INTELLIGENT RISK

knowledge for the PRMIA community

July 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

SPECIAL THANKS

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

FIND US ON

prmia.org/irisk @prmia

INSIDE THIS ISSUE

editor introduction

Steve Lindo
Editor, PRMIA

Dr. **David** Veen
Editor, PRMIA

Nagaraja Kumar Deevi
Editor, PRMIA

The July 2019 issue of *Intelligent Risk* features articles on managing Strategic Risks, which are risks that an organization voluntarily accepts in order to achieve superior performance. When managing strategic risks, a focus on identifying, assessing and managing the risks in the organization's business strategy leads to acting when risks are realized.

The articles submitted by PRMIA members for this issue of *Intelligent Risk* cover a broad set of perspectives on this topic, ranging from insights on FRTB, cybersecurity, digital transformation, climate change, and business concentration to LIBOR's demise and algorithmic trading. The issue also has quality articles that focus on governance in relation to managing strategic risk, which allow us to see financial and global perspectives.

We hope you enjoy reading the articles published in this issue as much as we did reviewing and editing them.

how hedging explains variability in the capital impact of FRTB

by **Eugene** Stern

introduction: BCBS QIS results

Perspectives on the capital impact of the new Basel regulatory framework for market risk, known as the Fundamental Review of the Trading Book (FRTB), have varied widely. The Basel Committee on Banking Supervision (BCBS) has emphasized that, in aggregate, the new rule shouldn't increase bank capital relative to the current Basel 2.5 regime. However, capital could change quite a bit at the individual bank level. In its March 2019 Quantitative Impact Study (QIS) of the new rules, the BCBS commented:[1]

> *While the average prospective Basel III market risk capital requirements across Group 1 and Group 2 banks relative to current market risk capital requirements are comparable, there is wide variability at the bank level. Outliers are far more extreme.*

Though the remark that average requirements are comparable warrants its own discussion[2], our focus here will be on the *wide variability*.

More specifically, below is a chart of summary statistics describing the changes in market risk capital across Group 1 and Group 2 banks taken from the BIS's March 2019 QIS[3], together with a boxplot of this data for the Group 1 banks (using the 5th and 95th percentiles as the range of the plot):

FRTB Market Risk Capital Increase (%) as Percentage of Current Basel 2.5 Capital

	Group 1	Group 2
Max	870.6%	875.2%
95% percentile	225.6%	377.0%
75% percentile	122.5%	138.4%
Median	63.9%	85.6%
25% percentile	23.5%	12.8%
5% percentile	-58.9%	-57.4%
Min	-64.3%	-79.3%
Weighted average	95.2%	66.3%

1 / See https://www.bis.org/bcbs/publ/d461.pdf, Section 4.3.2, "Overall impact of the revised minimum capital requirements for market risk," bottom of p. 74.

2 / When we discuss the average, we need to remember we are tracking a moving target, as updates to FRTB since its initial January 2016 release have decreased the expected total capital requirement.

3 / See https://www.bis.org/bcbs/publ/d461.pdf, Annex C, p. 151.

What we see is that the bank at the 5th percentile saw its market risk capital under FRTB drop by almost 60% relative to today's Basel 2.5 regime, while the bank at the 95th percentile saw a rise in market risk capital of 225%. To once again quote the BCBS: Outliers are far more extreme.

What accounts for this variety of results across banks? Broadly, the impact of FRTB differs significantly depending on both the bank's book and the choices it makes about how to implement the rule.

The most basic implementation choices are whether to use the Internal Models Approach (IMA), and for which desks the bank should seek IMA approval.

As of the first release of FRTB in 2016, most large banks expected to stay on IMA and started planning accordingly, but many pulled back as its complexity became apparent, and some may end up not using IMA at all. Many banks' QIS submissions at this stage are based partly or entirely on the Standardized Approach (SA), so there needs to be an understanding of the variability observed so far in an SA context. As the SA appears at first glance to be completely prescribed and uniform across banks, what can account for the large differences we see in capital impact?

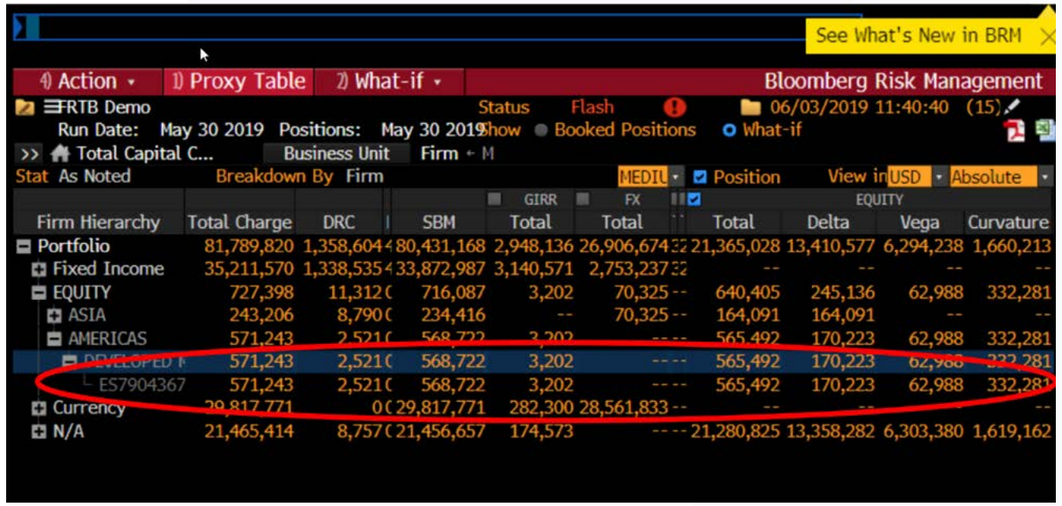
hedging effects

One variable is if and how, the bank hedges. This is because SA typically generates high capital charges for unhedged positions, but allows substantial netting when it recognizes a hedge. Banks will need to carefully assess how the hedges on their books will be treated under FRTB SA, and how the capital relief from hedging compares to that accorded today under Basel 2.5. Operationally, banks will need to do this analysis on demand for prospective trades, so as not to be surprised when a trade carries a high charge or a hedge turns out not to yield the capital relief the bank may have expected.

For example, suppose a client asks a large bank to write a close-to-the-money put option on 70,000 shares of Meridian Bioscience equity (ticker VIVO, current market price USD 11.3 per share), a maker of medical test kits. As of this writing, VIVO has a market cap of approximately USD 480M, classifying it as a small market cap stock.[4] Suppose further that the bank would like to delta-hedge with an exposure to the underlying, but finds itself having trouble finding that stock to short in the market.

4 / By paragraph 21.79 of https://www.bis.org/bcbs/publ/d457.pdf (the 2019 final version of the rules), companies with market cap under USD 2 billion are classified as small caps.

First, the bank might consider the impact of leaving the position unhedged. In calculating Sensitivities Based Method (SBM) delta and curvature, the bank needs to apply a risk weight of 50%[5] to a position with roughly 44% delta. A pre-trade analysis (see below using Bloomberg's MARS Market Risk FRTB-SA system) shows leaving the trade unhedged would result in a substantial SBM capital charge, as seen below for the line labeled "ES7904367":



Caption: Pre-trade FRTB-SA capital analysis for an unhedged short equity put option. (Source: MARS Market Risk.)

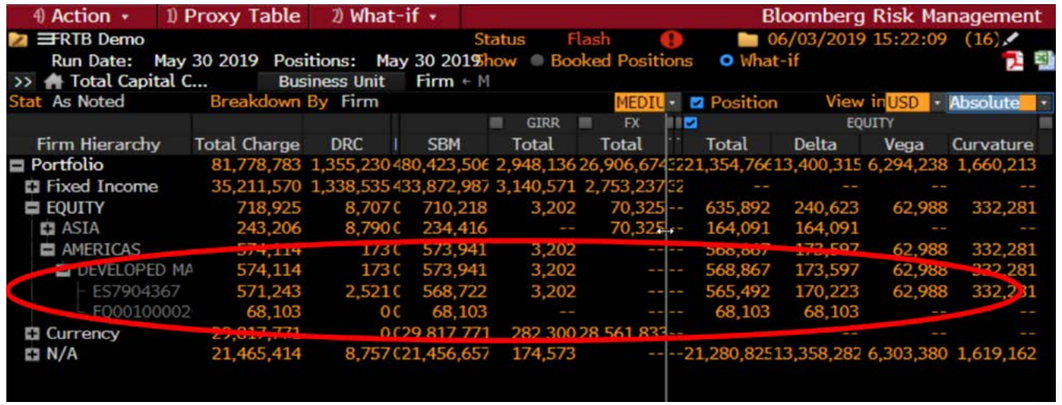
Next, the bank starts to look in earnest for a hedge. Say it quickly finds an opportunity to sell short a larger cap equity in the medical supplies sector, Abbott Laboratories (ticker ABT, current market price USD 75.5 per share). Before executing the trade, it runs another on-the fly pre-trade check of the capital impact. Here is a summary of the analysis, which we again ran using the pre-trade what-if screen in MARS Market Risk:

Since ABT's market cap is several orders of magnitude above the cutoff of USD 2 billion, it falls under equity risk bucket 5 for SBM (large market cap, advanced economy with a smaller risk weight of 30%). However, since the exposure and the hedge fall in different risk buckets, the bank may only apply a correlation of 15% to the pair under SBM.[6] If we think of the formula for SBM as a variant of parametric expected shortfall, we are adding a slightly negatively correlated (opposite sign delta) position. Because the correlation is slight, the volatility (risk weight) of each element will have a higher impact on the calculated risk of the pair than any offsetting correlation effect.

In our pre-trade analysis, we find that the short equity position (see line labeled "EQ00100002" and the "Developed Markets" line above the pair, which represents the capital of the two together) actually does not reduce the total delta charge of the Developed Markets book:

5 / See table in paragraph 21.77 of https://www.bis.org/bcbs/publ/d457.pdf, equity risk bucket 10, small cap market cap, advanced economy.

6 / By paragraph 21.80 of https://www.bis.org/bcbs/publ/d457.pdf.



Caption: Pre-trade FRTB-SA capital analysis for a prospective hedge finds that it fails to reduce the capital charge. (Source: MARS Market Risk.)

Of course, if the bank did manage to short the actual underlying, it would get more favorable capital treatment, as the risk factor driving the delta of both the option and the hedge would be the same, and the exposures would net. (Note however that even in this case, the vega and curvature charges associated with the option would not be offset.)

index treatment

Another class of cases where the treatment of hedges makes a substantial difference is when a bank has exposures to indices and funds. For example, the bank may write an option on an equity or credit index, and use a subset of the index constituents to hedge. To capture this properly, the bank needs to represent this exposure in terms of the index constituents, so that these can be offset against the hedge. The key challenge here is to capture the constituents and measure the exposure of the index position to each one. This is commonly referred to as taking a look through approach.

The final FRTB rule offers banks a partial choice under SA of whether or not to take a look through approach. To explain this, we recall that under SA, index exposures will typically incur two capital charges: one under the Sensitivities-Based Method (SBM), and another, typically smaller, charge under the Default Risk Charge (DRC). The original 2016 formulation of the rule required banks to take a look through approach to index exposures both for the SBM and for the DRC. This was relaxed somewhat in the final 2019 version of the rule, giving banks the option not to look through to constituents for SBM only (though look through is still required for the SA-DRC). Correspondingly, the final rule introduced new risk buckets representing index exposures (broken up into developed and emerging market buckets for equity, and into investment grade and high yield buckets for credit) to give banks a way of mapping index exposures if they choose not to look through.

While avoiding look-through modeling for SBM appears simpler for the bank, it can lead to higher capital charges, because opposite exposures to an issuer in the index position and in the hedging portfolio cannot net properly without using look-through.

For example, the correlations between exposures to equity index buckets and exposures to individual equity names are set at 45%.[7] While the effect here is less extreme than in our previous example, 45% is still not a high correlation, which drops even further in the "low correlation scenario" banks must consider as part of the SA calculation, leading to an even higher capital charge. This underscores the importance of having access to constituent data on both equity and credit indices and funds in order to be able to look through:

SX3P 1 748.49 +9.29
At 11:50 d 0 739.89 H 748.49 L 737.78 Prev 739.20
SX3P Index | Display | Export | Alert | Member Weightings
STOXX Europe 600 Food & Beverage Price EUR | 24 Members | Currency LCL
Members | Historical Summary
3) Stats | Group by None | 4) Fields | As of 06/03/2019

	Ticker		Name	Weight (%)*↓	Shares	Price
11)	NESN	SE	Nestle SA	31.263256	1,734.811526	101.4400
12)	DGE	LN	Diageo PLC	15.000089	1,997.320514	3,362.0000
13)	ABI	BB	Anheuser-Busch InBev SA/NV	12.384077	855.256613	73.0200
14)	BN	FP	Danone SA	9.316732	643.951888	72.9600
15)	RI	FP	Pernod Ricard SA	6.422988	203.711072	159.0000
16)	HEIA	NA	Heineken NV	4.493110	238.004280	95.2000
17)	KYG	ID	Kerry Group PLC	3.121814	152.251312	103.4000
18)	CARLB	DC	Carlsberg A/S	2.463325	105.652480	878.0000
19)	ABF	LN	Associated British Foods PLC	2.011179	360.132586	2,500.0000
20)	MOWI	NO	Mowi ASA	1.871484	438.685365	210.6000
21)	HEIO	NA	Heineken Holding NV	1.778929	100.176892	89.5500
22)	LISN	SE	Chocoladefabriken Lindt & Spruen…	1.457988	0.108557	75,600.0000
23)	ORK	NO	Orkla ASA	1.273852	824.824620	76.2400
24)	CCH	LN	Coca-Cola HBC AG	1.263688	198.563405	2,849.0000
25)	CPR	IM	Davide Campari-Milano SpA	0.788582	454.998720	8.7400
26)	TATE	LN	Tate & Lyle PLC	0.759273	468.308934	725.8000
27)	BARN	SE	Barry Callebaut AG	0.750684	2.170294	1,947.0000
28)	GLB	ID	Glanbia PLC	0.607051	202.732301	15.1000
29)	RCO	FP	Remy Cointreau SA	0.564662	23.169202	122.9000
30)	BVIC	LN	Britvic PLC	0.537371	265.227493	907.0000

9) Analyze List *Index Weight (%) Calculated by Bloomberg

Caption: Equity index constituents and weights. (Source: Bloomberg, as seen in the MEMB function on the Bloomberg terminal.)

looking ahead

Whether through explicit requirements in the rules, or through higher capital charges in case of modeling mismatches, FRTB is pushing banks to upgrade their market risk data, analytics, systems, and processes before the go-live date of 1 January 2022. The extreme variability that we see today in the QIS results may yet prove temporary, but there is substantial work ahead for many banks. But while FRTB certainly poses challenges, it brings opportunities as well, and as the deadline draws nearer, many banks are looking to enhance their risk platforms - not only to bring predictability to capital requirements, but to improve the accuracy and robustness of how they manage market risk.

7 / Again, see paragraph 21.80 of https://www.bis.org/bcbs/publ/d457.pdf.

MARKIT ITRX EUR SUB FIN 06/2 | 1) Export to Excel | CDS Index Member List

Index	MARKIT ITRX EUR SUB FIN 06/24	BB Number	ITXEU531
RED Code	2I667EBW1	Deal Spread (bp)	100
1st Accrual Start Date	03/20/19	Current Spread (bp)	181.1778/189.0099
Maturity Date	06/20/24	Version	1

Sector All | Pricing Source CBGN | Derived Spreads

	Company Name	Wgt	ISIN	RED Pair	Corp Tkr	5 Yr CDS Tkr	Spread (bp)
11)	Aegon NV	3.334	XS1061711575	007GB6AG7	AEGON	CAEG02E5	N.A.
12)	Allianz SE	3.334	DE000A1RE1Q3	DD359MAH9	ALVGR	CALZ2E5	N.A.
13)	Assicurazioni Generali SpA	3.334	XS0802638642	0E996BAE1	ASSGEN	CASS2E5	N.A.
14)	Aviva PLC	3.334	XS0138717441	GG6EBTAF3	AVLN	CAVL2E5	N.A.
15)	AXA SA	3.334	XS0122028904	FF667MAC0	AXASA	CAXA2E5	N.A.
16)	Banco Bilbao Vizcaya Argentaria SA	3.334	ES0213211099	EF2985AF8	BBVASM	CBBV2E5	N.A.
17)	Banco Santander SA	3.334	XS0291652203	EFAGG9AI0	SANTAN	CBSH2E5	N.A.
18)	Barclays PLC	3.334	US06738EAC93	GG8839AB6	BACR	CY349216	N.A.
19)	BNP Paribas SA	3.334	FR0010092189	05ABBFA06	BNP	CBNP2E5	N.A.
20)	Commerzbank AG	3.334	DE000CB07899	2C27EGAJ3	CMZB	CMZ2E5	N.A.
21)	Cooperatieve Rabobank UA	3.333	XS0429484891	NP489IAA8	RABOBK	CRAB2E5	N.A.
22)	Credit Agricole SA	3.333	FR0010138487	FH49GGAK7	ACAFP	CACA2E5	N.A.
23)	Credit Suisse Group AG	3.333	XS0118514446	HK9FHLAE1	CS	CCS2E5	N.A.
24)	Danske Bank A/S	3.333	XS1068866950	2F9999AM0	DANBNK	CDAN2E5	N.A.
25)	Deutsche Bank AG	3.333	DE0003933685	2H6677AF6	DB	CDB2E5	N.A.
26)	Hannover Rueck SE	3.333	XS0541620901	4F16FDAB0	HANRUE	CHAN2E5	N.A.

Caption: Credit index constituents and weights. (Source: Bloomberg, as seen in the MEMC function on the Bloomberg terminal.)

author

Eugene Stern

Global Market Risk Product Manager, Bloomberg LP

Eugene Stern is head of market risk products at Bloomberg, working on the firm's enterprise risk services business, which ties together market and reference data, instrument-level analytics for both risk managers and the front office. He helped start the business and has held a number of different leadership roles in product management, implementations, and client services.

Previously, Eugene spent ten years at RiskMetrics where he started as a quant researcher, building models for market and credit risk, and eventually moved to the business side, leading the product management team and overseeing all offerings across the risk business.

Eugene holds a Ph.D. in Math from UC Berkeley, and worked at the University of Pennsylvania as a lecturer in mathematics before beginning to work in risk.

the rise of the machines and how algorithmic trading has overtaken the market: the good and the bad

by **Alexander** Marinov

As the theme of this month's edition of Intelligent Risk is strategy risk perhaps it makes sense to discuss one of the biggest challenges within the financial industry and that risk is automatic trading.

what is automatic trading?[1]

It is the sets of processes and procedures designed by a group of highly specialized PhDs in creating a piece of software that drives decision making via a set of pre-defined triggers, signals, news or events a given outcome. In essence, it is a piece of software that makes split second decisions about potential investment opportunities in milliseconds.

There are two areas to explore - one is automatic trading, and the other is high speed trading.

Basically, high speed trading is a type of automatic trading that is very fast, very much focused on a very liquid asset class, such as equities, and one which requires a lot of investment in speed, reduction in latency and overall scale, so to complete thousands of thousands of simultaneous orders in one go.

what are the benefits?[2]

Markets operate on the notion of market efficiency. That is, there is the genuine interest of all parties to have fair prices that equalize supply and demand. If there is a short-term discrepancy, traders or investors would exploit it until that opportunity is no longer profitable, thereby bringing the market into equilibrium.

Having higher liquidity is beneficial for all parties in the economy as that means it is easier to sell goods and/or services and it helps reduce the bid/ask spreads by the sheer volume of the transactions that are being carried out.

The same goes for the financial markets, where a business might want to buy a foreign currency hedge to mitigate the fluctuations of their foreign revenue streams.

The other side is that algorithmic trading should remove any possibility for market collusion and cartels. Conspiracies, especially on the scale that we have seen over the last few years such as Libor and exchange rates would bring such instances to a minimum.[3]

what are the risks?

Some would argue that the risks from completely automatic trading are too great and that they could easily bring the wider economy. The fact is that a lot of trading is automated today and a lot more is about to come into the marketplace under the explanation that it would increase efficiency, decrease transaction costs and generally be beneficial for the whole economy.[4]

Such systems from the way they were designed to the way they operate they would require minimum to no human intervention. What is the harm in that?

Algo trading brings other problems as well. The code becomes too complex and not easy to disseminate, which makes decision making extremely hard, especially for the viability of executing large projects and transactions because they can bring erroneous data not just to a company but also to an exchange, thereby threatening the financial viability of the marketplace.

Another aspect that sometimes gets neglected has to do with the flaws that are present in these systems as they can come from numerous directions: 1) technical - where the issue may be present in the overall development, training, validation and checking of the system that could lead to an inaccurate output; 2) usage flaws - when the deployment of an algo can give false impression or bias in the decision making process of end users; 3) security flaws - where internal or external players have access to the data, design or even output and are able to manipulate it for their own gain.

A clear example of this is the case of Knight Capital. Due to failure of its automated system it executed millions of erroneous trades, both long and short, that ultimately led to a loss of close to $460 million and the ruinations of the company itself shortly after. Later it was acquired by a rival company - Getco LLC.[5]

Another clear example is the single biggest drop in the Dow Jones Index was caused in 2010 by a "flash crash" that caused the index to drop by 9%, equivalent to about $1 trillion supposedly triggered by algos overreacting to market news.

The main issue is that these algorithms are extremely opaque and in effect they are black boxes, where sometimes even the person who wrote them cannot be sure what their functionality might be once it is implemented in a real market environment. The fact is even the most sophisticated code, even the one based on machine learning techniques that tries to teach market dynamics, can become entangled in bias, false triggers or even unpredictability that untangling it can bring dire consequences.

The main flaw of an algorithm is the design and what information they are being fed. Sometimes when there are spikes in the market that could make the software react in strange ways and trigger vary drastic trading behaviors as the spike in the VIX in February 2018 showed, when the index doubled in one day.[6]

The biggest risk of all is the strategy risk for an organization because if an organization relies on such systems for its decision-making process it could exposure them to financial, operational and even reputation risks, which could have drastic consequences.

references

1 https://www.investopedia.com/articles/trading/11/automated-trading-systems.asp

https://www.investopedia.com/articles/active-trading/101014/basics-algorithmic-trading-concepts-and-examples.asp

https://www.ig.com/uk/trading-strategies/automated-trading-explained-181218

https://cointelegraph.com/explained/trading-bots-vs-humans-explained

https://theconversation.com/algorithms-have-already-taken-over-human-decision-making-111436

https://blog.quantinsti.com/growth-future-algorithmic-trading/

2 https://www.nasdaq.com/forex/education/advantages-of-algo-trading.aspx

https://medium.com/datadriveninvestor/how-automated-trading-can-increase-your-trading-profits-371ae1f828fe

https://www.mckinsey.com/~/media/McKinsey/Industries/Financial%20Services/Our%20Insights/Two%20routes%20to%20digital%20success%20in%20capital%20markets/Two-routes-to-digital-success-in-capital-markets.ashx

https://www.mckinsey.com/~/media/McKinsey/Industries/Financial%20Services/Our%20Insights/How%20the%20capital%20markets%20infrastructure%20industry%20is%20reinventing%20itself/How-the-capital-markets-infrastructure-industry-is-reinventing-itself.ashx

https://www.pewinternet.org/2017/02/08/code-dependent-pros-and-cons-of-the-algorithm-age/

3 https://www.theguardian.com/business/2017/jan/18/libor-scandal-the-bankers-who-fixed-the-worlds-most-important-number

https://www.investopedia.com/terms/l/libor-scandal.asp

https://www.cfr.org/backgrounder/understanding-libor-scandal

https://www.ft.com/content/1b63dd84-c8bc-11e8-ba8f-ee390057b8c9

https://www.independent.co.uk/news/business/news/rbs-barclays-fine-essex-express-cartel-currency-market-rigging-a8916981.html

https://www.bbc.co.uk/news/business-30003693

https://uk.reuters.com/article/global-currencies-scandal/timeline-the-global-fx-rigging-scandal-idUKL5N1F14VV

https://edition.cnn.com/2019/05/16/business/banks-foreign-exchange-fine/index.html

4 https://citywire.co.uk/wealth-manager/news/fca-algo-trading-could-make-small-errors-into-extreme-events/a1091478

https://business.nasdaq.com/marketinsite/2018/MT/Best-Practices-in-Algorithmic-Trading-Compliance.html

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/289016/11-1226-dr7-crashes-and-high-frequency-trading.pdf

https://home.kpmg/uk/en/home/insights/2017/06/stamping-out-conduct-risk-in-algorithmic-trading.html

https://blogs.deloitte.co.uk/financialservices/2018/02/effective-governance-of-algorithmic-trading-in-wholesale-markets.html

https://www.fca.org.uk/publication/multi-firm-reviews/algorithmic-trading-compliance-wholesale-markets.pdf

https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/risk/lu-risk-algorithmic-machine-learning-risk-management.pdf

https://futurism.com/professor-technology-controlling-us

https://www.pewinternet.org/2017/02/08/code-dependent-pros-and-cons-of-the-algorithm-age/

https://www.cnbc.com/2018/02/06/market-sell-off-driven-by-algorithms-strategist-says.html

5 https://dealbook.nytimes.com/2012/08/02/knight-capital-says-trading-mishap-cost-it-440-million/

https://medium.com/@bishr_tabbaa/the-rise-and-fall-of-knight-capital-buy-high-sell-low-rinse-and-repeat-ae17fae780f6

https://money.cnn.com/2012/08/09/technology/knight-expensive-computer-bug/index.html

https://www.bbc.co.uk/news/magazine-19214294

https://citywire.co.uk/wealth-manager/news/fca-algo-trading-could-make-small-errors-into-extreme-events/a1091478

https://news.efinancialcareers.com/uk-en/329751/jpmorgans-new-guide-to-machine-learning-in-algorithmic-trading

https://www.pinsentmasons.com/out-law/news/uk-regulators-to-tighten-rules-around-algorithmic-trading

https://medium.com/@alexrachnog/ai-for-algorithmic-trading-7-mistakes-that-could-make-me-broke-a41f94048b8c

https://www.investopedia.com/news/how-algo-trading-worsening-stock-market-routs/

6 https://www.bloomberg.com/opinion/articles/2018-02-14/is-vix-manipulated-or-hedged

https://www.bloomberg.com/news/articles/2018-02-06/credit-suisse-says-it-saw-no-losses-from-vix-linked-securities

https://www.cnbc.com/2018/02/06/the-obscure-volatility-security-thats-become-the-focus-of-this-sell-off-is-halted-after-an-80-percent-plunge.html

https://www.ft.com/content/2f478e8e-0c30-11e8-8eb7-42f857ea9f09

https://qz.com/1198961/dow-and-sp-500-plunge-while-vix-more-than-doubles-in-one-week/

https://www.bloomberg.com/news/articles/2019-02-06/the-day-the-vix-doubled-tales-of-volmageddon

author

Alexander Marinov

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

high business concentration as a source of strategic risk

by **Aleksei** Kirilov, **Valeriy** Kirilov

The article is devoted to the analysis of the irregular distribution of capital in the real sector and in the US banking system. The Lorenz curve and the Gini coefficient are used as the analysis tools. It is shown that the distribution of business, both in the real sector of the economy and in the US banking sector is extremely uneven. The Gini coefficient for assets in the banking sector over the past 27 years has increased to a value of 0.93. Such a high concentration of banking business reduces the stability of the US banking system and thereby increases the strategic risks for both banks and the economy as a whole.

The stability of the economic system depends on many factors, including the distribution of resources within the system. As a rule, a system with distributed resources is much more stable than a centralized system. The low resilience of the centralized system to external or internal influences may be one of the main strategic risks for the system as a whole.

For the study the real sector of the US economy and the US banking system were selected. The Lorentz curve[1] and the Gini coefficient[2] were used for the analysis. The values of capitalization of companies were used as initial data as of May 9, 2019. There were data on the capitalization of 4,332 US companies and banks traded on the stock exchanges. ETFs and other funds are not included in this number. Table 1 shows the distribution of the number of companies and their total capitalization in 9 sectors of the economy.

Sector	Number of companies	Total capitalization, mln USD
Technology	596	7,845,732
Financial	1,237	7,037,846
Services	642	5,705,817
Healthcare	720	3,883,593
Consumer Goods	287	3,456,423
Basic Materials	376	2,365,782
Industrial Goods	300	2,120,932
Utilities	80	990,011
Conglomerates	94	57,556
Total	4,332	33,463,694

Source: https://finviz.com

1 / The Lorenz curve is a graphical representation of the distribution of some parameter. It was developed by Max O. Lorenz to represent inequality in the distribution of wealth.

2 / The Gini coefficient is a measure of statistical dispersion, intended to represent some variable distribution, and is the most commonly used measure of inequality. Developed by Italian statistician Corrado Gini.

We have calculated the parameters of the Lorenz curve based on data on the market capitalization of these 4,332 companies. The calculation results are shown in Figure 1. In the same figure, the curve corresponding to the hypothetical distribution of capital, at which the maximum entropy value would be achieved, is constructed. A straight line corresponds to an absolutely uniform distribution.

As can be seen from Figure 1, the actual distribution of companies by capitalization is extremely uneven, the calculated Gini coefficient is equal to 0.87.

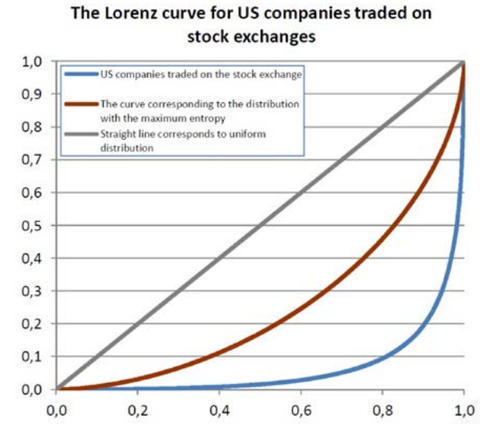


Figure 1

Lorentz curves were constructed and Gini coefficients were calculated for all 9 sectors. The calculation results are shown in Table 2.

Sector	Total capitalization, mln USD	Gini coefficient
Healthcare	3,883,593	0.90
Technology	7,845,732	0.88
Financial	7,037,846	0.87
Consumer Goods	3,456,423	0.86
Services	5,705,817	0.85
Basic Materials	2,365,782	0.82
Industrial Goods	2,120,932	0.82
Conglomerates	57,556	0.74
Utilities	990,011	0.62

Table 2

As can be seen from Table 2, the highest values of Gini coefficients are observed in the following sectors: Healthcare, Technology, Financial, and Consumer Goods. As an example, Figure 2 plotted the Lorenz curves for Healthcare, Consumer Goods and Utilities.

The Gini coefficient for the “quasi-equilibrium state” with a maximum entropy is 0.5. Thus, the value of the Gini coefficient of all 9 industries is much higher than the value of the Gini coefficient for the “quasi-equilibrium state”. The values of Gini coefficients for the sectors Healthcare, Technology, Financial, Consumer Goods are especially great. The high Gini coefficient values for these sectors reflect an extremely high degree of stratification in terms of capitalization. Thus, the share of companies with huge capitalization is very high.

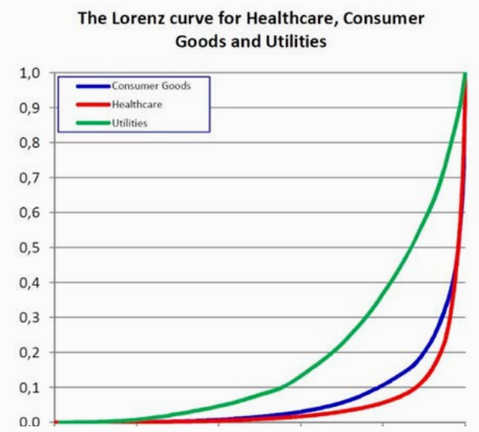


Figure 2

This, of course, means an increased level of risk for these sectors in the event of a sharp decline in the capitalization of one of these companies. Thus, the extremely high stratification of companies in terms of capitalization creates a strategic risk.

In our opinion, the dynamics of changes in the distribution over time is of considerable interest. Such analysis was made on the basis of data on the US banking system, available at https://www.usbanklocations.com. The change in time distribution of banking assets was investigated.

Figure 3 shows the Lorenz curve for the distribution of assets of all US banks as of the end of 2018. Note that this is not capitalization, but the assets of banks. The Gini coefficient in this case is 0.932. In the same figure, the lines corresponding to the hypothetical distribution of assets, at which the maximum entropy value would be achieved, as well as the absolutely uniform distribution of assets, are constructed. Similar calculations were made for the assets of Russian banks as of the end of 2018, data source http://www.finmarket.ru/database/rankings.

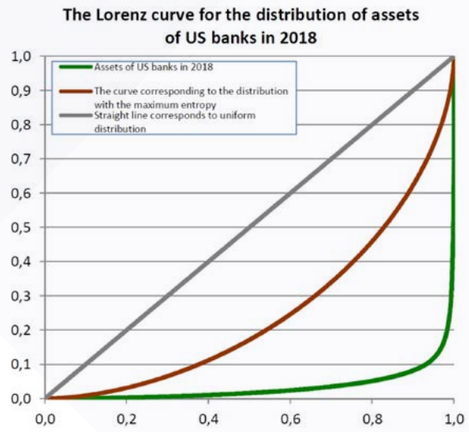


Figure 3

In this case, the Gini coefficient was also 0.932. It is known that the Russian banking system has a high proportion of state-owned banks. For example, the share of assets of the six largest banks under state control is 64.6% of the assets of the entire banking system of the country. Some state-owned banks, for example Russian Agricultural Bank (fourth in terms of assets), regularly received financial support from the state to cover losses due to poor asset quality. The Central Bank of Russia recently was forced to capitalize and take control of Promsvyazbank (ninth by assets) and Otkritie Bank (seventh by assets), also because of the poor quality of assets. Therefore, the stability of the Russian banking system is assessed very cautiously by the leading rating agencies.

The equality of Gini coefficients for the assets of American and Russian banks, that is, the equally high level of concentration of banking business in both countries with a completely different structure of the economy is extremely surprising, and raises big questions about the sustainability of the American banking system.

According to our assumption, there may be two probable explanations for this coincidence of Gini coefficients. First, over the past 10 years, due to various reasons, primarily the tightening of regulatory requirements, the number of banks both in the United States and in Russia has decreased significantly. In the USA almost by 35%, in Russia almost by 56%. And probably most of the business of liquidated banks passed to the largest banks. Secondly, in both countries, it was banks that became the beneficiaries of the economic policy being pursued. In the US, this was a quantitative easing (QE) program implemented by the Fed after 2008, in Russia it was foreign exchange earnings from the export of oil, gas, coal, metals, etc.

Let us analyze how the Gini coefficient changes over time for the distribution of assets of American banks. Figure 4 shows the values of the Gini coefficient for the distribution of assets of American banks from 1992 to 2018.

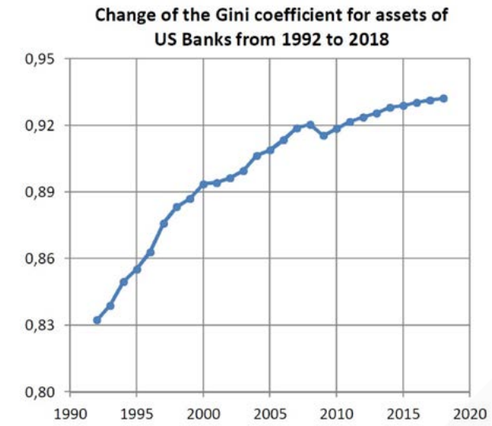


Figure 4

As can be seen from the data presented, the degree of stratification by assets among banks increases, that is, the concentration of banking business increases. This reflects the increased risk to the banking system in the event of serious problems in one or more of the largest banks. What was already observed during the financial crisis of 2007–2008 and the bankruptcy of Lehman Brothers. In other words, several banks appear in the system again, which can be defined as “too big to fail”, see for example [1] - [5].

Figure 5 shows the annual increment of the Gini coefficient for assets of US banks as well as increment of the US GDP (the sources https://tradingeconomics.com, https://data.worldbank.org). As can be seen from the figure, the change in the Gini coefficient correlates quite well with the general state of the economy. Correlation coefficient is 0.75; R2 = 0.56.

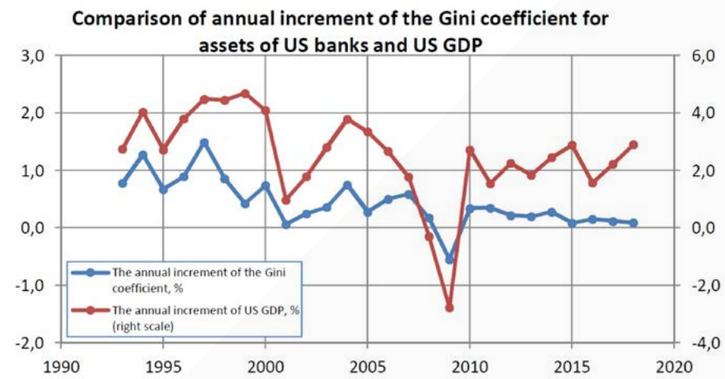


Figure 5

In conclusion, we note that the Gini coefficient can be used to analyze the degree of concentration of business both in the economy as a whole and in individual industries. Under certain conditions, too high concentration of business can be a source of strategic risk. And the Gini coefficient can be used as a measure of such risk.

references

1. Dash, Eric (20 June 2009). “If It’s Too Big to Fail, Is It Too Big to Exist?”. New York Times. Retrieved 16 September 2012, https://www.nytimes.com/2009/06/21/weekinreview/21dash.html
2. “History of the Lehman Brothers”. Harvard University Library-Lehman Brothers Collection. Retrieved December 1, 2010, https://www.library.hbs.edu/hc/lehman/Exhibition/Introduction

references

3. Mollenkamp, Carrick (September 16, 2008). “Lehman Files for Bankruptcy”. Wall Street Journal. Archived from the original on December 22, 2010. Retrieved December 22, 2010, https://www.wsj.com/articles/SB122145492097035549
4. Richard W. Fisher; Harvey Rosenblum (March 10, 2013). “Fisher and Rosenblum: How to Shrink the ‘Too-Big-to-Fail’ Banks”. Wall Street Journal. Retrieved 14 March 2013, https://www.wsj.com/articles/SB10001424127887324128504578344652647097278
5. Who Is Too Big To Fail: Are Large Financial Institutions Immune from Federal Prosecution?: Hearing before the Subcommittee on Oversight and Investigations of the Committee on Financial Services, U.S. House Of Representatives, One Hundred Thirteenth Congress, First Session, May 22, 2013, https://www.govinfo.gov/content/pkg/CHRG-113hhrg81760/pdf/CHRG-113hhrg81760.pdf

authors

Aleksei Kirilov

Partner at Conflate LLC

Conflate is a Russian management consulting company specialized in strategy, risk management, asset management and venture investment. As the partner of Conflate, Aleksei is responsible for asset management and venture investment. He specializes in the US stock and debt markets. Aleksei has more than 15 years of experience in financial services including development of financial strategy and financial KPI, liquidity management; controlling system, allocation of expense on business unit, financial modeling and debt finance. He has cross industries experience: banks, oil & gas manufacturing, real estate.

Aleksei has an MBA from Duke University (Fuqua School of Business), a financial degree from Russian Plekhanov Economic Academy and an engineering degree from Moscow Engineering Physics Institute.

Valeriy Kirilov

General Manager at Conflate LLC

Valeriy has 15+ years’ experience in risk management and management consulting (BDO, Technoserv, then at Conflate). Besides he previously worked in the nuclear power industry (safety of Nuclear Power Plants).

Valeriy has an MBA from London Metropolitan University as well as a financial degree from Moscow International Higher Business School MIRBIS and an engineering degree from Moscow Engineering Physics Institute. He holds the PRM and FRM certifications and the certificate of Federal Commission for Securities Market of series 1.0. Valeriy was a member of the Supervisory board of the Russian Risk Management Society in 2009 – 2010.

interview with Arnaud De Lavalette, senior project manager ADA* in charge of the Digital Finance Initiative

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

2 billion people lack a financial account in emerging economies. There is an up to **90%** lower cost from providing digital rather than physical accounts.

Adam Can you describe the Digital Finance program and its goals?

Arnaud The Digital Finance Initiative (DFI) was established in 2017 to help microfinance institutions (MFIs) to define and to implement their digital strategy. Many in microfinance think of “digital strategy” as mobile banking, but this is a much broader look than that, taking into account all systems within the organization in order to improve their financial and social performances and, as a consequence, to favor financial inclusion in their country. We look to innovators and help them accelerate the development of financial inclusion by encouraging them to open up new alternative distribution channels to improve their geographic coverage and to offer new innovative products and services to their beneficiaries and/or to improve their operational efficiency.

Adam Can you provide an example?

Arnaud Initially, the Digital Finance Initiative is aimed at the small and medium-sized MFIs (Tier II and Tier III) based in sub-Saharan Africa, the majority of which are members of the group of the Least Developed Countries. These are often remote areas, where electricity, skilled staff and technology support can be challenging to deliver and maintain. We provide these MFIs the benefit of support of a dedicated team which helps them to identify their needs, to identify the digital solutions and “roll up our sleeves” implementation help. We usually provide a financial contribution, as well as support to manage the project once we have all agreed to a strategy that makes sense for all the stakeholders.

When an MFI has a physical counter where business is transacted, their risks are perceived as somewhat manageable. When you add data collection and management, mobile banking and other digitally managed products, the risk becomes more robust and something new for many microfinance providers. Protection of data, integration with 3rd party platforms, and cyber security become all important as they expand their capabilities and products they offer. Only a few MFIs are taking advanced precautions, and we discuss early the risk associated with a digital implementation to make sure we address its importance.

Adam So, are these MFIs starting from scratch?

Arnaud Some are, and some have legacy systems. This can be a challenge for them, as often they have outgrown them or recognized the issues of having one when an employee is recruited elsewhere - leaving them without the inhouse expert to support the system.

We recommend cloud-based systems for reliability and for features, but they too create a new level of risk, so we make sure the MFI has the tools they need to make the proper decision on the approach that makes the most sense for them and the people they serve. Unfortunately, our organization, ADA, is one of the few that is there as an unbiased consultant and implementor. I wish there were more.

Adam Describe the process ADA takes

Arnaud **Step 1: Initial workshop to identify the priorities**

The DFI workshop brings together MFI senior managers for a week. It aims to give them a complete vision of the various challenges, opportunities and constraints represented by the new technologies. It gives them the keys to analyze all possible scenarios for integrating digital into their strategy and to evaluate the expected impacts in technical, operational, financial, and regulatory terms. The aim is for participants to emerge from the workshop with clear ideas about the digital strategy they wish to adopt.

Step 2: Pre-project phase: establishing a digital project

MFIs that wish to continue the adventure first have their new project validated by their governance. Then, supported by me and local consultants, they can launch their action plan. This plan provides for the establishment of specifications, the publication of calls for tenders and the selection of technical service providers, the establishment of a schedule, and finally the drafting of a co-financing file which will be submitted.

Step 3: Pilot phase: implementation of the digital project

After acceptance of the file by the Committee, the implementation of the project can start with a pilot on the scale of one or two agencies. At this stage, ADA offers the MFI financial support, as well as support in all areas impacted by the project: redefinition of procedures, staff and client training needs, risk management. As soon as the test phase is complete and conclusive, the MFI deploys the project throughout the network. It is at this moment that the accompaniment of ADA stops, having then considered the institution as autonomous.

Adam It sounds like important work.

Arnaud It is very rewarding and has tremendous impact as underserved people become exposed to new products that can be truly life changing. We make sure the digital solutions are well thought out, mitigate risks, and can adapt easily to the future.

**ADA is a founding Member of the Risk Initiative in Microfinance and a contributor to the creation of the RIM Graduation Model utilized by PRMIA-RIM members. To learn more visit www.riminitiative.org or www.prmia.org.*

author

Arnaud de Lavalette

Arnaud de Lavalette, Senior Project Manager, is currently leading the Digital Finance Initiative at ADA, helping African MFI digitalize their operations. He is a seasoned expert in microfinance and SME funding with over 10 years of experience in this domain in Asia (Nepal, India and Philippines), West Africa and Latin America (Mexico).

In the SME domain, Arnaud has worked in Nepal where he conducted surveys for the IFC and supported SME entrepreneurs with the European Commission. In India he designed an investment vehicle (equity fund) which aimed at supporting Indian social SMEs.

In the microfinance sector – beside many technical assistance missions around the world, he managed the turnaround and sold MicroCred Mexico, and more recently was CEO of mBank Philippines, a greenfield banking project financed by international investors (FMO, Finnfund, MBH) and Smart the leading telecom company in the Philippines.

Currently, he works with ADA on a new digital finance project, helping African MFI digitalize their operations, i.e. integrate the mobile services as communication and distribution channels and migrate MIS into the cloud. As of now, half a dozen institutions are accompanied in their change process.

Prior to joining the development sector Arnaud gained a bright experience in both finance and new technologies. He started his career as an auditor with Arthur Andersen (3 years), evolved as a controller and finance analyst (3 years) and founded a web agency he has managed for 7 years.

Insights from a statistical analysis of cybersecurity data breaches

by **Thomas** Lee, PhD and **Nagaraja** Deevi

Cybersecurity risk is difficult to estimate, difficult to communicate and difficult to understand, especially for the non-expert. This is a problem because the non-expert includes people who set priorities and resources such as senior management, the board of directors and government regulators. Another problem is that, since large data breaches are rare, non-experts often don't realize one has taken place until it is too late.

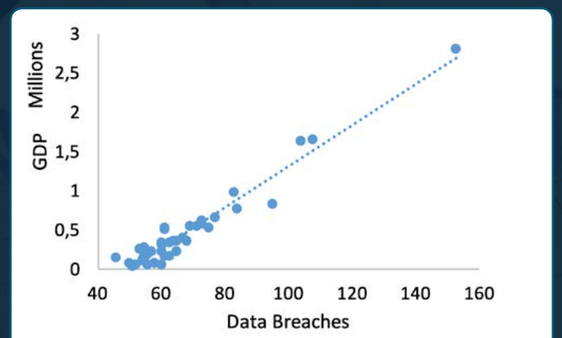
what the data revealed

We recently concluded a statistical analysis of the 2018 data breaches from Maryland State Attorney General[1] and were surprised by what the data seemed to be telling us: there is a simple way for non-experts to characterize cybersecurity risk.

Data breaches made public through Maryland Attorney General are special in that they involve companies located across the entire United States, they include all types of Personally Identifiable Information (PII) data and they represent the full range of data breach sizes. Because of these properties, we were able to use this source to estimate how many PII data breaches were not captured and, therefore, how many total PII data breaches occurred across all of the United States.

We performed our analysis by looking for patterns in the data using regression models, and our first model found that the number of annual data breaches per state is directly related to the state's gross domestic product (GDP)—with a surprisingly good R-squared of 95%.

This is surprising since, with something as random as data breaches, which are prevented with an array of complicated cybersecurity controls, we are accurately characterizing the number, state-by-state, with just the state's GDP.



Plot of the number data breaches by state, plotted against state GDP. We have corrected the number of observed data breaches by the number of missing due to distance from Maryland. The graph shows that the number of breaches by state are not as random as expected.

GDP correlates to the number of data breaches in states with small populations, like Nebraska or Alaska, as well as in states as large as California, New York or Texas, and in states with economies as seemingly diverse as California and Iowa. An R-squared of 95% means there is little randomness in the number of data breaches and that, while data breaches are random on the microscopic level, they are predictable on macroscopic level.

This means that data breaches can be characterized, and that we can draw general conclusions about how to reduce them.

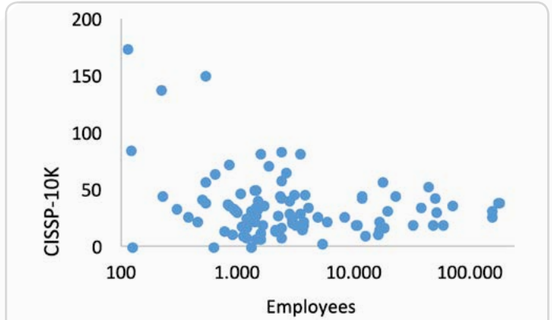
a surprisingly simple relationship

Our second model characterized the differences between companies that experienced data breaches and companies that did not. We focused on factors that were publicly available for both sets of companies. One factor we could measure across all companies is the number of trained cybersecurity employees. Since the most common cybersecurity training certification is the CISSP[2], we used this certification to establish a metric: the number of CISSP certified employees per 10,000 employees in each company (CISSP-10K).

We were surprised to find that the probability of a data breach was a strong function of the lack of certified employees, based upon company size. Said differently, companies with a low CISSP-10K ratio were overrepresented among companies that experienced data breaches in 2018. Even more telling, among companies that experienced large data breaches, the CISSP-10K ratio increased significantly post-breach. Apparently, these companies were reacting to the consequences of the data breach and bolstered their cybersecurity.

This simple, yet strong relationship between CISSP-10K and probability for data breach was a surprise, because cybersecurity is complicated.

We therefore assumed that this simple metric must be a proxy for something that we could not measure: perhaps cybersecurity spending, perhaps the number of cybersecurity controls, perhaps the ability of the CISO to communicate risk and secure budget. But when we looked at the heavily regulated banking industry, where we assume a uniform and robust deployment of security controls, we were surprised at the variability in the headcount of trained cybersecurity employees: the CISSP-10K ratio varied by more than an order of magnitude, and this variability was consistent with the pattern of data breaches in 2018.



CISSP certified employees per 10,000 employees (CISSP-10K) for 100 banks, plotted against company size by employees. The graph shows a large variation in trained cybersecurity headcount, which strongly correlates with probability of data breach. Some banks are actually quite large yet have zero CISSP trained employees.

Some banks with more than 1000 employees actually had zero CISSP certified employees. Of course, very large banks had hundreds of CISSP certified employees, but it was a low ratio of CISSP to total employees that we found to be predictive of a data breach.

We see a clue to the large variability in the CISSP-10K ratio when we look at a city like Atlanta, where several companies have experienced large data breaches over the last couple of years, and where trained cybersecurity employees are simply moving from one company to another, following the latest large data breach.

The large variability in CISSP-10K in a heavily regulated industry, and the movement of trained employees from one breach to the next, suggest that companies are competing for a limited supply of trained cybersecurity employees to implement their cybersecurity programs.

message to C-suite, boards and regulators

We don't mean to imply that CISSP certification is the most important, but this most common certificate does show us that the ratio of trained employees is important. We don't mean to imply that simply hiring trained people is the answer, but our analysis does suggest that a trained workforce is the foundation upon which to layer effective controls and management support. If you are the CEO, the CFO or board of directors, we don't mean to imply that you should micro-manage the security budget: leave that to the CISO, the person trained to manage your cybersecurity.

But if you do help decide the priority of cybersecurity, a simple way to assess risk is to compare the ratio of trained cybersecurity employees against your industry average—if you don't have more, you don't have enough. Average is not enough because our analysis shows companies that are average still have a significant probability of a data breach. One can see how average is not enough by simply pairing the approximately 7 million firms in the United States (according to the United States Census Bureau) with the approximately 85 thousand trained cybersecurity people (according to (ISC)2)[3], the average per company overall, is less than one.

There is clearly a shortage of trained cybersecurity people and our analysis of 2018 data breaches suggest that this is an important limiting factor for companies to reduce the frequency of data breaches. In regulated industries like healthcare and banking, the current focus by regulators is not likely to be effective, since we see wide variability from company to company in the ratio of trained employees—and the supply is limited. If we want to see an improvement in cybersecurity—training is the key.

1 / Security Breach Notices, www.marylandattorneygeneral.gov

2 / Certified Information Systems Security Professional – for more details, consult https://en.wikipedia.org/wiki/Certified_Information_Systems_Security_Professional

3 / Member count from www.isc2.org/About/Member-Counts

authors

Dr. **Thomas** Lee

Dr. Thomas Lee is the chief executive at VivoSecurity, with decades of experience pioneering methods in statistical analysis, image processing and digital signal processing for science, industry and cyber risk. Thomas has degrees in physics, electrical engineering and a PhD in Biophysics from the University of Chicago. He has multiple patents and papers published in peer-reviewed journals and is an expert in software, operating systems and hardware vulnerabilities, and enterprise operations. He is a recognized expert in quantifying Operational Risk, including fraud and cyber-risk, and a frequent speaker at events such as PRMIA and Op Risk North America and the Federal Reserve's Research Conferences.

Nagaraja Kumar Deevi

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

how the federal home loan bank system builds capacity at its member institutions

by **Melissa** Deven and **Jessica** Nick

strength of the federal home loan bank (FHLBank) system

Liquidity risk is the risk an institution may not be able to meet short-term financial commitments. This typically occurs due to the inability to convert a security or hard asset to cash without a loss of capital or income. During the 2007 financial crisis, financial institutions experienced increased demands for cash, largely from existing borrowers, as well as from counterparties and short-term creditors. As a result, liquid assets fell across financial institutions, while demand for cash continued to rise. In order to meet this demand, many institutions turned to wholesale funding sources, such as debt markets, brokered CDs (BCDs), repos, and fed funds; however, these sources began to dry up. During this same time period, the FHLBank System issued debt in the capital markets in order to increase its lending to institutions, as shown below in Figure 1.

Historical FHLBank system advances (in billions)

Figure 1.

Source: Office of Finance; as of 2018

The FHLBank System – comprised of 11 separate Home Loan Banks – provide contingent liquidity, funding for mortgages and asset liability management, and additional funds for housing finance and community development to approximately 6,800 member institutions across the United States (Office of Finance, March 2019). Member institutions include thrifts, commercial banks, credit unions, insurance companies, and community development financial institutions. As a Government Sponsored Enterprise, the FHLBank System has access to robust capital markets, which enables it to provide competitively priced funding.

a contingent and everyday liquidity source

The FHLBank System has a safe and reliable record as a wholesale funding source relative to other sources such as debt markets, BCDs, repos, and fed funds, which was proven during the 2007 financial crisis. Member borrowings from the Federal Home Loan Bank of Chicago (FHLBank Chicago) rose by more than 50% from Q1 2007 to Q3 2008. In a FHLBank member's SEC filing, it stated: "The Corporation maintains diverse and readily available liquidity sources…The Bank pledges eligible loans to the FHLBank as collateral to establish lines of credit and borrow from the entity." Figure 2 below depicts a decline in other wholesale funding sources following the last financial crisis while FHLBank advances grew to be the primary wholesale funding source at Illinois and Wisconsin bank and thrift financial institutions.

The FHLBanks are dependable liquidity providers as credit is only extended on a secured basis. The System has proven its reliability by not sustaining any credit losses on member institution borrowings for 87 years. The FHLBank System continues to expand eligible collateral classes and improve the pledging process in order to generate higher contingent liquidity and borrowing capacity for member institutions. Both securities and loans are eligible to be pledged as collateral. Categories include single-family 1-4 residential first liens, agency MBS/CMOs, multi-family loans, commercial real estate, home equity loans, and additional classes. As of year-end 2017, the total book value of the FHLBank Systems' eligible collateral rose to $3 trillion with a reported borrowing capacity of $2.2 trillion!

Illinois and Wisconsin bank & thrift wholesale funding

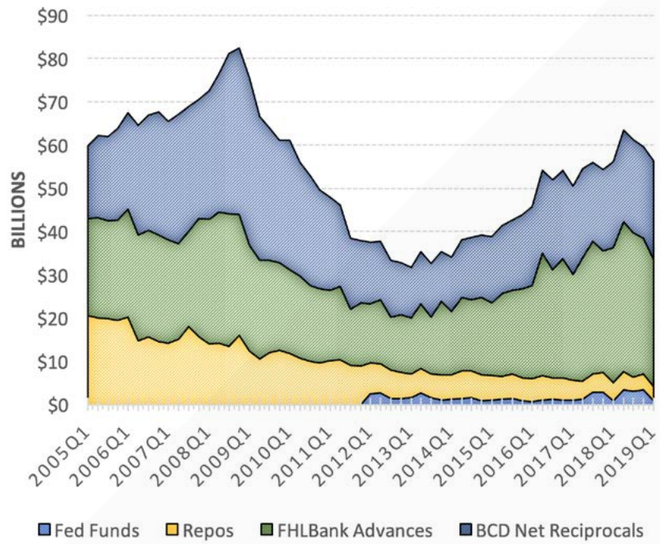


Figure 2.

Source: FDIC; as of 2019 Q1

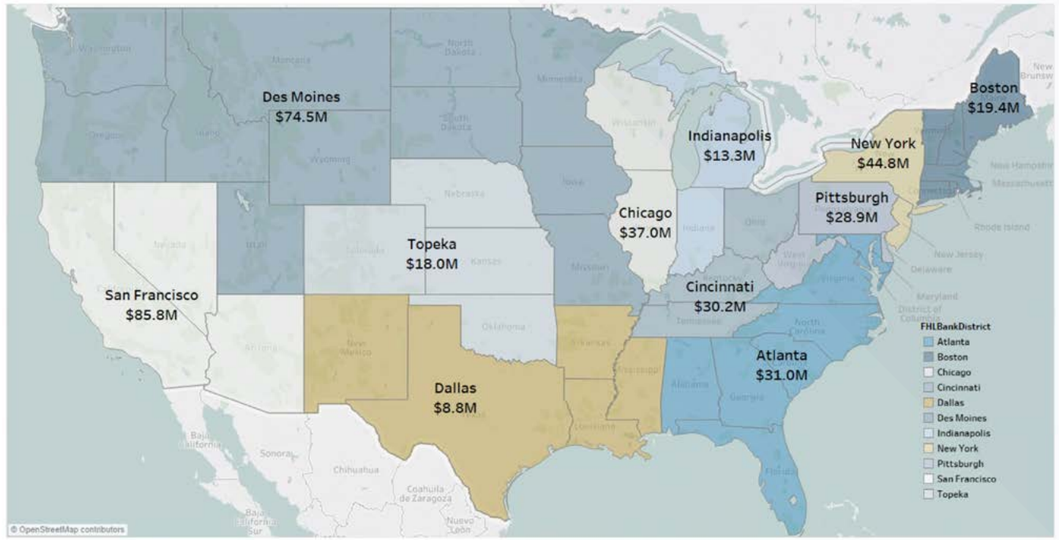
Member institutions not only view the FHLBank System as a source of back-up liquidity but also view it as a source of everyday liquidity. Approximately 80 percent of U.S. lending institutions rely on the FHLBank System (Federal Housing Finance Agency, April 2019). Federal oversight and standard bank regulation helps each FHLBank remain conservatively managed and well capitalized.

community investment funding

At any given time, a substantial number of member institutions use FHLBank loans to make a difference in their communities. In addition to providing on-demand liquidity, the FHLBank System promotes community development through two of the nation's most successful ongoing housing initiatives: The Affordable Housing Program and the Community Investment Cash Advance Program.

The Affordable Housing Program (AHP) stimulates lending efforts by FHLBank members by supporting homeownership financing programs and the accessibility of rental housing for low- to moderate-income applicants. In 2017, the FHLBanks awarded nearly $400 million in funding and supported over 40,000 housing units as depicted in the map in Figure 3. Since the program's inception in 1990, the FHLBanks have awarded approximately $5.8 billion in funding, which has supported approximately 865,000 housing units throughout the United States.

2017 FHLBank Statutory Contributions*



*Individual FHLBank statutory contributions are based on each FHLBank's earnings from the previous year

Figure 3. Source: FHFA; as of 2017

Additionally, the Community Investment Cash Advance Program also encourages the FHLBank's core mission by providing discounted funding to members in order to support the financing of housing or other economic development initiatives to benefit low- and moderate-income households and neighborhoods. In 2017 alone, the FHLBank System collectively funded approximately $4.6 billion for housing projects, $97 million for economic development projects, and $3.8 billion for community development projects. These projects range from commercial, industrial, and manufacturing projects to social services and public facilities.

"In our opinion, within the U.S. housing finance policy framework, the FHLB System has a critical public-policy role, as one of the most important national liquidity providers to U.S. mortgage lenders, particularly during stressful conditions, when private-sector liquidity often proves unreliable. We believe the critical nature of this role was clearly demonstrated in the U.S. mortgage crisis of 2008, during which advances (loans to client-owner members) outstanding peaked at $1 trillion. Since then, with the ebb in financial stress, advances have declined as member institutions regained access to alternative funding sources for mortgages, particularly deposits. In addition, the system provides some support for affordable housing and community investment programs." (Standard & Poor's, October 2015)

conclusion

In summary, the FHLBank System is an increasingly central funding source for institutions in the United States driven by its balanced and diversified funding position. During the early part of the last financial crisis, the FHLBank system played a central role as a "lender of next-to-last resort" by providing funding to its membership. As the economies in Wisconsin and Illinois have improved and loan demand has climbed, the FHLBank System and its members have worked together to provide funding for housing, businesses, and investments to fuel growth in communities.

authors

Melissa Deven Senior Analyst, AVP / Federal Home Loan Bank of Chicago (FHLBank Chicago)

Melissa Deven is a Director of Member Strategy and Solutions at the Federal Home Loan Bank of Chicago. Ms. Deven has been with the FHLBank Chicago for 7 years and she uses her financial industry knowledge and understanding of the mortgage market to benefit the members she serves. Prior to this role, Ms. Deven worked on the Member Transactions Desk at the FHLBank Chicago, and previous to that Ms. Deven worked on the Collateral Operations and Safekeeping group at the Bank. Ms. Deven received her Bachelor of Science in Business Administration in 2012 and MBA in 2016 from Indiana University.

Jessica Nick Analyst, Member Strategy and Solutions / Federal Home Loan Bank of Chicago

Jessica Nick is an Assistant Director of Member Strategy and Solutions at the Federal Home Loan Bank of Chicago. Jessica joined the FHLBank Chicago two years ago, where she has gained valuable insight and knowledge on depository funding strategies, asset liability management, and FHLBank Chicago products and solutions. Jessica also assists the team through her data analysis and visualization skills to develop strategies for member institutions to better serve their needs.

Prior to joining the FHLBank Chicago, Jessica graduated summa cum laude with a Bachelor of Science degree in Finance and a minor in Data Analytics from Arizona State University in 2016.

can a globally endorsed business identity code be the answer to risk data aggregation?

by **Allan** D. Grody

The financial crisis and its aftermath taught us that the activities and risks of global financial institutions transcend sovereign boundaries of regulation. It also taught us that the ability of regulators to observe risk building up in the financial system is critically dependent on a more granular and timely view of aggregated financial transaction data. Regulators embraced these revelations and embarked on a series of published consultations to define global initiatives that would standardize and uniquely identify market participants and their contracts and financial instruments. These standards would be embedded in financial transactions and used to identify and aggregate financial transaction data. It would make possible the long-sought means to efficiently aggregate data into meaningful and timely input for analyzing any single firm's enterprise risk and, ultimately, multiple firms' systemic risk.

A fundamental observation of our digital era is that the financial industry has evolved to rely almost completely on a technology-based ecosystem. Information technology has increasingly replaced human involvement in the life cycle of financial transactions with software applications operating across globally networked computers. This level of automation in financial services gives the appearance of a smoothly functioning digital-age industry where straight-through-processing rules, human interaction is minimized, algorithms control trading, and risk models mitigate risk.

In reality, the smooth functioning of all of these automated processes is dependent on improvements in a fundamental pillar of finance, data standards. Multiple handoffs of financial transaction data amongst and between financial institutions, regulators, and hundreds of financial market utilities relies on translating thousands of non-standard data elements, including hundreds of identifiers for the same financial market participants.

In the aftermath of Lehman Brothers failure in 2008 it was revealed that neither Lehman nor its regulators; nor its clients, creditors and counterparties had a common understanding of the risk exposure that existed at Lehman. That common understanding required a common identifying code that computer software could interpret as Lehman Brothers. That this did not exist over all the generations of technology that financial systems evolved through was a revelation to all.

This revelation drove the Group of Twenty's (G20's) newly appointed global standards body, the Financial Stability Board (FSB) in 2010 to sanction a series of global data standards initiatives. This included the global legal entity identifier (LEI) initiative, a unique, unambiguous and universal code for business entities participating in the financial system. This was to become a universal standard to eventually replace all proprietary codes used to identify business entities across the global financial supply chain.

Another significant lesson learned from the global financial crisis was that banks' information technology and data architectures were inadequate to support management of financial risks. Because of weak risk data aggregation capabilities many banks lacked the ability to aggregate risk exposures and identify concentrations quickly and accurately at the bank group level, across business lines and between legal entities. This required a more granular view of risk, a view at the transaction level to compliment the position and balance sheet levels that were the cornerstone of the global risk agenda to that point.

Without computers knowing the precise digital fingerprint, the 'financial barcode' of a financial transaction, too many automated processes fail, manual reconciliation intervenes, delays in payment occurs, risk and costs increase, and the vision of a seamless automated supply chain remains unfulfilled. To compound the problem, a formal discipline of risk management had been imposed by regulators on a mainly unintegrated technology ecosystem that embodies legacy software applications running back, middle and front office operations of both financial service firms and financial market utilities. Data mapping of thousands of non-standard digital fingerprints between these systems adds to quality deficiencies in risk data and significant time delays in risk reporting.

The Bank for International Settlements' Basel Committee on Banking Supervision (BCBS) has stepped in and asked regulators to oversee formal technology upgrade programs and data aggregation processes for financial institutions. The initiative is known as BCBS239 (Principles for effective risk data aggregation and risk reporting). BCBS239 has generated new and significant demands for data standards and technology upgrades at financial institution. It suggested that the use the LEI would facilitate its risk and data aggregation framework now being implemented by the global systemically important banks (G-SIBs).

In the US, pending legislation H.R.1530 - 115th Congress (2017-2018): Financial Transparency Act calls for common identifiers for information reported to financial regulatory agencies or collected on behalf of them. This includes a common legal entity identifier (presumably the LEI but not specifically referenced in the legislation) and common data formats. Prior attempts to have each of the eight (8) major regulatory agencies under the Financial Stability Act of 2010 (also known as the Dodd-Frank Act or the Wall Street Reform and Consumer Protection Act) initiate their own mandates proved unmanageable.

Finally, the FSB recently completed a consultation, a Thematic Peer Review of the LEI in which they solicited input from industry members and analyzed responses to a questionnaire developed by regulatory members to survey their individual constituencies. In summary, the FSB sees LEI adoption in absolute terms as relatively low. The issuance of LEIs is mainly concentrated in Canada, the EU and the US where it is estimated that coverage ranges from 2% to 7% of all eligible legal entities in their respective territories.

In these three territories, the FSB states that the LEI has come the closest to meeting the G20's objective. However, the initial and single most important use of the LEI was to be in trade aggregation across sovereign borders in OTC derivatives markets. Trades with the LEI included, along with associated financial transaction data, are being reported to one of twenty-five (25) trade repositories. Aggregation across these repositories is not yet functional even though 1.4 million LEIs have been issued, mainly for participants in the OTC derivatives markets.

A broader adaption of the LEI is necessary along with standardization and use of a unique product identifier (UPI) and unique transaction identifier (UTI). These three identifiers along with standard critical data elements comprising the components of an OTC derivatives trade are required to be reported to these trade repositories before meaningful data aggregation and risk analysis can be conducted.

The FSB states that such low issuance of LEIs limits the ability to effectively support further regulatory uses. Those regulatory uses was set for it by the G20 when they requested “global adoption of the LEI to support authorities and market participants in identifying and managing financial risks”. To realize this objective each financial transaction, originated within a FSB member jurisdiction, must contain the LEI of each financial counterparty, each financial reference entity and the LEI of the transactions’ supply chain participants. Without such a common financial market participant identity, universally applied, the buildup of a contagion leading to systemic risk cannot be detected, nor can individual risks of financial institutions’ common counterparties be assessed.

author

Allan D. Grody

Allan Grody is President of Financial InterGroup Advisors, a financial industry consultancy. In his early career he worked in various capacities in multiple segments of the financial industry. In a later career he was a partner and the founder of Coopers & Lybrand’s (now PwC’s) Financial Services Consulting Practice. At NYU’s Stern Graduate School of Business he founded and taught their risk management systems course.

He is an Editorial Board Member of the Journal of Risk Management in Financial Institutions. He has been an expert witness on trading patent infringement and shareholder class action litigation; is a contributing opinion editor for The Hill; and has authored numerous academic papers and trade articles focused on risk adjusting the financial system and reengineering financial institutions.

defining organizational risk appetite for digital transformation strategy

by **Vivek** Seth

The technology landscape of the business across the world is transforming at a rapid pace, and institutions both international and domestic are riding the wave of digital transformation to increase their operational efficiency and deliver enhanced customer service. This new era of adopting innovative technologies by organizations is aimed at generating higher revenues, access to wider consumer market, and long-term multi-fold increase to the bottom line.

However, organizations must keep in mind that such digitalization attempts can potentially increase the risks of doing business which may not become apparent until the technological innovations are used on a wider scale and over a long period of time. The flip side of digitalization could be the amplification of its side effects to the people, systems and corporate social environment. It is crucial for long-term viability that corporations have in place a defined Risk Appetite framework that is used to monitor the residual risk associated with digital transformation strategy.

Outlined here are the emerging technological strategies that organizations worldwide are adopting in the spirit of digital transformation. While doing so, the corporations should keep in mind the inherent risks associated with these technological innovations, articulate their risk appetite for such risks and undertake remedial actions when risk occurrence exceed the organization’s tolerance levels:

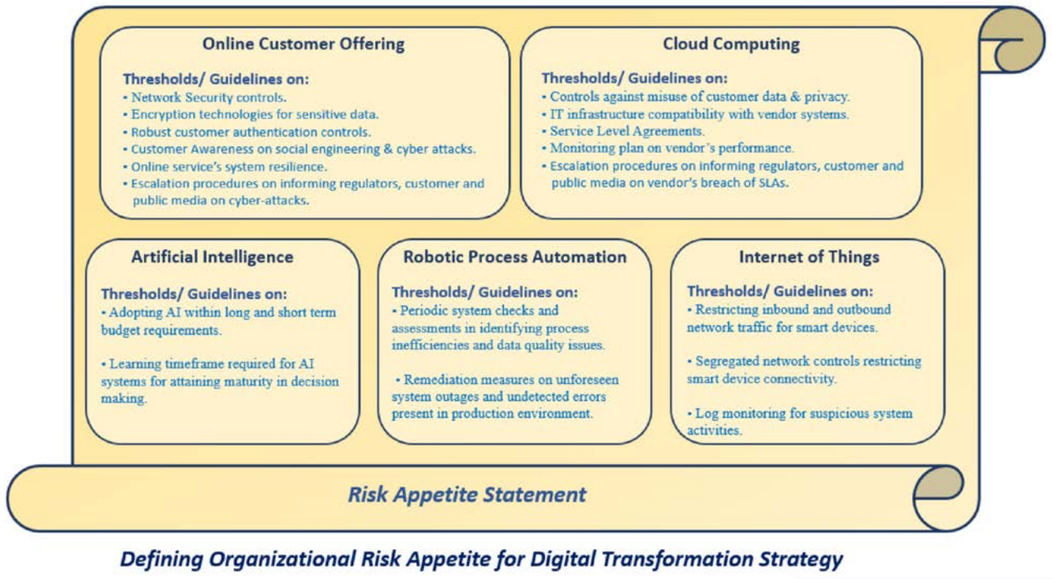
Online Customer Offering:

Customer services offering over the Internet comes with the challenges of protecting customer data against unauthorized access by malicious cyber-attacks and maintaining customer expectation of high availability of online services. Depending on the criticality of online data, appropriate level of security control measures should be put in place including encrypting data, multifactor customer authentication, and up-to-date network monitoring infrastructure against cyber-attacks and social engineering attempts. In its risk appetite statements, organizations should clearly articulate the tolerance levels on online service’s system resilience and thresholds when to inform regulators, customer and public media depending on the incident severity and success of cyber-attacks.

Artificial Intelligence and Robotic process automation:

Using Artificial Intelligence (AI) can have limitations of being too expensive in the short term and requirement of sufficient learning timeframe before AI reaches reasonable maturity. Both AI and Robotic automation attempts are relatively new, and failures may occur due to reasons such as software bug, obsolete system in use, weak network security infrastructure against cyber-attacks, etc.

Even in cases with due planning, previously undetected errors may lead to a systemic widespread issue across the business process & system data, thus resulting in amplified losses. The risk appetite statement should cover periodic system checks and assessments in timely identifying process inefficiencies, data quality issues and guidelines for adopting remediation measures. Automation should be understood as a means to achieve process efficiency and not a cure-all all alone by itself.



Defining Organizational Risk Appetite for Digital Transformation Strategy

Cloud computing:

Cloud Computing is essentially a form of outsourcing where all or part of the computing platform and/or software solutions is managed by a third-party vendor. The organization's risk appetite statement should clearly articulate the key challenges that come with IT infrastructure sitting outside the organization's direct supervision and control. Key areas to monitor include enforcing robust controls against misuse of customer data & privacy and ensuring compatibility between company's IT infrastructure and vendor systems. Third party service offering could also at times become an issue due to technical outages, vendor IT upgrade downtime and connectivity issues. The Risk Appetite framework should also define minimum level of service agreements per agreed Service Level Agreements (SLA) that vendors need to adhere with. Risk Appetite should also articulate the monitoring plan on reviewing data security and service offering and control framework for complying with the expectations of customers, business stakeholders and regulators.

Internet of Things:

Organizations are widely encouraging the use of smart electronic devices such as smart phones, state-of the art printers and other network devices that connect to institution IT infrastructure over the Internet. While defining the Risk Appetite for use of such devices, the risk of using such devices should be clearly understood. Such smart devices often have minimal security controls compared to computer platforms and are more likely to be used to gain unauthorized access. The risk appetite should provide guidance on restricting inbound and outbound network traffic for smart devices, segregated network controls restricting smart device connectivity to confidential data. Framework on log monitoring for suspicious system activities should also be covered broadly in the Risk Appetite statement.

Bringing it all together:

As part of digital transformation, organizations should ensure defining an articulate Risk Appetite Framework at the onset that covers the key risks associated with innovative technical solutions, guidance on robust controls for risk mitigation and threshold levels for monitoring the organization's risk profile. The Risk Appetite should be used consistently and periodically by organizations while adopting innovative technological advancements such as enhancement on online service offerings, automating it manual processes, digital outsourcing and adoption of emerging technologies. Organizations that adequately stay within the thresholds of its Risk Appetite will be able to limit the downside risks associated with adopting changes and stay successful harnessing the upside potential of digital transformations.

author

Vivek Seth

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

the demise of LIBOR: what to expect

by **Ira** Kawaller

Although LIBORs continue to be the most widely used benchmark interest rates in the US, their days are numbered. Largely due to concerns about manipulation, regulators and major market participants are forging ahead with plans to supplant the current reliance on LIBORs as benchmark interest rates with an alternative set of rates by the end of 2021. By all indications, the heirs apparent for benchmark interest rates are interest rates based on secured overnight financing rates (SOFRs), which reflect financing costs in the overnight repo market for government securities. Being derived from observed transactions rates, SOFRs are expected to be less susceptible to market manipulation than the survey-based LIBOR postings.

Ultimately, a transition to new benchmark interest rates would provide for widespread reliance on these substitute benchmarks across a diverse set of institutional funding sources, with comparability of designs in related derivatives. While aspects of the transition have yet to be worked out, when all is said and done, the financial landscape would be best served if hedgers can readily transact derivative contracts that allow for locking in sequences of interest rate resets over the period when LIBOR gets phased out, where the original pre-transition hedge objectives would still be realized. Unfortunately, that outcome seems quite unrealistic during the transition phase.

To orient the issue, it's important to appreciate the difference between the way LIBORs work today as benchmark interest rates and how the SOFR-based benchmarks will work in the future. In both cases (i.e., LIBOR-based debt and SOFR-based instruments) lenders and borrowers will agree to the principal amounts, accrual periods, and the reset and settlement dates; but LIBORs are determined as of reset dates (defined as the starting date of an accrual period for which a new rate would be applied), while the effective SOFRs will be determined in arrears. That is, we'll know the LIBOR that will apply in each accrual period at the start of each period, but we'll only get to know the effective interest rate in SOFR-based funding at the end of each accrual period.

Beyond that, the applicable money market rate under the SOFR regime is currently determined with either of two methodologies. For some instruments, that interest rate is calculated using the average of the overnight rates during the accrual period. For others, the calculated rate is the compounded daily overnight rate. This dichotomy makes it tricky for developers of SOFR-based derivatives. Conceivably, they could – and in fact, do -- build two distinct derivatives reflecting these two calculation designs. Practically speaking, the difference between these two respective calculations would likely be trivial – as in less than a basis point in most cases, but still…

The potential problem for entities with current hedges that extend beyond the transition date is that their initially expected hedged outcomes may not be realized. For example, if, at present, a LIBOR-based exposure has been hedged with a properly structured LIBOR-based derivative – i.e., one where the derivative's notional value is set to be equal to the principal amount being hedged and where starting and ending dates, settlement dates, and reset dates of the derivative mimic those of the exposure's accrual periods – the hedge outcome will be known with certainty from the start of the hedge, as long as the exposure and the derivative remain unchanged through their respective lives. For instance, a properly structured LIBOR-based debt hedged with a LIBOR-based swap will foster a realized interest expense equal to the swap's fixed-rate plus or minus any spread to LIBOR dictated by the original (unhedged) variable interest rate exposure.

Upon transition to an alternative benchmark interest rate, however, a different post-hedge interest rate could be realized. A difference could arise because of either of two possible developments. The first has to do with the spread applied to the new benchmark; and the second has to do with the introduction of arrears rate fixing.

With respect to this first concern, it should be understood that both parties to any benchmark-based debt instrument should be negotiating and agreeing to an all-in rate, consisting of the benchmark plus the spread. In such negotiations, the "correct" spread should represent a value consistent with the difference between the credit quality of the benchmark rate and the credit quality of the debtor. Thus, different credit qualities for different benchmark rates should justify different respective spreads. Exactly how the spread in any given transition will be determined, however, is yet to be determined, fostering at least some degree of uncertainty and hence basis risk.

A second source of uncertainty would arise as a consequence of SOFR pricing in arrears. If the hedge existed in a stable interest rate environment and if the "correct" spread were applied after the transition, the originally expected post-hedge effective interest rate would be realized before and after transition. On the other hand, if, during the accrual period, interest rates generally rise, the cost of borrowing under a SOFR-based rate would be higher than that under LIBOR pricing (had it existed); and conversely, if interest rates generally move lower during the accrual period, the SOFR-based funding costs would be cheaper.

The accompanying table shows a history of 1-month LIBOR with 1-month daily averages of SOFR. We assume accrual periods with each accrual period commencing on the first business day of the month. Critically, the appropriate LIBOR for that start date is the rate posted two London day's prior.

During this time period, one-month LIBOR averaged 11 basis points higher than the average of SOFRs over the corresponding term, but the differences were highly variable. At one extreme, LIBOR was almost 19 basis points higher than its associated SOFR, and at the other extreme, LIBOR was lower by less than a basis point. Importantly, this sample is extremely limited, and actual differences that might arise during the transition period could turn out to be much greater – or not.

In any case, whether the transition will prove to be beneficial to the debtors' side or the lenders' side remains to be seen.

This outcome will largely be determined by the magnitudes of the revised interest rate spreads and to a lesser extent by the path of overnight interest rates during the transition period. Rising overnight interest rates during any accrual period post transition would work to the detriment of the borrower and to the benefit of the lender, and vice versa with declining overnight rates.

Reset Date	Two Day's Prior	1-Mo. LIBOR	Average SOFR	Difference
5/1/18	4/27/18	1.907	1.730	0.177
6/1/18	5/30/18	1.982	1.837	0.146
7/2/18	6/28/18	2.092	1.914	0.178
8/1/18	7/30/18	2.082	1.917	0.164
9/3/18	8/30/18	2.104	1.968	0.135
10/1/18	9/27/18	2.256	2.184	0.072
11/1/18	10/30/18	2.299	2.221	0.079
12/3/18	11/29/18	2.349	2.351	-0.001
1/2/19	12/27/18	2.522	2.472	0.050
2/1/19	1/30/19	2.509	2.404	0.105
	Maximum	2.522	2.472	0.178
	Minimum	1.907	1.730	-0.001
	Range	0.615	0.742	0.180
	Average	2.210	2.100	0.110

Finally, the development of a viable SOFR derivatives market place requires a foundation in the futures market. That is, over-the-counter derivatives dealers won't offer these products unless they can lay off their risk somewhere; and that somewhere is a futures market where SOFR futures contracts are actively traded. Currently a number of SOFR futures contracts have been listed on futures exchanges. And although liquidity in these contracts is quite limited at this time, interest in these contracts will likely grow as the date for a benchmark transition becomes more imminent.

references

1. https://www.newyorkfed.org/newsevents/speeches/2019/hel190226
2. https://www.bis.org/review/r190318f.htm
3. https://www.americanbanker.com/news/libor-is-going-dark-in-2021-and-some-banks-arent-ready
4. https://www.afponline.org/ideas-inspiration/topics/articles/Details/libor-vs.-sofr-big-changes-are-coming-for-u.s.-treasurers
5. https://www.cftc.gov/PressRoom/PressReleases/7911-19
6. https://www.federalreserve.gov/econres/notes/feds-notes/indicative-forward-looking-sofr-term-rates-20190419.htm

author

Ira Kawaller

Ira Kawaller is the principal and founder of Derivatives Litigation Services. Before Derivatives Litigation Services, Kawaller was the President of Kawaller & Co., LLC, which assisted commercial enterprises with their strategic and accounting issues pertaining to derivative instruments. Kawaller holds a Ph.D. in economics from Purdue University and has held adjunct professorships at Columbia University and Polytechnic University.

greening up enterprise risk management

by **Peter** Plochan & **Andrea** Orsag

the urgency is rising

Climate change, limited natural resources, water scarcity and other environmental and related social events can have an immediate and high direct impact on business — affecting sales, performance, reputation or even overall license to operate. What's more, failure to anticipate and manage climate change-related risks can also have financial, reputational and legal consequences.

According to a report from the UN's Intergovernmental Panel on Climate Change[1], we have 10.5 years to cut CO2 emissions before the consequences become catastrophic. Extreme weather events and the failure of climate-change mitigation and adaptation have also been highlighted as the top risks in the World Economic Forum's 2019 Global Risks Report[2].

impact of climate change on banks

In the past few years, concerns around environmental impact, climate change and related social impacts have increased dramatically, causing considerable uncertainty for the overall economy. When thinking about their strategy and the economic outlook for the next 3-5 years, incorporating climate change risks should come naturally to banks because, if they do not include this angle, they might miss important risks and business drivers as well as related business opportunities.

Climate change is already costing banks money in a number of ways, for example:

- A farm loan not getting repaid due to the poor crop yields caused by extremely dry weather
- A plastic producer losing business due the anti-plastic regulations
- A company receiving a huge environmental fine for its unclean production practices and waste pollution
- An oil company left with stranded assets due to tightened regulations
- Global operations of multinationals losing their license to operate because of water challenges
- Manufacturers suffering disrupted production cycles due to their supply chains failing to deliver limited resources as agreed

In the examples above, the likelihood of losing money is severely impacted. According to a recent speech by Sarah Breedon of the Bank of England[3], a lack of action could mean heavy losses, with estimates of between $4 trillion and $20 trillion in asset value destroyed.

1 / IPCC Special Report on Global Warming of 1.5°C

2 / World Economic Forum Global Risks Report 2019

3 / Avoiding the storm: Climate change and the financial system

perspective of banking regulators

Banking regulators and central banks are paying increasing attention to climate change as source of a financial risk. The recently established network of 40+ central banks & regulators – The Network for Greening the Financial System (NGFS) - openly recognized the need for the banking industry to act.

"***Climate-related risks are a source of financial risk.*** *It is therefore within the mandates of central banks and supervisors to ensure the financial system is resilient to these risks*[4]*"*

Network for Greening the Financial System
First comprehensive report

A call for action

Climate change as a source of financial risk

This NGFS's call to action report provides the following recommendations intended to inspire all central banks, supervisors and relevant stakeholders to take the necessary measures to foster a greener financial system:

1. Integrate climate-related risks into financial stability monitoring and micro-supervision, covering two areas:

- **Assess climate-related financial risks in the financial system** by adopting key risk indicators to monitor climate related risks, perform quantitative assessment of the financial industry including a climate change risk specific scenario analysis and integrate it into macroeconomic forecasting and financial stability monitoring.

- **Integrate climate-related risks into prudential supervision** by setting supervisory expectations to provide guidance to financial firms and directly engage with them to ensure that climate-related risks are understood, discussed at board level, considered in risk management and embedded into firms' strategy and risk management processes.

2. Integrate sustainability factors into their own portfolio management, which relates to portfolio management performed by central banks themselves on the portfolios under their own management.

3. Bridge the data gaps, when building on G20 GFSG/UNEP initiatives. The NGFS recommends that the appropriate public authorities share data of relevance to Climate Risk Assessment (CRA) and, whenever possible, make them publicly available in a data repository.

4, 5 and 6. Focus on building awareness and knowledge sharing by establishing internationally consistent climate and environment-related disclosures and building a "green" taxonomy to factor in all the above.

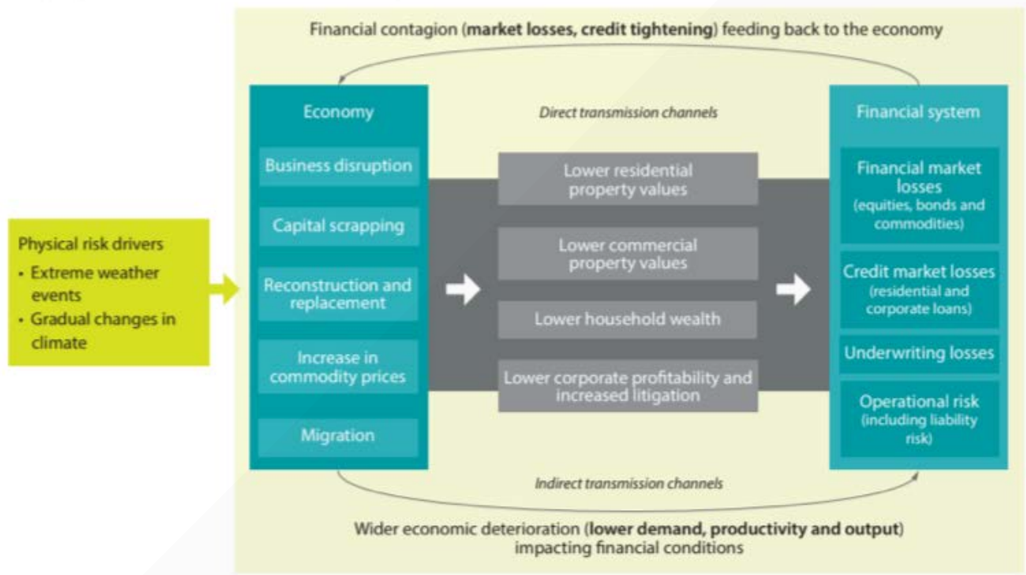
While the above recommendations are not binding, it is expected that they will be translated into the requirements set and actions taken by local regulators and central banks, and thus cascaded down to individual banks in some form.

climate change risk exposure

According to the NGFS framework, climate change may result in physical and transition risks that can have system-wide impacts on financial stability and might adversely affect macroeconomic conditions. Thus, due to climate change, banks are exposed to:

Physical impacts including the economic costs and financial losses resulting from the increasing severity and frequency of extreme climate change-related weather events (e.g. heat waves, floods, wildfires) as well as longer term progressive shifts of the climate (e.g. changes in precipitation, extreme weather variability, ocean acidification, rising sea levels).

From physical risk to financial stability risks

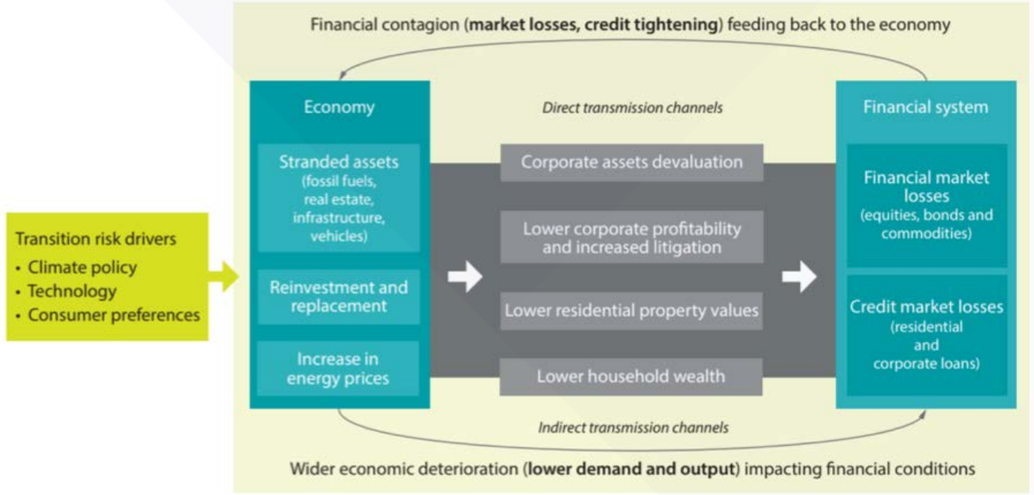


Source: NGFS: A call for action - Climate change as a source of financial risk

4 / A call for action: Climate change as a source of financial risk

Transition impacts relating to the process of adjustment towards a low-carbon economy. The potential risks to the financial system from the transition are greatest in scenarios where the redirection of capital and policy measures, such as the introduction of a carbon tax, occur in an unexpected or otherwise disorderly way.

From transition risk to financial stability risks

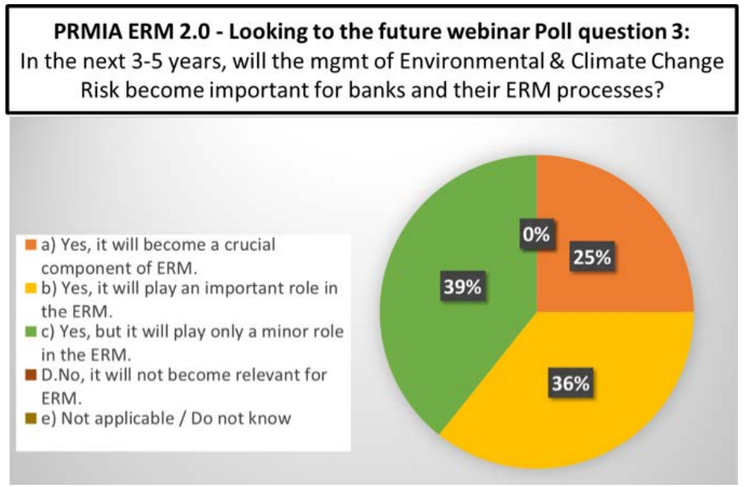


Source: NGFS, Call for action - Climate change as a source of financial risk

incorporation of climate change risks into enterprise risk management

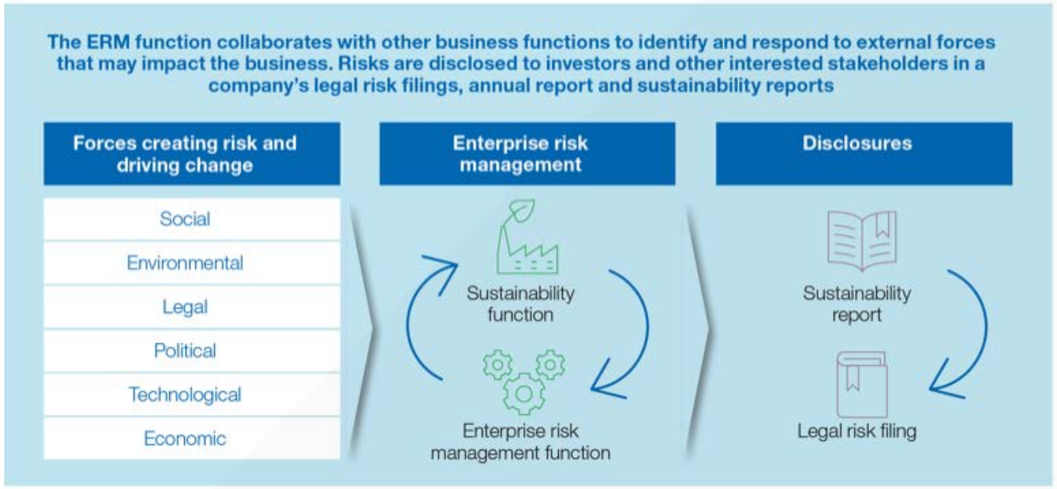
Banks have to start incorporating climate change and sustainability risk into their enterprise risk management (ERM) framework. In particular, forward looking ERM programs need to consider their impact on the bank's performance over the horizon of the next 3-5 years. Rather than adding a new risk category under the strategic risk umbrella, banks need to think how these climate change risk drivers impact their credit risk, market risk and operational risk profiles.

According to 70% of the participants in a recent PRMIA webinar ERM 2.0 - Looking to the future[5], management of environmental and climate change risk is going to play either a crucial or major role in the bank's ERM framework.



Source: PRMIA Webinar ERM 2.0 - Looking to the future – poll survey

One inspiration for how that could be done is the joint initiative by COSO[6] and WBCSD[7] on Applying Enterprise Risk Management to Environmental, Social and Governance-related Risks[8], which provides useful guidance and practical examples on how to incorporate environmental and climate change risks into banks' risk management processes and decision taking.



Source: WBCD

5 / PRMIA ERM 2.0 - Looking to the future

6 / Committee of Sponsoring Organizations of the Treadway Commission

7 / World Business Council for Sustainable Development

8 / Applying Enterprise Risk Management to Environmental, Social and Governance-related Risks

Moreover, the NGFS initiative is planning to provide additional guidance in this area, namely:

- **A handbook on climate and environmental risk management** setting out steps to be taken by supervisors and financial institutions to better understand, measure and mitigate exposures to climate and environmental risks.

- **Voluntary guidelines on scenario-based risk analysis** where the NGFS is working to develop data-driven scenarios for use by central banks and supervisors in assessing climate-related risks.

the way forward

It will be interesting to observe over the coming years how the banking industry copes with the challenges linked to climate change. Initiatives like the ones by NGFS or WBSCD help to provide a common understanding and a benchmark that banks can relate themselves to.

One thing is sure: we will see much more attention going to the assessment of environmental and climate change risk both at the individual bank level and also at the financial system level, considering both the current circumstances and also the potential future outlook and impact.

authors

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).

Andrea Orsag

Andrea Orsag is a co-founder and partner at MissionC, strategy advisory on a mission to accelerate the transition to Circular Economy on a global scale. Andrea is a consultant with 10+ years of experience combining Risk Management, Strategy and Change Management cross-industry, both for the commercial sector and not-for-profit organisations internationally. She has a Master's degree in International Business and studied Sustainable Finance & Investments at Harvard. She regularly acts as a moderator, facilitator and a speaker on topics related to Circular Economy and Sustainability.

understanding strategy risk and how to manage it

by **Branan** Cooper

Strategy risk is not always undesirable. Sometimes, the strategy risk is worth doing business with a third-party vendor because it outweighs the impact of not doing business with them and can help to move the business forward. In fact, if the risk is truly strategic to the organization and the appropriate precautionary steps are taken, the risk could help an organization achieve their best performance.

what is strategy risk?

Per regulatory guidance such as FDIC FIL 44-2008, strategy risk, or as they refer to it "other" risk, is defined as the following:

"The types of risk introduced by an organization's decision to use a third party cannot be fully assessed without a complete understanding of the resulting arrangement. Therefore, a comprehensive list of potential risks that could be associated with a third-party relationship is not possible. In addition to the risks described above, third-party relationships may also subject the financial organization to liquidity, interest rate, price, foreign currency translation, and country risks."

In addition, a risk that may be considered strategy can include categories such as human resources, commodity, complexity, venture capital, etc.

first steps to managing the risks

Once you have identified the third-party strategy risk(s) that potentially exist in the relationship, evaluate it further by listing the risk category in the template you are using to complete vendor risk assessments. It's encouraged to complete the risk assessment as part of your initial vendor vetting, and if you move forward with the vendor, as part of ongoing monitoring.

The risk assessment assists with achieving a regulatory risk rating – often high, moderate or low risk – and by including questions related to the specific strategy risk(s) identified, it will help the organization configure the most accurate final risk rating. Once you have determined the risk rating, you have identified the inherent risk of doing business with the third party.

first steps to managing the risks

If you have decided to outsource call center activities, there's a chance this may include some offshore operations. Therefore, in this case, you will need to very carefully consider country risk and dig a little deeper when reviewing the vendor. You may want to ask yourself questions like the following to properly evaluate this strategic risk:

- Can you truncate U.S. consumer data?
- Are you able to ensure they have a clean desk policy?
- Is there a lot of crime and geopolitical climate in the area?
- What do their hiring practices look like?
- Are the OFAC and background checks on key management clean?

the 4 risk options

Once the inherent risk is fully identified, evaluate the risk further to decide how you wish to proceed.

There are 4 possible outcomes:

1. **Accept the Risk:** If you choose to accept the risk, this means you have done your due diligence, likely performing a cost-benefit analysis. You have concluded the advantages of outsourcing to the third party vendor for a product/service do indeed outweigh the disadvantages. Therefore, the organization accepts the risk posed. In this case, you will move forward with the third party but continue to monitor the potential risks.
2. **Avoid the Risk:** If you choose to avoid the risk, this means you have completed your due diligence on the third party and the risk is too large to prove beneficial to your organization. Meaning, in the end, it's too risky and there's a high likelihood that the risk will impact the organization in a harmful way at some point.
3. **Transfer the Risk:** If you choose to transfer the risk, this means you have moved forward with the vendor; however, you have decided to outsource some or all of the risk to another third party. (e.g., purchasing additional insurance coverage to protect your organization).
4. **Mitigate the Risk:** If you choose to mitigate the risk, this means you have identified the inherent risk present and have taken steps to reduce the risk as much as possible. After mitigating risk, your organization should be comfortable with the risk that is left, otherwise known as the residual risk. This is certainly the step most commonly used.

Managing risk is what it's all about. Strategy risk, along with the other categories of risk identified in the guidance, is a key component of ensuring that your organization is aware of the risks of doing business with a third party. While you can never eliminate risk, you can identify it and control the risk.

author

Branan Cooper

Branan Cooper is the Chief Risk Officer at Venminder. He has over 25 years' experience in the financial industry with a focus on the management of internal processes and controls – most notably in third party risk and operational compliance. Branan joined Venminder from Bancorp Bank where he was senior VP and Director of Third Party Risk Management. He held similar positions with PartnersFirst, the credit card division of Western Alliance Bancorp, and at MBNA America. Branan is a member of InfraGard and PRMIA, an advisor to the Center for Financial Professionals and board member for the Global Sourcing Resource Network.

managing strategy risks

by **A. J.** Giacobbe

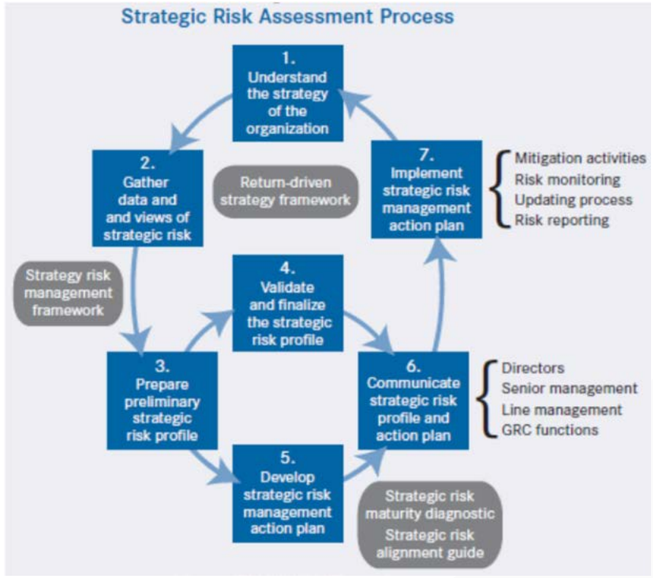
If you look up the definition of the word “strategy” you will find that it is often associated with military history. The term comes “directly from the Greek strategia ‘office or command of a general,’ from strategos ‘general, commander of an army (etymonline.com).’” The history of the concept of strategy is often attributed to the ancient Chinese military leader, Sun Tzu through his teachings in The Art of War. In this classic text, Sun Tzu teaches that “planning leads to victory (Tzu).” Further research will show that it wasn’t until the 19th century that the term was adopted for business use (etymonline.com) and as much as the word is used in business today, Sun Tzu’s lessons of military strategy are equally important and relevant in business – it is planning that will lead to victory.

Risk in inherent in business as it is in war. For banking in particular, credit risk is the obvious risk and is given a lot of attention in the process of strategizing. There are, of course, other risks to be mindful of when setting strategy, including but not limited to operational, market and regulatory. The Office of the Comptroller of the Currency (OCC) defines strategy risk as “the risk to current or projected financial condition and resilience arising from adverse business decisions, poor implementation of business decisions, or lack of responsiveness to changes in the banking industry and operating environment.” These risks exist based on any leadership’s planning and ability to execute.

According to the OCC’s Semiannual Risk Perspective for the Spring 2019, “strategy risk is elevated for many banks.” In their analysis, the OCC attributes the increased level of risk to “rapid industry changes, poor business decisions, imprudent or incomplete change management plans, pressure to reduce expenses and control costs, the burden of some technology systems, resource limitations, and need for scale of operations (OCC.gov).”

In a business context, a firm’s Board of Directors and executives determine the strategy and are accountable for executing their strategy. As a result, these are the people who “own” the risks inherent in the activities conducted to achieve their stated goals. They must understand how their companies make money by serving customers while seeking to sustain and enhance value for their owners – all while appeasing governments, communities, employees and other stakeholders that are impacted by the existence of these enterprises. Setting and communicating a successful strategy is an enormous responsibility and further complicated by competition fighting for the same piece of the pie. This is where the war is fought and can only be won through disciplined execution of a sound strategy that has been well thought through and supported by data where possible.

This is why it is so important to embed risk management excellence into the formulation of any strategy. First, the team must truly know the business, the markets, customers and then how those customers can be best served through efficient and effective operations. Next, risk can be assessed through collecting data and learning about how your business can be negatively impacted. Had Wells Fargo understood that their strategy to cross-sell products and services to customers was implemented through misaligned incentives that allowed rogue employees to serve their own interests by opening accounts to unknowing customers, they might have been able to manage the risk or significantly reduce the fallout they experienced. It’s easy to assess this in hindsight and not at all easy to assess when setting strategy. Though, through practices such as scenario analysis, external loss data analysis and learning from experience, banks should now have these risks assessed and if cross-selling is a critical component of their strategy, one would expect proper alignment of incentives and other controls are being tested and analyzed with findings reported up the chain and, ultimately, to the Board to keep themselves in check.



https://corpgov.law.harvard.edu/2012/08/23/strategic-risk-management-a-primer-for-directors/

Military leaders are, perhaps, the greatest strategists and risk managers of any profession. I attribute that to their incredible discipline and dedication to their cause and relentless pursuit of considering risk in their strategy formulation. Boards should take notice when setting their strategies and have the discipline and dedication of understanding risk and continuous learning to make their organizations stronger.

reference

1. https://hbr.org/2012/06/managing-risks-a-new-framework

The opinions expressed in this article are my own and do not necessarily represent my employer’s views.

author

A.J. Giacobbe

A. J. Giacobbe is a vice president in Enterprise Risk Management at the U.S. operations of a large global bank. He has 15 years experience in the financial services industry in risk management and regulatory compliance roles. A. J. serves on the Ethics Committee of PRMIA and has earned the organization's Operational Risk Management (ORM) certificate. His bachelor's degree is from the University of Delaware and he holds a Master of Arts degree from Rutgers, The State University of NJ and MBA from the D'Amore-McKim School of Business at Northeastern University. Beginning his career in New York, he is now based in Boston, MA. He lives with his wife, Rebecca, and two young daughters outside of Boston. He enjoys ice hockey and playing the drums.

managing strategic risk in technology and financial modeling

by **Rita** Previtali

where strategic risk occurs

Strategic risk in relation to technology and financial modeling occurs when financial institutions embrace advanced technology. Managing this risk requires consideration of the possible drawbacks of innovative advances, high costs of implementation, and the consequences of attempting to develop super-complex models utilizing the plethora of data made available by advanced technology.

One example of advanced technology is the "Cloud." Cloud technology is a powerful data aggregation development available to institutions that seek to obtain a competitive edge by optimizing the use of client and services data originally housed in separate, siloed (not communicating), legacy systems. Migrating data from many different siloed systems into the 'cloud' and utilizing cloud computing enables economies of scale and swift accessibility to global data, facilitating analytical research and expansion of customer base and services, while complying with domestic and international regulatory laws.

The strategic risk in cloud technology varies according to the type of adoption. Cloud technology can be implemented on public clouds, private clouds, or bare metal servers. The first two are run on virtual servers that can be shared with other users/clients with obvious security risks. These alternatives, albeit perhaps more economical, would not be able to satisfy the client privacy conditions sought by financial institutions and their regulators. The third alternative, bare metal servers, are physical servers used by a single 'tenant' and will protect data from the obvious risk generated from sharing virtual space. They allow banks to create their own virtual servers without having to share virtual computing space with other cloud users.

Another example of advanced technology is Artificial Intelligence (AI). Financial modeling risk becomes more complicated when utilizing AI. Through Machine Learning (ML), which uses AI technology, developers and analysts create algorithms to analyze behaviors and patterns in order to predict the likelihood of outcomes such as client credit payment behavior or the valuation of sophisticated structured products. ML needs large amounts of data to achieve reliable results. This data is typically stored in the cloud. Cloud data provides ML initiatives with the ability to develop and use more accurate financial models to create newer, more sophisticated products, readily detect product correlations, and better support regulatory reporting.

Financial modelers can use ML confidently to develop all kind of algorithms and analyze as many financial outputs as necessary to reach reliable product market valuations.

However, strategic risk emerges when modelers become overconfident in the output of their models, in part because they are supported by large amounts of data that leads them to overlook other factors, such as the capacity of traders, counterparties, clients, and managers to completely grasp the components and interactions of their models. Models not totally clear to traders can lead to inaccurate hedging that, if affecting big positions/portfolios, could result in substantial losses.

Another type of strategic risk is that counterparties/clients who, after entering into exotic transactions based on these models, find that these transactions produce unexpected, negative outcomes, can claim misrepresentation leading to regulatory scrutiny, even penalties, and reputational risk exposure.

A third type of strategic risk is that models not clearly understood by managers can lead to weak oversight of marketing and product offerings, also exposing the bank to regulatory scrutiny and reputational risk.

how strategic risk can be mitigated

To mitigate the types of risks stated above, it is imperative to establish strong risk governance, guided by strategies such as:

- **Board Committee's responsibility**: It should be the Risk Committee's responsibility to select the type of cloud technology that the institution will rely on for years to come. Points for consideration in making that decision should include: regulatory expectations for safe-guarding clients' privacy, data latency, global accessibility, growth potential, and server price comparison.

- **Risk framework:** A well-thought-out and comprehensive operational risk framework needs to be in place that includes assessment of data gathering, standardization, safeguarding, and protection before it is uploaded to the cloud, and data management once it resides in the cloud.

- **Model review:** A plan must be developed to establish a rigorous model review and validation methodology for models spanning from plain vanilla to the most innovative and exotic structured products. "Risk management procedures should include a formal treatment of model risk and periodic re-evaluation of models".[1]

- **Model oversight:** A strong operational risk process is needed to verify that the validator is following model risk validation principles, such as those outlined on the MLARM, Risk Management Handbook: documentation, soundness of model, independent access to financial rates, benchmark modeling, health check and stress-test the model and that substantiates a validator's "assurance that the model offers a reasonable representation of how the market values the instrument and that the model has been implemented correctly".[2]

1 / PRMIA – Market, Liquidity and Asset Liability Management, Risk Management Handbook. Pg. 49, Mitigating Model Risk

2 / See reference #1

conclusion

To summarize, while financial institutions, banks in particular, are strategically adopting advanced technologies that provide them with tremendous tools to improve client service growth and greater financial model accuracy, among other benefits, they must determine the risks inherent in the adoption of these technologies and carefully outline and employ operational risk control directives that will safeguard their path towards secure and confident growth.

author

Rita Previtali

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

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

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

PRMIA launches Chennai, India Chapter

PRMIA launched its Chennai chapter with an inaugural conference at Image Hall No. 2, Indian Bank, MRC Nagar, Chennai on June 21, 2019.

The theme of the inaugural conference was Digitalization of Indian Economy: Opportunities and Threats.

On the auspicious International Yoga Day, the PRMIA chapter commenced with a traditional lamp-lighting. Several reputed thought leaders and experts from diversified industry graced the event.

Inaugurating the event, Ken Radigan, CEO, PRMIA said, “Initially established in the United States in 2002, PRMIA now operates in 48 cities and is well recognized for competency-focused training, professional certifications, and global networking. India is a top destination for PRMIA given the huge interest of Indian professionals for PRMIA credentials.”

According to Dr Nirakar Pradhan, PRMIA Director and APAC Representative for Asia Pacific, the launch of PRMIA’s 2nd Chapter in Chennai, a few months after the Mumbai Chapter, will go a long way in addressing the huge demand from Indian finance professionals for risk management education, training and certifications.

The evening was marked by several experts from diversified industry coming together and sharing unique insights among the audience. It was a pleasure listening to Padmashree Dr Rabi Narayan Bastia’s personal experiences and anecdotes on risks that are prevalent in the energy sector, especially his ability to draw parallels between life-threatening risks from global warming, water shortage, and increasing environmental pollution to financial risks were commendable.

The presentation by Mr Sriram Kannan demystified the understanding of blockchain and highlighted how the financial services industry could derive business benefits by implementing blockchain. Mr Udaya Bhaskara Reddy, Chief Risk Officer & GM, Indian Bank, threw lights on the threats, challenges, and opportunities facing Indian banks as they ‘go digital’. An enlightened panel joined by Mrs Bhagylaxmi Patnaik, Mr. T. L. Arunachalam, Whole Time Director & President, Bharat Re-Ins. Pvt. Ltd Mr Subramanian from TCS answered a variety of questions and shared their perspective on various risks engaging banking and financial industry today.

The event, sponsored by Indian Bank and organized by PRMIA volunteers received huge interest and participation from a wide range of industry players comprised of senior bankers, corporate leaders, risk professionals, risk consultants, audit firms, business media, academicians, students, technology solution providers, and industry watchers.

Thanking all for the interest and support for the event, Mr S. K Choudhury, Regional Director, Chennai Chapter, announced the continuing of similar events in the future also as it provides an excellent platform for a wide range of stakeholders to share ideas and best practices, besides participating in PRMIA globally recognized education, training and networking opportunities.

PRMIA mentor connect

by **Adam** Lindquist

Mentoring is not a new idea. When you were growing up and your parents or other older adults taught you a skill, you were being mentored by them, often through valuable hands-on learning.

Most successful leaders credit mentors for helping guide their success. Bill Gates considers Warren Buffet a critical mentor to his success and helping him understand the importance of larger contributions to the world. Sir Richard Branson said of his seeking out his Mentor Sir Freddie Laker, the airline mogul, to help him get his airline off the ground, “Understandably there’s a lot of ego, nervous energy and parental pride involved, especially with one- or two-person start-ups…Going it alone is an admirable, but foolhardy and highly flawed approach to taking on the world.”

If these recognized leaders are continually seeking mentors, you should too. We all have been mentored in our lives but only a few of us have participated in a formal mentoring program. It can seem intimidating, but it shouldn’t be and isn’t with PRMIA Mentor Connect.

defining your role mentor or mentee?

When you register for PRMIA Mentor Connect, you need to define your role. Are you someone who is a leader looking to help guide and develop a peer as a mentor, or are you someone hoping to develop skills and perspectives as a mentee? Are you looking for technical or soft skills help that could best be provided by a peer who understands our industry? Perhaps you’re both!

The first step is to define what role you seek and register into the program with a clear understanding of what you want to accomplish.

finding success with a mentor

Harvard Business Review published an article on mentoring we feel does a great job of identifying what makes a mentoring relationship successful. But we expanded on it from feedback from the PRMIA Mentor Connect program.

1. Put the relationship before the mentorship.

The key to a successful mentoring is the relationship. One piece of research, conducted by Belle Rose Ragins, a mentoring expert and professor at the University of Wisconsin-Milwaukee, demonstrated that a mentee's success requires a basic relationship with their mentors. The bottom line is a trusting relationship, where the mentor and mentee are working towards a common goal. We are fortunate that the PRMIA Mentor Connect program utilizes a personality matching approach that is designed to connect peers together that helps create that comfortable rapport. To support this process, we have short videos and "starting guides" to get the conversation moving and progressing.

2. Focus on character rather than competency.

Too many mentors see mentoring as a training program focused around the acquisition of job skills. Now, this may be the reason you as a mentee connected, but don't let a great relationship be so focused on technical skills that you miss a bigger opportunity. The best leaders go beyond competency, focusing on helping to shape other peoples' characters, values, self-awareness, empathy, and capacity for respect. Let's face it, most of us could benefit from developing our softer skills along with our technical ones. An honest evaluation from a mentor about how we come across could have as much, or more, impact on our career than a technical skill.

3. Be loyal to your mentee and your mentor.

A great mentoring program is one of honesty yet void of personal bias. The best mentors avoid overriding the dreams of their mentees. If an employee and a job aren't a good fit, or if an ambitious employee realistically has limited upward mobility in a company, a good mentor will help that employee move on. A mentor's job is to not only uncover a mentee's strengths, but also to look for their underlying passions to help them find their calling. It's been said that the world prefers conventional failure over unconventional success; good mentors should encourage exploration of the latter.

4. Be open to your match.

I have enjoyed a career where I have gained many perspectives on how solutions are implemented in different businesses. My "Vertical Integration" of one approach into another industry has resulted in great success and in some cases industry disruption because no one in that industry had ever approached it in that way before. Be open to connecting with a mentor or mentee in a different industry, and even a different culture. Their perspective may trigger an opportunity that you never imagined, while opening your eyes that your approach isn't the only option.

5. Register.

You must be a PRMIA Sustaining Member to participate in the PRMIA Mentor Match program. Register or learn more about **Mentor Connect**.

If you have questions about the program or are interested in learning more about how your Company can leverage our award-winning software, please contact me at adam.lindquist@prmia.org.

author

Adam Lindquist

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

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

June 22 – September 13

EGYPT AND KSA RISK MANAGEMENT CHALLENGE

August 9 – Cairo

ILLIQUIDITY RISK OF TRULY ILLIQUID ASSETS

August 14 – Webinar

PRM™ TESTING WINDOW

August 19 – September 13

FUNDAMENTALS OF FINANCIAL RISK MANAGEMENT VIRTUAL TRAINING

Weekly classes open each Tuesday, August 20 – September 3

OPERATIONAL RISK MANAGER CERTIFICATE PREP TRAINING

Weekly classes open each Monday, September 9 – October 28

ASSOCIATE PRM CERTIFICATE PREP VIRTUAL TRAINING

Weekly classes open each Monday, September 9 – November 4

PRMIA HUNGARY CHAPTER RESEARCH CONFERENCE

October 17 - Budapest

EMEA RISK LEADER SUMMIT

November 5 – 6 – London

CANADIAN RISK FORUM

November 11 – 13 - Montreal

INTELLIGENT RISK

knowledge for the PRMIA community

PRMIA
Professional Risk Managers'
International Association