

Day 2 was started with a recap of revolts around liberal democracies. Voter behavior was closely examined to understand future political trends that will impact regulation and trade policy. One of the most acknowledged new realities was the much closer interaction between politics and economics. Populist leaders are taking a more active role in the decision-making process of formerly independent institutions.

After a recap on politics, we had our Brexit strategy panel looking at the reshaping caused by Brexit. An evolving topic as of writing this summary, it was the same on the day of the conference as cabinet ministers were playing the resignation domino game. The conclusion is the largest challenges are people and talent when it comes to relocation as companies need to move families, which is a complex process in itself when there isn't school capacity to absorb the inflow, and need to build new relationships in the new jurisdictions.

The risk management function has evolved a lot. And we will have a close examination of how the function is evolving, and what strategies risk leaders should employ to function best. Where is credit risk managed in the institution, and how are the lines of defense interacting? The overall trend is for the front and second lines to get closer together, but there are different approaches around that macro trend. For example, 31% of respondents said the front line is driving credit risk management, and 33% said the risk department is the driving force. More diverse hiring in terms of skill-set has been reported by 60% of participants.

Cyber risk has become a key topic for boards after high profile and costly hacking scandals hit the wires around 2014. Cyber has become a key component of operational risk, and 82% of respondents said their boards are significantly more fluent and dedicate more agenda time to cyber than 5 years ago. Translating cyber attacks into potential exposures seemed to be the best way to get the message across.

The 4th edition of the EMEA Risk Leader Summit will be held November 5-6, 2019 at Bloomberg headquarters in London. The same frank conversations about risk will take place under Chatham House Rule. This year's focus will be on Cyber Trust, Alternative Lending, Talent Development and the intersection of Technology and Risk.

Explore insights from EMEA Risk Leaders in the 2018 Event Report.

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

March 16 – June 21

IBOR REPLACEMENT

April 17 – Amsterdam

ADVANCED OPERATIONAL RISK MANAGEMENT VIRTUAL TRAINING

Weekly classes open each Tuesday, April 23 - June 11, 2019

ESTABLISHED FIRMS JOINING BLOCKCHAIN ECOSYSTEMS PRUDENTLY

April 24 – Webinar

BREXIT – WHERE TO FROM HERE?

April 25 - London

FROM FIRE-FIGHTING TO BUSINESS AS USUAL

April 25 - Toronto

DYNAMIC RISK PROFILING

May 1 - Webinar

REGULATORY AUDIT READINESS: PEOPLE, PROCESSES, TECHNOLOGY

May 14 – New York

BALANCE THE TWO SIDES OF AI: BENEFITS VS. RISKS

May 15 – Webinar

MICROFINANCE INSTITUTION ASSESSMENT TRAINING FOR INDEPENDENT ASSESSORS

May 22 – 24 - Luxembourg

ENTERPRISE RISK MANAGEMENT 2.0 – LOOKING TO THE FUTURE

May 22 - Webinar

MODEL RISK MANAGEMENT VIRTUAL TRAINING

90-minute virtual lessons are released each Tuesday, May 28-June 25, 2019. Available 24/7.

HOW TO DETECT ANOMALIES USING MACHINE LEARNING

May 29 - Webinar

EMEA RISK LEADER SUMMIT

November 5 – 6 – London

CANADIAN RISK FORUM

November 11 – 13 - Montreal

INTELLIGENT RISK

knowledge for the PRMIA community