European Risk Management Council

Risk Landscape Review

December 2020

- Improving Resilience post-COVID
- It’s the Fragility that Matters
- The Purpose of Organisations?

DEAR READER,

I am delighted to present Q4 2020 edition of the Risk Landscape Review which includes three articles.

The ongoing COVID-19 crisis continues to reshape the risk landscape of the financial services and dominates the agenda of the risk management leaders across the world. To address the global challenge, we publish an article "**Improving Resilience post-COVID: Role of Risk Management**" written by Dr Christian Pedersen, Head of Risk & Compliance at Accenture (Growth Markets). Dr Pedersen focuses on critical areas of the operational resilience framework and proposes practical steps to enhance it.

One of the fundamental questions that the COVID crisis raised is: how should we improve our preparedness for tail risk events? In his article "**It's the Fragility that Matters**" David Dredge, Chief Executive and Chief Investment Officer at Convex Strategies, discusses fragility of the financial system, weaknesses of popular risk metrics and ways to make the system less fragile.

Peter Neville Lewis CMIRM, Director at Risk Coalition Research Company, in his article "**The Purpose of Organisations?**" reminds us that even in the midst of the deepest crisis in living memory, culture, purpose, integrity and social values remain paramount for an organisation to survive the crisis and thrive.

My huge thanks to all contributors.

Enjoy the reading.

Yours sincerely,

Dr Evgueni Ivantsov

Chairman of European Risk Management Council

Table of Contents

Improving Resilience post-COVID: Role of Risk Management

By Dr Christian Pedersen, Head of Risk & Compliance, Accenture (Growth Markets)

The COVID-19 outbreak is an unprecedented shock for people and business across the globe and amplifying an already highly volatile risk landscape. Though the pandemic will ultimately recede, volatility and disruption are here to stay. As the health and humanitarian impacts of the COVID-19 pandemic evolve, so do business and economic challenges. Organizations looking to balance their immediate needs with longer-term opportunities will see the trade-offs play out across three waves of impact: The Now, the Next and the Never Normal:

- The Now includes an emphasis on supporting people, customers and suppliers.
- The Next will feature refocusing the business to withstand new threats and seize new opportunities.
- The Never Normal will require navigating rapid shifts in cultural norms, values and behaviours.

The time to shape a mindset of bold business transformation powered by new approaches to technology and responsible leadership is underway - leaders are moving fast.

This rapid evolution is not least required in risk management. COVID-19 alone is a significant business risk, but it has also exacerbated and reshaped risks that companies were struggling to get to grips with before the outbreak. Domestic and geo-political tensions deepened while new working practices and use of new collaboration tools create new cyber vulnerabilities and points of weakness for fraudsters and criminals seek to exploit. Large, frequent swings in financial markets exacerbate credit, market and liquidity risk.

The Risk function needs to play a substantial role in preparing business for future volatility and crises, for new regulation that may materialize, and to grasp the opportunities (and mitigate further significant impacts) that emerge as the pandemic recedes. The Risk function should question its core purpose. Is its role purely to mitigate downside, or does it now have an active and more important role in accelerating growth?

Progressive risk functions do both, partly through improving operational resilience. Risk leaders should prioritise building stronger relationships with executives across the business, but particularly those in technology, IT, and operations. This will allow Risk to inform and influence business and technology strategy and build resilience across the enterprise - which in turn protects against shocks and helps ensure competitive customer service. It may be considered sufficient by some to wait for and comply with emerging regulation, but it will be necessary to move well beyond this to reap competitive advantage.

There are several areas where Risk functions immediately need to improve:

1) Expand data sources analysed - This is key to detecting threats and uncover potential opportunities. For example, online news and social media can be harnessed to create so- called digital signals that identify early indicators of future COVID-19 case hotspots, changing customer behaviour and preferences, and credit warnings

2) Make greater use of internal data - All too often, internal data exists in siloed systems, making it near impossible to extract, aggregate, synthesize, and analyse. Risk functions should aggregate data into a centralized database or data lake to ease analysis and onboard new data – it's critical to be involved in this transition even if run by the business

3) Turn data into insights - To draw useful insights from internal and external data, Risk functions should explore the array of new artificial intelligence and machine learning-based tools, advanced analytical and predictive modelling techniques.

4) Look to intelligent technologies - Many businesses already use intelligent technologies to scan network activity to detect cyber breaches. The same technology can be deployed to identify other activities that may constitute a risk, such as early indicators of poor conduct, fraud, identity theft, or customers with poor credit.

5) Don't overlook less sophisticated tech - More established technologies like cloud and robotic process automation (RPA) should not be overlooked and can help streamline manual processes. This frees up time for the Risk function to detect, analyse, and mitigate new and emerging threats.

One of the most critical areas to challenge resilience today is the increase in cyber risk. Detailed modelling of cybersecurity performance has identified two distinct groups among respondents. About 15 percent of the banking and capital markets firms surveyed have significantly higher levels of cybersecurity performance compared to their industry peers. These leaders exceed the capabilities of the average group in four areas in particular:

- Stopping attacks: A nearly fourfold advantage in preventing targeted cyberattacks.
- Finding breaches faster: Four times faster at detecting a cyber breach.
- Fix breaches faster: An almost threefold advantage in speed of remediation.
- Reduce breach impact: Twice as effective at containing damage from a successful attack.

Our research found that the current average cost per attack for average performers was $380,000 per incident. If they could attain a leader's level of performance in detecting attacks and fixing breaches, they could reduce the cost per attack by 72 percent or $273,000 per security breach. With an average of 22 incidents per year, this equates to $6 million in annual savings. Apart from the financial loss, leaders also benefit from reduced reputation risk from events and an overall smoother and less interrupted business process leading to competitive benefits in customer service.

Cybersecurity leaders are fast responders. They can find and stop breaches before significant damage is done. They spot anomalies, trigger an investigation and eradicate the threat. Others over-spend on defence and under-spend on offense — meaning not enough time is spent building fast, sophisticated detection-and-response capabilities.

Moreover, one of our survey-based studies among IT professionals found that the average corporate network is accessed by 89 vendors every week. This ecosystem is likely to grow in scale and importance over time. The same study found that 71 percent of respondents expected their companies to become more reliant on third parties in the next two years. There are big challenges in managing third-party cyber risks. Large volumes of data can overwhelm the teams responsible for managing compliance. The complexities of global supply chains, including the regulatory demands of various regions or countries, add to the strain.

A dizzying variety of technologies are available in the cybersecurity area, including when dealing with third parties. Our studies have found that leaders highlight three technologies in particular:

- Next-Generation Firewall (NGF)
- Security Orchestration Automation and Response (SOAR)
- Privileged Access Management (PAM)

This is combined with policies, governance and enforcement such that any third party connected to your network requires the same security standards that you do. Only with a rigorous and transparent process in place can the business comfortably leverage third parties, including leading technology firms and start-ups, in preparing for the post-COVID world without a risk of cyber-attacks leading to significant disruption, financial loss or reputational damage.

The Risk function's skills profile should evolve commensurately to be fit to analyse and mitigate the emerging risks, whilst effectively leveraging new analytical technologies. As Risk increasingly works with advanced tech, vast quantities of data, and staff from other groups, the modern risk professional needs to evolve. Recruitment can help, but existing teams also need to be retrained and transferred, bringing intimate knowledge of business, analytics and technology. The business will also be better prepared to weather and thrive in future volatility by inspiring a culture of curiosity and willingness to challenge within the Risk function.

In conclusion, operational resilience will be not only sufficient but necessary for institutions to secure a sound reputation and competitive positioning in an increasingly digitised post-COVID world. As competitors and business partners digitise and regulators shape baseline responses, we will see industry leaders pull away from the pack. The Risk function and its contribution to improving operational resilience will be a major factor in determining who are the future leaders.

We see the biggest challenge for Risk functions as ensuring the right level of technology-literacy and innovative use of both new data and modern modelling techniques. The most immediate threat of growing cyber security in lieu of industry digitisation and use of third parties is just a taster of the challenges to come.

The article makes use of and refer to the following studies:

https://www.accenture.com/sg-en/insights/financial-services/coronavirus-risk-management
https://www.accenture.com/sg-en/insights/security/invest-cyber-resilience
https://www.accenture.com/sg-en/insights/financial-services/cyber-resilience-study-banking-capital-markets
https://www.accenture.com/sg-en/insights/financial-services/cyber-resilience-study

It's the Fragility that Matters

By David Dredge, Chief Executive and Chief Investment Officer, Convex Strategies

We are regularly asked questions, even at times asked to give presentations, along the lines of "can we predict risk events?" The short version of the answer/presentation goes something along the lines of: NO.

We cannot predict when or where lightning might strike and spark a forest fire. We certainly can't predict if the next major wildfire will be triggered by lightning, or power lines, or campers, or motorcycle backfires, or kids playing with matches…..by definition you can't predict the unpredictable. What we can do, however, is to take note of fragility. Random unpredictable lightning strikes do not cause uncontrollable forest fires unless they strike an already fragile forest system. Without an accumulation of dry underbrush and trees, it is pretty hard to get a significantly damaging forest fire. This comes back to the known scientific premise about the relevance of endogenous risk – where fragility exists, versus exogenous events – the shocks that expose the fragility. If you want to avoid the risk of property damage due to forest fires, don't own property in the midst of forests that are clogged with dry underbrush and trees. If you can't avoid that, best to buy insurance early, before everybody else realizes the same, and have a well thought out escape plan!

Nassim Taleb defines fragility as something that is harmed by disorder (short optionality/volatility), while coining the term 'antifragility' as its opposite, ie something that benefits from disorder (long optionality/volatility). What is the "crisis" that the central banks are fighting? It is the fragility of the debt driven economic system that, when struck by the spark of a global pandemic, risks erupting into a mass conflagration of destruction.

Maybe the simplest way to define the fragility of the economy is the lack of loss absorbing capital in the food-chain of leverage. What in our world of derivatives we refer to as 'uncapitalized tails'. We all got to see this very clearly back in 2008 when the decline in the collateral value of US homes triggered losses that could not be absorbed by the global banking elites, forcing an explicit taxpayer bailout and the implicit stealth tax of inflation being imposed on present and future non-asset holders. Naturally, policy makers and regulators don't see the crisis as being the fragility of the system that they promulgate, but rather explain it off as yet another unpredictable exogenous shock.

To quote from a recent paper by Bill White (former BIS Economic Research Head): "the policy regime has encouraged the belief that economies face liquidity problems when the underlying problem is really one of insolvency" thus "the path we are on is unsustainable because the underlying problems grow worse over time while the solutions become more constrained"[1].

[1] https://www.ineteconomics.org/uploads/papers/WP_131-White.pdf

Bill is, of course, correct. It is not a liquidity problem, but rather an insolvency problem due to the high levels of leverage/lack of loss absorbing capital.

How is it that these market players are allowed to impose risk on the stability of the entire system through their use of leverage? How have we let, what we like to call Agency Bias (ie fiduciaries who participate on the upside but not the downside), imperil the wellbeing of the entire financial universe yet again? Most simply put, by allowing, indeed mandating, that they use a risk methodology that benefits their asymmetric incentive structure to the detriment of end capital owners and society. It is not too much to say that the use of probabilistic, ergodic process, Gaussian based risk methodologies is destroying the world. Bluntly, Value at Risk (VaR) isn't just wrong, it is dangerous and perhaps even more sinister than that.

The use of leverage by fiduciary risk takers, fuelled by their ability to misrepresent risk through standardized measures such as VaR and significantly encouraged by the moral hazard expanding practices of policy makers, has built fragility of unprecedented scale. Once again requiring unprecedented policy support ride to the rescue when the spark of the pandemic found the accumulated dry underbrush.

In a recent speech by Federal Reserve Vice-Chair Randall Quarles, he commented on the March 2020 disfunction in traditionally deep and efficient fixed income markets as "the pressure on longer-dated government bonds was sufficient to impair pricing for some of these bonds in this normally deep and liquid market, an outcome that we would not normally expect."[2]

This necessitated their intervention to address wrongly behaving markets. The official premise being that markets behaved wrongly relative to their models of risk, as opposed to an alternative premise that their models of risk behaved wrongly relative to markets. Funny old game.

A very quick and simple single asset mean-variance based Value at Risk calculator can be used to show the shortcomings of such Gaussian based methodologies. The below simply shows the US Treasury Index with a mean-variance based distribution of daily returns over an 18-month data series (see figure 1 & 2). The light blue distribution is a simple mean-variance normal distribution over the data period, while the darker blue line is the same but builds in the actual realized skew of the period. We do this over two 18-month data series, one ending on 28th February, 2020, and one ending on 19th March, 2020.

[2] https://www.bis.org/review/r201021a.pdf

Figure 1: US Treasury Index 18mth daily returns data to 28 Feb 2020

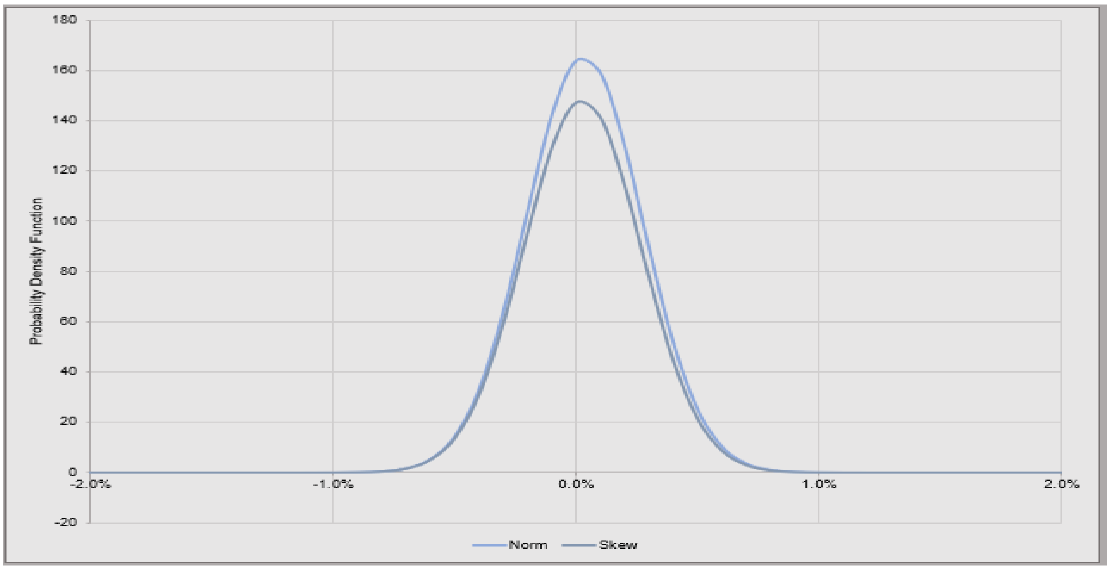
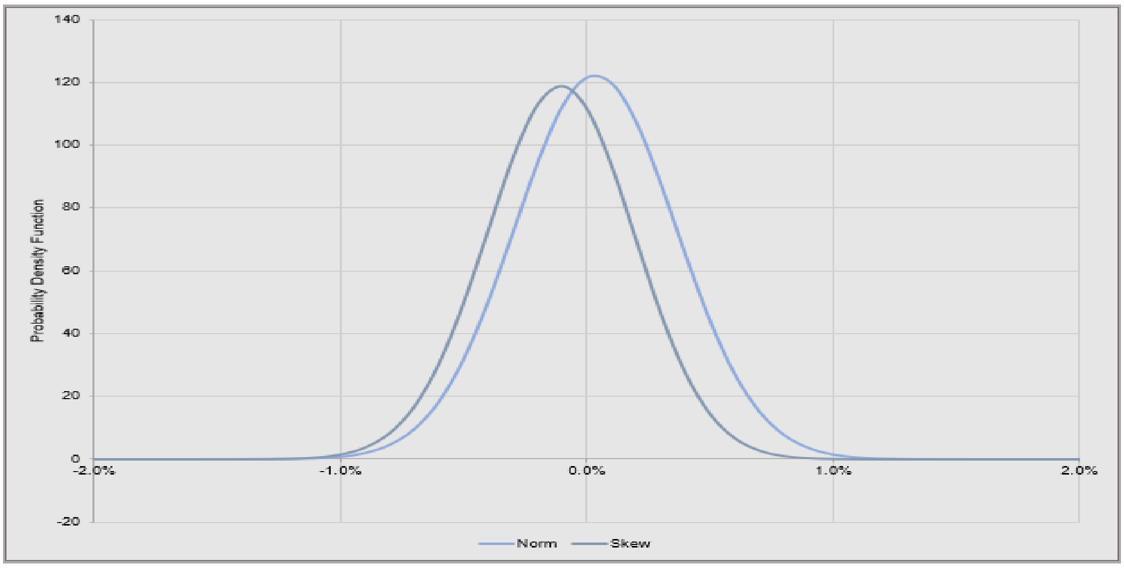


Figure 2: US Treasury Index 18mth daily returns data to 19 March 2020



While the difference doesn't look like all that much in this simple representation, from a risk perspective it is very significant, as indicated by the leftward bias of the skew distribution in Figure 2. At the end of February, a holding in US Treasuries would have shown a 99 percentile worst case loss of -0.67%. A mere three weeks later and that 99 percentile worst case loss has expanded to -1.84%, with an actual single worst day occurrence of a -1.88% loss! Imagine from a bank perspective, a supposedly zero Risk Weighted Asset that they hold no capital against just incurred a loss 2.8x larger than their risk projection, even worse for the traditional investment portfolio that is treating fixed income as a risk mitigant and de facto giving themselves capital relief from holding (likely levered) positions in it against their equity/growth holdings.

This simple mechanism helps clarify why it is low risk (high leverage) things like AAA Super Senior Tranche Sub-Prime CDOs or Eurozone Sovereign Credits, and their respective regulatory treatment, that tend to necessitate bank bailouts and central bank interventions, as opposed to explicitly risky credit activities. You could say the mismeasurement of risk is more dangerous than the riskiness of risk. As the old Mark Twain saying goes: “It ain’t what you don’t know that gets you into trouble. It’s what you know for sure that just ain’t so.”

You could stretch this to a conclusion that the “system” would be safer if banks and other financial institutions took actual risk, that paid some actual return, eg High Yield Credit, capitalised that risk appropriately, and then managed positively convex, negatively correlating exposures to protect against losses in tail events. Instead, they seemingly prefer highly levered, faux riskless, strategies with virtually nil capital protecting against the mis-measured future losses. It is possible to imagine that the former could lead to a less systemically risky financial system!

This brings us back to where we started, the system is fragile. It is impossible to predict when/where/how a spark may occur, but the good news is you don’t need to! It is possible to a) recognize and to some extent even measure fragility, (eg. think reverse testing stress analysis, least worst outcome/maximin scenarios) thus giving the chance to avoid it, and b) adjust exposures to add positive convexity to a portfolio. We say it over and over again: avoid things that don’t participate on the upside but have correlated asymmetric downside, then add truly asymmetric convex protection against the downside, thus allowing you to take more upside participating risk. Arithmetic Average Annual Returns and Value at Risk models are harbingers of Agency Bias strategies, run for the benefit of the fiduciary. Geometric Compounding and Convexity are beacons for the benefits of end capital owners.

The Purpose of Organisations?

By Peter Neville Lewis CMIRM, Director,
Risk Coalition Research Company

Integrity has no need of Rules

(Albert Camus – Nobel Prize (Lit) 1957, died 1960.)

Integrity stands for a set of moral values (or virtues) which have been known for as long as civilised humans have existed. It is closely linked to purpose. At the heart of both is collaboration with other humans beings and the natural universe. Integrity derives from the Latin word Integer, meaning whole. So values and purpose need to be wholly aligned if our world and our lives are not to get out of kilter.

We need a primacy of purpose, both social, commercial and economic, as a driver of behaviours in corporate culture. This is what will underpin more productive and sustainable business models, whilst reducing potential long-term damage. Without due attention to purpose and values many organisations will stall, stumble and eventually dis-integrate.

According to Grant Thornton in their 2020 Corporate Governance Review of FTSE 350 Annual Reports, only 50% of the 280 companies assessed talked about Purpose - not great. But to compound this low percentage just a miserable 6% measured the impact of their corporate purpose. Do the other 94% simply not care?

Clearly the message is not reaching corporate boards. One suspects, without access to any hard data, that the percentages for not for profits will be significantly higher due to their social purpose.

Imposing rules and regulations can be counter-productive. Whilst those designed to enhance safety are in principle good, they need the consensus of all participants for them to work. Traffic lights are a useful example and there is almost universal acceptance of their social values. Yet studies show that, when removed, people exercise greater thoughtfulness and care to avoid harming others. There is no increase in accidents. The reason is that individuals are encouraged to take greater responsibility for their decisions.

Organisations, however, are wrapped up in bundles of rules, codes, policies, procedures etc which largely remove personal responsibilities. Adherence to these is either rewarded or punished. The culture of the nursery!

Do we really want to treat adults as moral infants?

For organisations to thrive and survive in the 21st century they need to collaborate more holistically across all sectors of society.

Pursuit of shareholders' interest above all others has now been challenged at the highest business level. At last year's US Business Roundtable of senior CEOs, Larry Fink of Blackrock ($7 trillion AUM) called for a "reassessment of core assumptions expected about ESG".

The four C's of Covid19, Climate, Culture and Cyber have changed, and will continue to change, the economic business case and model. The current existential crisis also challenges what was often an abstract notion or desired outcome in our thinking about "doing good" and now makes these thoughts only too real. It's become tangible!

Survival is the name of the game but surely not at the expense of others. Organisations and their leaders who are seen to be acting morally and virtuously for all their stakeholders are more likely to see their trust rating and reputational standing improve. This is where reference to a clearly defined purpose statement embedded at all employee levels, plays a crucial role in guiding decision-making and risk taking. Please take note the 94% of FTSE purpose deniers.

A healthy culture is one of the key areas of scrutiny for regulators.

- Is there a psychologically safe, inclusive and diverse culture (in both human and cognitive terms) that can be positively affirmed?
- Does this permeate all levels of an organisation?
- Can all employees whoever they are, bring their "whole selves" to their work without fear of prejudice or disrespect?
- Can organisations point to reliable indicators that all their people exhibit and exemplify good behaviours?
- Is behavioural performance measured as regularly as financial performance? If not, why not? Which drives which?

The answers to these questions, one suspects, lies mostly in the don't know/don't do spectrum.

In a corporate world where more and more is being asked of individual employees to combat an environment where there is a commercial, environmental or social crisis (however large or small) almost every week, how people respond, make decisions and behave is crucial. Can large organisations be sure that across multiple business units and geographies all of their employees:

- do the Right thing?
- do it in the Right way?
- do it for the Right reasons? and….
- do it, above all, based on the Right moral values?

If we have a purpose based on doing things right – acting with integrity - we have a clear direction of travel. To make this happen, we need to work out what it will take to achieve our objectives.

This is strategy (based on purpose, values and goals) and we need to achieve this effectively and efficiently in a viable and sustainable way. We call this delivery - a term preferable to execution, (which has been appropriated by business), with its darker connotations.

Driving all this are the decisions we first make and then take, which involve assessing the risks inherent in meeting our purpose focused goals. It is therefore self-evident that purpose, anchored by moral values, determines risk - never the other way round, a fundamental flaw in many risk frameworks and functions!

Purpose also determines moral behaviours beyond token compliance with regulatory guidelines. The Senior Managers & Certification Regime is welcome as far as it goes but it does not really address the deepest natural aspects of our humanity. Professor Roger Steare (Cass Business School) has cleverly labelled this our Moral DNA, encompassing humility, care/empathy, courage, self-discipline etc. Philosophers refer to these as virtues which are core to our human essence. Transgress these and we are on a slippery slope to moral complacency and eventually a moral vacuum. We lack integrity.

The reputational harm which follows then becomes an issue, particularly in financial services and indeed the Basel Committee now regards “reputational risk” as part of the Pillar2 capital adequacy testing. Social capital is being viewed on a par with risk capital.

It adds a new dimension to VAR - Value or Values at Risk?

Regulators are also now making a stronger connection between operational and, what they somewhat crudely term, conduct risk.

So, to recapitulate, there is an urgent need for financial services businesses, in particular, to recalibrate their business priorities with a greater emphasis on good and fair outcomes for every stakeholder. The court of public opinion may otherwise hold them to account and, in some cases, find them guilty of abusing their licence to operate with terminally damaging consequences.