PUBLISHED BY

CLEAR PATH ANALYSIS

OPERATIONAL RESILIENCE FOR BUY-SIDE INVESTORS

Managing the process of business continuity in investment management through challenging times

JUNE 2020

SPONSORS

milestone group

FRS Invest | Pro™

CONTENTS

OPERATIONAL RESILIENCE FOR BUY-SIDE INVESTORS

Nick Miller, Head of Asset Management, Wholesale Supervision, Financial Conduct Authority

Paul Roberts, Chief Executive Officer, Milestone Group

Frank Carr, Chief Marketing Officer, Financial Risk Solutions

Mike Tumilty, Global Chief Operating Officer, Standard Life Aberdeen

Nick Simms, Director, Cornwood Risk Management (former Operational Resilience Director, M&G Plc., and Programme Manager for Pandemic Flu programme, NHS Tower Hamlets)

Professor Gianluca Pescaroli, Assistant Professor in Business Continuity and Organisational Resilience, University College London's Institute for Risk and Disaster Reduction

Amanda Flynn, EMEA Regulatory Change Manager, J.P Morgan Corporate Investment Banking

CLEAR PATH ANALYSIS

Clear Path Analysis is a media company that specialises in the publishing of high quality reports, events, and online trade media and market intelligence websites in the financial services and investments sector.

FOR MORE INFORMATION:

W www.clearpathanalysis.com

T +44 (0) 207 688 8511

E marketing@clearpathanalysis.com

We value your interest as without our readers there would be no reports.
Please fill out our short survey to give your feedback. The survey will take approximately 3 minutes and all feedback is anonymous.
Click **HERE** to access the survey.

Thank you for helping our reports be the best they can be.

TELL US WHAT YOU THINK

SPONSOR

Milestone Group is an institutional fintech firm serving the investments industry and is recognized globally as the architect of a new class of digital enterprise and industry level solutions based on its pControl investment platform. Milestone Group provides a fresh approach to data, process and product management delivering transparency and operational agility as integrated capabilities across key investment and operational functions.

Currently supporting some $17 trillion in assets, pControl solutions are driving industry innovation for asset allocators including pension funds, fiduciaries and multi-asset product providers, and are category leaders in NAV automation and fund oversight including backup NAV capabilities. Milestone Group's innovative pControl SmartSourcing™ cloud delivery model provides intelligent and more flexible blended operating model choices. Clients trust Milestone Group to consistently deliver innovative and dynamic solutions backed by deep industry expertise. For more information, visit: www.milestonegroup.com

With over 20 years delivering Investment Administration software, Financial Risk Solutions Ltd (FRS) is a trusted technology partner to asset managers, life assurance and wealth management firms worldwide. Led by an expert team of actuaries, compliance and IT specialists, clients license FRS software to help navigate the ever-changing challenges of growth, regulatory pressures and competition in the industry.

The award-winning* InvestPro™ platform is relied on by over 65 blue-chip financial services and BPO clients to reduce operational costs, increase efficiencies and mitigate risk in the manufacture and management of investment products. More than 150,000 funds are managed on the Invest|Pro™ platform today.

Delivered on-premise or cloud-hosted, Invest|Pro™ securely automates multiple complex fund administration processes including oversight, unit-pricing, cash allocation and rebalancing; and NAV validation of operational activity performed by outsourced partners; and in Europe monitoring and reporting for PRIIPs, KID requirements, and Pillar III asset reporting for Solvency II.

FRS is part of the Constellation Software Inc. group and headquartered in Dublin, Ireland, with offices in Hong Kong and Sydney.

For more information visit frsltd.com or follow FRS on LinkedIn at www.linkedin.com/company/frs-ltd

**2019 - Best Solvency II Tech Solution - Insurance Asset Management Awards, Pensions Technology Provider of the Year - Irish Pensions Award, 2017 & 2018 – Tech Firm of the Year – Insurance Asset Management Awards, 2016 – Tech Provider of the Year, Governance Risk and Compliance – Risk.Net Awards.*

Regulator update – the quest for organisational resilience and what it means in practice for firms

Interviewer

Noel Hillmann,
Chief Executive Officer,
Clear Path Analysis

Interviewee

Nick Miller,
Head of Asset Management, Wholesale Supervision, Financial Conduct Authority

SUMMARY

- *The switch from office to home working introduces a new emphasis on monitoring and surveillance of staff activity*
- *Cyber risk is a growing threat to investment groups and the imperative to keep up to date on threat tracking*
- *The definition of 'plausible' will need to rethought post the Covid-19 crisis*
- *The job of the regulator is to prod, question, and respond, but senior managers must decide on the most suitable resilience plans for their firm*

Introductory Statement from Nick Miller

We have been living through a period of extraordinary economic turbulence so it would not be possible for me to provide a complete answer to how regulation can and should change. What I can offer here is some observations of what we have seen so far through the current period for buy-side investment groups and then perhaps some scenarios that certainly we expect firms will be thinking about over the coming weeks and months.

It is certainly true to say that we have seen some really high levels of volatility with some extraordinarily heavy trading flows reflecting very significant client activity at the back end of March and early April. Despite this, what we have seen is that redemptions have been broadly manageable for the sector. We've seen very few outages and none that seem to have, at least so far, caused us concern that they may be of significant harm to clients. Continuity for clients has been there throughout.

Broadly speaking, the investment sector has done well, so far, and has held up remarkably well. This is good to see because operational resilience, as you know, has been a priority for the regulator. My team and I have spoken about it a lot firms across the sector for the past couple of years.

As a regulator, we have wanted to ensure that firms are able to deploy as much energy, focus, time, and resource as possible on ensuring continuity. We have therefore pushed back several deadlines for consultations on some of our policy work. We have expressly put down a couple of pieces of proactive supervisory work in certain cases. Importantly, we've made a number of announcements in the market, not only around the importance of maintaining open and orderly global financial markets but also allowing some flexibility and some forbearance, recognising that firms have needed to focus on the immediate crisis management piece.

There have been several interventions across the sectors, retail and wholesale. Particularly in relation to asset management, we have put down a marker to give extra time for delivering fund accounts.

All of this is of course in the background of an extraordinary switch, literally overnight, from working in the office to working from home. It is true to say that now pretty much the whole of the City of London is working remotely, not at backup sites, but from home. This is certainly true of asset managers where we see almost all staff, barring some essential workers, working from home. This is an extraordinary change and achievement but raises a whole number of questions, in particular around monitoring and surveillance. For example, how are senior managers ensuring that their teams are maintaining good conduct and contributing to upholding market integrity in their trading? Whilst we do recognise that this is a challenge, equally, it is not good enough to say that you just can't do it. We have seen firms taking strong proactive action. We recognise that and it is good to see.

An area of challenge during periods of extreme volatility is valuation. We have done a lot of work on valuation, which is really important to us and to ensuring a good, fair deal for clients. We did a review on this area called our hard to value assets review, which we did back in the later end of 2018. A video summarizing our feedback is still available on the website and we would encourage you to look at this if you are interested.

We point out some areas of good practice but also some areas where we felt the industry could do a bit more.

Another area that has been in focus, for at least as long as I have been in this role, is fund liquidity management. This is about ensuring that you are continuing to operate your collective vehicles appropriately and in line with a good product governance and good outcomes for your investors. This obviously speaks to liquidity management tools such as swing pricing. There is a question here around how effective, consistent, and fair the application of liquidity management tools has been for investors throughout this period.

Of course, this period gives us a lot of interesting data because the use of these tools intuitively will have been more significant than 'normal times', so this is a particular area that we have been monitoring. We do expect firms to proactively reach out to us where they think funds might be coming into difficulty but redemptions have proved manageable so far.

An area that has been of particular interest on the operational resilience agenda has been that of cyber risk. The vulnerabilities have increased here and in fact we have seen today that cyber-attacks are continuing and can be quite significant. Here we want to ensure that firms are doing their best to maintain their cyber defences at this time and that they are doing everything they can to protect the integrity, not only of client assets, but client data. This is a particular risk for the asset management community because you often hold significant data on a client, as well as the nodes, inter connections, and inter relations that you have with other firms as well.

There has been an interesting and somewhat worrying uptake in scams and asset management hasn't particularly been a sector where we have seen so much of this activity previously. What we are seeing now is increased use of phishing emails by rogue actors who are claiming to act on behalf of legitimate firms.

> “WE HAVE WANTED TO ENSURE THAT FIRMS ARE ABLE TO DEPLOY AS MUCH ENERGY, FOCUS, TIME, AND RESOURCE AS POSSIBLE ON ENSURING CONTINUITY”

Another important factor is how you are dealing with your clients, are you communicating with them effectively, do they understand what is going on with their products and investments, and are you considering whether all of your fund range will remain viable in the future? Also, what is this period telling you about client activity and how is this effecting the thinking for your strategy, for your product range both as it exists now but also for what is coming down the pipeline.

Overarching, all these issues, governance is absolutely critical. We recognise that it is increasingly difficult to organise meetings as you can't physically get all of your directors around a table, but nevertheless facilities such as Zoom are there and in fact, technology has improved dramatically over the past couple of years in using these types of virtual communications. We do expect to see really strong board oversight maintained at the level of the authorised fund management entity.

Whilst decision making may become clunkier, more difficult and less efficient you always need to maintain your decision making and governance processes and the best interests of your customers, regardless of market conditions. It is important that you are documenting and thinking carefully about these decisions and recording them appropriately.

Covid-19 has accelerated change in many areas but some things do persist, such as LIBOR transition, which is something that we are continuing to focus on. We have been clear alongside other global authorities that the end of 2021 is the end date for LIBOR. Funds should be working on this basis and this includes asset managers. This does recognise that some of the interim milestones that we had hoped to be met by the industry have obviously moved.

This is also true for all of the value assessment work that has been going on. We are seeing these reports coming through now in material volumes, which is interesting, and has been picked up by the press with different types of commentary. This does speak to the important point on governance whereby you need to ensure that the decisions you are making are in the best interest of your customers and that you can justify them if need be.

For this period, whilst it has had significant human and economic costs that will be with us for the foreseeable future, it is interesting to see what useful data we can gather from it about our attitudes to risk or what constitutes a severe event. Whilst we would all consider this severe; I am not sure we all would have considered it plausible. Certainly, this question of plausibility is particularly important for the sector, as stress testing will need to be rethought. That being said, there is a more fundamental strategic question for this sector, which is around what this sector is going to look like in the future, what is the purpose of the sector and how will it deliver, even during times of economic hardship for many people? How do you navigate this situation and ensure you provide good products for a range of customers who may not be as well off as they used to be, as this situation may be with us for a number of years?

Noel Hillmann: Thank-you for your opening thoughts. What are some of the internal thoughts within the regulator in terms of what 'severe' might be re-defined as? How can the definition of 'plausible' be redefined, as to take into consideration such events as those that we have been experiencing this year?

Nick: The reality is that we are going to need to work through these questions in some detail and very carefully over the coming weeks and months.

It is certainly the case that what constitutes a severe but plausible event is significantly more severe and plausible than many firms had envisaged. We have been talking a lot to firms about the possibility of extreme market volatility or outages. What has changed is that it is no longer appropriate to assume that a period of calm markets will continue for a number of years, so that in 10 years there might be another crisis. The range of economic outcomes that you need to be factoring in and thinking about is significantly different now. Of course, this means that your models need to change, and you will need to update them.

The Federal Reserve (the Fed) is talking about 25% unemployment, or something similar to that level, which is extraordinary. No-one could have predicted this, but you do have to plan and think about these things.

The counter argument to this is that you can't plan for a crisis to happen every month, so there is a balance to be struck here. We do recognise this and although the regulator is happy to guide and give frameworks and guidance, ultimately the answers will have to come from the industry as this is the heart of the accountability regime. We talk so much about governance because we want to see firms thinking carefully about the future, their plans, envisaging risks and thinking how best to mitigate them.

> It is very important that firms are challenging suppliers to understand what their risks of diversification are

We do not expect perfection or for firms to foresee every outcome, but we do expect them to be carefully considering them.

Noel: When it comes to setting minimum operational resilience standards for providers, what kind of information is the regulator likely to ask for going forwards? What questions are you advocating investment firms ask their third-party providers?

Nick: The point is that firms have business risks and they need to oversee them, particularly in a sector like asset management which is heavily reliant on outsourcing, delegation, inter-group arrangements, none of which in themselves are negative. It is more about how you are overseeing them. It is very important that firms are challenging suppliers to understand what their risks of diversification are, how they can demonstrate that their systems and back up plans are resilient through a crisis and what thinking they have done around this. Again, we are not expecting perfection or zero failure. It is not so much about will it fail but rather how quickly it comes back on again if it does fail.

If you are reliant on one firm in one jurisdiction to provide a key business service, you might need to think about this. This isn't to say that we have all the answers or that we know what the future is going to look like. This is an area to consider and these are the kinds of questions that firms are going to need to start thinking on.

Covid-19 has demonstrated that operational resilience is not a theoretical construct that the regulators have dreamed up to annoy firms, but it is real and pretty meaningful.

Noel: **Would regulators more widely appreciate the investment industry diversifying their supplier base and having back stops to their first line suppliers by having second line suppliers and so forth?**

Nick: Yes, that is broadly speaking true. The question that the regulator will always ask is, what happens when things go wrong? The analogy to this is that if the supplier to your trading platform or back office systems goes down, what is your back up? If your supplier can't give you a back up option that you are happy with, then frankly you need to think about an alternative.

We have global supply chains now and this is becoming very real and obvious for all economic sectors but particularly financial services. This isn't an issue so long as you can manage it and understand the risks.

If it is all concentrated with one firm and in one jurisdiction and there is a national strike, what would you do then? This isn't just about compliance, the rules and framework, but actually it is about good business planning.

Noel: **In terms of getting a set of optimal standards for operational resilience in place, are there key pointers you can tell us about that regulators will be asking investors and suppliers?**

Nick: There are going to be several factors which will all depend on their scale, models, etc. It is not as straight forward as simply saying, if you can't outsource it comfortably then it has been insourced. However, in some cases that might be the case.

Again, it speaks to the idea that you need to have a backup plan, so that if the first option fails you have another option. If the company you are reliant on goes bust, what is your next option. It is these types of questions that you need to be thinking about and it will depend on the type of service, the firm, scale, etc. What is interesting about this pandemic is that the system has really been stressed and we have seen a degree of inefficiency creep in with areas slowing down. There hasn't been a big crunch, which is great, but what would happen if there was? At what point do you start to worry about not having a backup or secondary plan available?

Of course, at some point, you must accept that there will be risks. It does come back, however, to whether you have thought about it carefully, appropriately and has it been through good governance processes. Has it been challenged at the board level? It also isn't just about third party suppliers but inter group suppliers as well, so that you need to recognise that if you are part of a group that is headquartered in the U.S and you are reliant on these inter group suppliers, then this is also an outsourcing risk.

Noel: **Broadly speaking would you largely expect investment groups to be bulking up the operational resilience department and risk units or are you happy that, in the majority, investment groups are well-positioned to insure themselves against this situation getting worse?**

Nick: We aren't in the business of telling firms how to run their business. We are here to ensure that the Chief Executive Officer, Chief Operations Officer, Chief Risk Officer, etc., are overseeing their businesses appropriately. Our position is that they need to ensure that they can draw on adequate amounts of human, financial, and non-financial resources when necessary. We may come in and challenge, prod and ask questions about how sensible they are being, which is the job of a regulator, but I don't want to get into a position where I am stating exactly how many people need to be working in a particular area. That would be us being very directive and prescriptive. This is not how I want my team to be operating. I want us to be shaping, guiding and framing the industry, but not being direct in telling people exactly how they should run their business.

Noel: **Considering the past couple of months, with Covid-19 and its globalised nature, has this strengthened the argument for a more global, interconnected approach by regulators? Do you for see greater cooperation between regulators in the future because of what we have seen with Covid-19 and how does this relate to Brexit related discussions?**

Nick: Within Europe and more broadly, regulators do need to maintain cooperation. We have been very closely working with a lot of European regulators, with the Luxembourg and Irish regulators in particular given that they oversee the European fund hubs.

Supervisory and regulator cooperation on the ground, particularly during a crisis, is critical. It is about communicating effectively, sharing, and having those principles in place. To a large extent, the legal framework for this is governed by the IOSCO Multilateral Memorandum of Understanding. There are various other protocols supporting that bilateral memorandum of understanding that we will have, which is agnostic to Brexit. It is absolutely critical, but it also demonstrates that it is a globalised world with global supply chains and what happens in a Luxembourg fund will affect a delegate manager in the US and the authorised manager in the UK, and so forth.

Noel: **Thank you for sharing your views on this topic.**

Operational resilience – new thinking in 'insurance' based operating model design

Paul Roberts,
Chief Executive Officer,
Milestone Group

SUMMARY

- *Regulators have shifted attention to preventing outages rather than how best to deal with their fallout*
- *Covid-19-19 has underscored the need to re-think plans and plan for the unplannable*
- *Oversight of fund accounting has been treated as a necessary evil, but new platforms are creating value-add through automated approaches*
- *Automation adds an additional check for added risk mitigation*

Progress rarely follows a linear path. More commonly, a series of incremental improvements is punctuated by a major leap, prompted perhaps by a breakthrough in technology, change of leadership or necessitated by crisis. At first glance, it would be easy to conclude that the disruption caused by the global pandemic of Covid-19-19 has effected such a leap in thinking about resilience and operating model design for the buy-side. The reality, however, is more nuanced.

At Milestone Group, we have been thinking differently about operational resilience for several years. Across the last few years, our thinking has been gaining ground within the industry – and with industry regulators. The fallout from Covid-19-19 has, in this instance, only underscored the importance of this new way.

The concept of Insurance as part of Business Continuity Planning

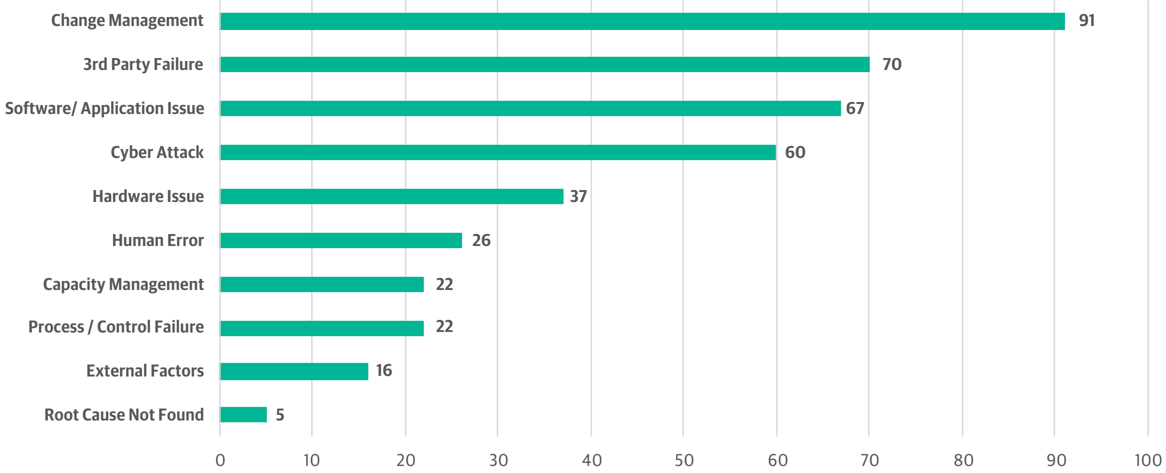
Previously, conversations about resilience focused on prevention. Detailed Disaster Recovery (DR) and Business Continuity Planning (BCP) policies laid out how businesses would avoid the failure of core operations. This concept underpinned the value proposition of outsourced providers for many years. It was common to hear the argument that outsourcing made good sense because the outsourcer had scale, critical mass of expertise, the ability to make significant investments in contemporary technology capabilities, and that they had invested heavily in DR in a way that an individual firm might find it hard to replicate. In short, it was just safer.

But what is increasingly clear is that this focus on prevention is no longer enough. Regulators globally have embarked upon a coordinated programme of raising awareness and expectations of responsible parties that is strengthening the accepted definition of resilience. This now specifically includes arrangements that a firm has made when an outage does occur, rather than focusing on preventative measures and assurances that this won't happen. The mantra is to plan for not if but when such an event occurs. In other words, alongside DR and BCP must sit the insurance policy.

In this context, we don't mean the textbook definition of insurance as a financial instrument to compensate in the event of a financial loss. It is about having a practical, alternative mechanism to deliver a business outcome when the primary way of achieving a given outcome fails unexpectedly.

If we look at the Financial Conduct Authority's (FCA's) data that provides insights into all operational disruption, it is no surprise that the theme of resilience continues to gather momentum. Note that third party failure is reported as the second highest contributor to operational disruption. Moreover, there are broad swathes of contributing factors that need to be addressed in operating model designs.

Root causes of Operational Disruption reported to the Financial Conduct Authority (FCA) between October 2017 to September 2018



Source: Financial Conduct Authority, Cyber and Technology Resilience: Themes from cross-sector survey 2017/2018, November 2018

In addition to the regulatory framework being developed in the U.K, there have been regulatory developments on similar themes in the U.S, Singapore, EU, and Australia. This confirms that this is not a fad but instead the new industry normal. Industry practitioners will need to embrace and understand how to efficiently achieve an embedded resilience culture, rather than resisting the discipline as a regulatory overhead.

The recognition of a shift in thinking from risk management is key. Understanding how the functions of a business are undertaken is expected. Disruptions will occur and Net Asset Valuation (NAV) production is one of the functions that is noted as being fundamental.

Resilience in the time of Covid-19-19

The disruption and dislocation caused by Covid-19-19 has underscored the need to plan for the unplannable.

In general, systems appear to have held up well in this pandemic with models not tested to their limits of processing and operation. There has been no wave of breakages that would point to a systemic frailty of individual technology.

What is interesting is the combination of events that has created scenarios that were not necessarily planned for as part of a normal Disaster Recovery or BCP arrangement. Consideration needs to be given to a combination of factors that collectively change the risk profile of firms and indeed the industry where these factors affect a wide range of industry players simultaneously.

There is also a heightened level of systemic risk due to the impact on staff, which is not limited to the workplace. Organisations that are heavily offshored in second or third world economies have generally had more adjustments to make than those firms who have retained a significant portion of local labour or who are more automated. The assumption that your staff would be able to access a primary or secondary location proved incorrect. The advent of mass working from home has put additional stress on staff who live in more crowded environments, in areas with limited or unreliable internet or who simply don't have access to a laptop. Beyond these logistical issues, staff may be distracted by issues relating to health or the loss of friends or relatives.

We have seen traditional BCP assumptions on how best to move work between sites now being rethought with the pandemic disrupting all locations. In this sense, distributed operating models are not a catch-all for resilience planning.

The principles that flow from an understanding of operating model design capacity – resilience planning – are increasingly focused on building resilience into technology rather than relying on people or offshoring.

When speaking to an organisation about the percentage of their staff that have been able to work from home and why, this has only been limited by their dependency on systems that do not conform to production management standards. This has not gone unnoticed, and will doubtless be a key learning point from the pandemic.

NAV production

As one of the most mission-critical functions of fund servicing, NAV production exemplifies the importance of the insurance-based approach. If you take a normalised expression of the end-to-end process associated with producing a NAV, it includes upstream activities such as trade processing, corporate actions, the striking of the NAV, followed by automated validations. Any exceptions are escalated, remediated, and then the NAVs are disseminated. This process may be undertaken internally or by an outsourced fund administrator. As you would expect, the typical fund accounting agent will use several technologies to manage this end to end process.

The process is supported by an operating model that can be thought of as having several layers that represent disciplines and infrastructure that need to work in concert to produce an outcome.

At the bottom, there is a data layer. Above this we have the functions that make up the end-to-end workflow. In the next layer is the unification of the end-to-end process: a workflow that links the functions and manages the statuses associated with the overall processes. The fourth layer is the control framework, typically represented by a dashboard that allows the fund accounting team to understand what is happening within their automated process. It provides the framework that deals with the exceptional circumstances across any of the layers of the operating model.

This is, of course, a simplified view. The production of a NAV is complex. Things can and do go wrong and result in errors and inaccuracies. On occasion there is a catastrophic failure of a component that causes a major delay or outage in the production process and the NAV may either be late or not delivered on that day.

As the NAV is required for clients to trade with confidence, it must meet multiple resilience criteria. Many asset managers are serviced by more than one fund accounting provider and consequently are overseeing multiple versions of the operating models. This presents huge challenges in terms of the consistency of processes, controls, data formats and reporting across their funds.

Historically, oversight of outsourced fund accounting has been treated as a somewhat necessary evil that has been thinly resourced and not fully recognised or supported as a business-critical function. Fortunately, this situation has changed dramatically in recent years, with professional oversight functions now the new norm and a range of automated options becoming available.

There is an emerging trend to utilise specialised investment oversight platforms that have the ability to accurately predict a NAV, which can be compared with the actual NAV and provide supporting analysis of any of the components that are contributing to the difference. Importantly, this can now be achieved without the need for shadow accounting.

Resilience is built into the NAV production process as the client can detect and alert their service provider to any errors prior to that NAV being disseminated to the market.

This approach has challenged fund accounting agents to provide data promptly to ensure that tight NAV release cycle times can be met. That challenge has – in the main – been met positively, as service providers realise that both they and their client benefit from more resilient processes.

This automation of the oversight process adds to the resilience of NAV production: by adding an independent check to NAVs produced using different checking methodologies and data elements ensures that the process does not replicate the same errors as the primary process, and does so in a timely way.

Introducing insurance based operating models

But there is an opportunity to take this further, in response to the recognition that on occasion, there will be an outage that will occur for reasons that were not foreseen. Regulators are making it increasingly clear that they not only expect firms to have in place contingency arrangements for interruptions to outsourced functions, but also that this will be considered an integral part of operating model design, considered with equal weight to internally run processes. This is a much higher and visible level of accountability for outsourced arrangements than has previously been the case.

But consider the situation when you are informed by your fund accounting agent that a NAV will not be available for some reason. No amount of oversight can rectify that situation. This is where the insurance-based model comes into its own.

Where this approach has been adopted, a firm will have built-in a back-up NAV capability. When required, it takes a computed expected NAV, puts it into a workflow and undertakes any data enrichment required, applies validations and provides an authorisation workflow that allows the alternative NAV to be released to the market as a backup NAV. The back-up NAV is providing the insurance that is independent of the cause of the service disruption. Of course, this process also needs to know how to handle confirming and synchronising with the actual NAVs when the accounting agent is back online.

Forward-thinking firms are building oversight and back up NAV arrangements into operating models from the start of an outsourcing deal, which offers protection during transition periods. Though, of course, this does require organisations to accept the possibility of an outage, which seems somewhat counterintuitive.

There has been a significant increase in organisations undertaking some form of oversight since our last survey in 2014. We found that 100% of firms surveyed are now undertaking some form of oversight. Additionally, 88% of respondents indicated that they now see it as important that oversight is undertaken independently from their fund accounting agents.

There has also been a notable increase in awareness of the role of the contingent or back-up NAV with a significant uptick in and intentions to undertake projects and implement robust contingency arrangements. 94% of firms indicate that they would expect any contingent or back up NAV to operate independently of the fund accounting agent. Nine out of 10 firms believe that regulators and fund boards have raised their expectations on this topic.

The resilience agenda is real, is here to stay and is being practically applied in meaningful ways throughout the industry. It is important to remember that when dealing with supply chains that cross corporate boundaries, we are likely to need to forge solutions that more simply traverse these boundaries and add value and resilience to both outsource suppliers and clients alike. We will see an increased level of clarity of understanding and thoughtful designs around business-critical functions that addresses fortification and core processes in much the same way that BCP and DR plans seem to do today. We will also see an increased focus on selectively using additional alternate insurance-based arrangements with critical functions that represent protection against a breakage or outage. Progress looks set to continue apace.

Raising oversight standards - it's time to focus on your outsourcers

Frank Carr,
Chief Marketing Officer,
Financial Risk Solutions

SUMMARY

With outsourcing on the rise, Financial Risk Solutions (FRS) CMO Frank Carr explores the implications for operational resilience and how with best practice and quality software relationships can strengthen between Asset Managers and their outsourced providers.

Good relationships with strong outsourcers are what every asset manager strives for and where these exist, outsourcers can expect more assets and business functions to come their way in the months and years to come. Fee, regulatory and competitive tension means that strategically fine-tuning the manufacture and distribution of great products, on top of asset selection, is more than enough for asset managers to perfect in the year 2020 - a time where assets under management (AUM) are reaching new levels.

The back office is sometimes not up to the task and can be a cumbersome and unprofitable poor relation in an otherwise relatively scalable global model. The emergence of new technologies, such as AI and machine learning is further increasing the demand for specialised and agile outsourced providers to support digital transformation.

Industry research points to the continued growth of outsourcing. A report from the Central Bank of Ireland[1] on outsourcing (November 2019), found that 40 per cent of regulated firms were planning additional outsourcing activity over the next 12 to 18 months. While PWC predicted "outsourcing of middle-office services, while still nascent in Asia, due to a lack of established providers and a reluctance to relinquish control, will nevertheless see an upward trend over the next decade" in their Asset & Wealth Management 2025 report "The Asian Awakening" (January 2019). [2]

This trend, however, adds further complexity to risk management processes and comes at a time when the industry is faced with increased regulatory pressure. As fund providers strive for higher standards with their people and systems, they must also consider their outsourced providers.

The Regulators view on oversight and key issues facing the industry:

At the Operational Resilience for Buy-Side Investors seminar in May this year, the Financial Conduct Authority's (FCA) Nick Miller provided a timely reminder of their policy and what organisational resilience means in practice for firms. His presentation included a look at appropriate oversight specifically for asset managers noting that it is important to understand what backup outsource providers have and what systems are in place to maintain the high framework of current industry standards. Also noted was an open communication policy to ensure satisfaction or raising concerns with providers to safeguard a culture of continuous improvement.

Knowing what good oversight looks like and having the confidence that fund managers are also alive to their risks and subject to independent scrutiny is a key part of the delivery.

At an industry level, Miller noted the FCA is keeping an eye at this difficult juncture between liquidity risk and the clear flow of information to consumers and investor groups. Cyber risk is also high on the agenda, which is comforting. During this challenging time, the last thing needed is for the sector to be compounded by unchecked cyber-attacks.

Further, it was reassuring to hear there is great co-operation from the United Kingdom with global regulators, with Luxembourg and Ireland in the context of the funds' industry, and separately with the Securities and Exchange Commission in the United States. With multi-lateral processes and agreements in place, global supply chains are strong but not immune to adverse shocks that can have significant international impacts. Therefore, all regulators must work together to mitigate such risks.

Improving risk management practices in asset management

There are three core pillars for asset managers to adhere to when raising standards and improving risk management practices in their firms and with outsourced providers:

1. Meeting compliance requirements and reducing the associated financial and reputational risk
2. Maintaining optimum staff, AUM and fund number efficiency ratios
3. Increasing regulator, board and client approval and satisfaction

Progressing each of these areas through the automation of governance risk and compliance supports asset managers in building a culture of transparency. Robust technology monitoring and reporting systems obviously play a crucial role.

At FRS, we developed InvestProTM Fund Oversight to provide an automated NAV and unit price validation framework. Where exceptions are identified, users can set the rule severity, edit rule conditions to change lower-bound and upper-bound parameters, add comments to rule violation and update exception messages.

Analysis of exception metrics are generated per rule, and the rules and exception severity are reported in real-time. The system prioritises the most impactful issues to be investigated and corrected first and can be set to 'stop down-stream processes' for severe compliance items.

Some of the value-added in a proprietary system that monitors, captures and records exceptions relates to instilling a strong corporate culture of continuous improvement, and importantly having the software to back up this culture. These improvements are tangible and physically recorded over time. Clients, the board and regulators like to see these improvements evidenced.

'Material outsourcers contracts' have come a long way in the asset management industry in recent years. In the past, it was areas like negligence that got the headlines. Now standards are achievable with software such that continuous automated checking is becoming mainstream.

Our experience at FRS teaches us that oversight software and systems should include these important areas;

- Fund valuation, investment mandate and regulatory compliance oversight
- Robotic automation to include scheduled automated activities once compliance is achieved and recorded, which includes time and date stamped records of human activity and sign off
- Exception based processing, with a full history of exceptions and associated resolution
- Interactive data visualisation to drill into data and graphical representations of all contributors to the fund valuation movement
- Audit trail and reporting with consistency across all business units
- Artificial Intelligence (AI) to identify outliers, which spark possible alerts recommending logical resolution options
- Collaborative AI metrics service focused on continuous improvement across the platform
- Multi-jurisdiction with core rules alongside country-specific rules, keeping each country's data separate with a consolidated view for analysis and validation
- Easy configuration and intuitive user interface to ensure teams are up and running quickly
- Cloud hosting can be ideal for multi-country operations, rapid scaling and maximum efficiency

Establishing solid relationships between Asset Managers and their Outsourcers

The purpose of operational resilience and oversight should be to identify issues, improve processes and commend good practice. Central to this is to provide early alerts of exceptions to be fixed before they become problems. This should be conducted in a collaborative, constructive way and importantly prevent or eliminate the future occurrence of problem areas. In the past oversight was a newly evolving area. Fortunately, now we see the dynamic has switched to provide detailed real-time information to the key roles across the business. Today, the heads of investment, finance, audit, IT and the Chief Risk Officer, have the oversight information they need simultaneously or at timely intervals.

Today, most asset managers can monitor and see when standards drop; service definitions are explicit and documentation plentiful. It is generally known whose role and responsibility every aspect of the process chain is. There is maturity in both customers and contracts, and suppliers are fully aware of their minimum obligations and are proactive. Tender processes also

> THESE IMPROVEMENTS ARE TANGIBLE AND PHYSICALLY RECORDED OVER TIME. CLIENTS, THE BOARD AND REGULATORS LIKE TO SEE THESE IMPROVEMENTS EVIDENCED

encourage improving standards. Getting the relationship right between the outsourcer and asset manager has just rewards in a situation where asset managers are pushing open doors for additional business in many market sectors.

Despite such progress, we still find that these relationships are failing. An EY survey[4] (2019) found that less than 25 per cent of organisations are reporting third-party exceptions or incidents and significant issues to the board. The Central Bank of Ireland[3] (2018) noted that 12 to 15 per cent of critical or important outsourcing arrangements undertaken by regulated firms surveyed are further outsourced to sub-contractors.

We understand that some outsourcers have different ways of looking at resilience. For example; one global asset manager uses an 'impact statement' approach at the individual incident level, which can help in the clarity. For instance, if settlement is late, the exact consequences and costs of this precise event are captured with the exception that happened.

What was previously considered to be severe and implausible is now suddenly acceptable due to Covid-19-19. This event is so severe and disruptive globally, with many businesses closed and home working the new normal. Modelling scenarios with this mindset of extreme circumstances in the outsource context of the delivery of service to clients can be an extremely difficult task.

At FRS, we developed two levels of oversight software to support new industry requirements - Invest|Pro™ Extra NAV and Invest|Pro™ NAV Insurance. This unique approach means oversight can be deployed within departments or geographies, where one set of funds may need extra rigour. Experience tells us there are sometimes five or ten per cent of funds that cause problems, so it is important to highlight these (if they are known) and apply additional rigour to these funds, which may have several additional data points to capture, report and provide oversight on. This helps the relationship between the asset manager and the outsourcer.

Invest|Pro™ Extra NAV uses a second different data source to your outsourcer and can be used when an outsourcer fails entirely or even just falls short. Although this happens rarely, it is essential in some markets to have such rigorous controls and plan for rare events. All Invest|Pro™ NAV's are calculated using two methods.

Because operational oversight needs to extend beyond one outsource supplier, Invest|Pro™ has also incorporated a tool to manage the governance of relationships. Combined with actual data and detail pertaining to each relationship, the Invest|Pro™ rules and exception framework monitors, measures and introduces a consistent culture across all essential suppliers.

It provides a comprehensive user-definable dashboard for monitoring outsourcers and other suppliers, with visual alerts and key metrics displayed in an intuitive, user-friendly way to assist asset management departments. Both the outsourcers and the client can use the same system to encourage the necessary access and standard raising culture brought about by close factual observation.

What is achievable with good oversight, today and in the years to come

Removing the emotion from oversight is essential when giving a critical appraisal of outsourcers, systems, processes or software.

This brings us back to the three pillars of good oversight:

1. Meeting compliance requirements and reducing the associated financial and reputational risk
2. Maintaining optimum staff, AUM and fund number efficiency ratios and
3. Increasing regulator, board and policyholder approval and satisfaction

We continue to see alignment in the adoption of the three pillars of good oversight with performance metrics. For example, where our clients are exceeding expectations in pillar 2, then pillars 1 and 3 tend to be satisfied also.

Below is an excerpt from an FRS user conference that demonstrates efficiency levels in the investment administration departments of various leading firms that are adopting automated oversight and completing processes on the software. One firm has six people processing and doing the oversight of GBP 26bn across their 6,000 fund of funds, 1,000 mirror funds and 800 individual portfolios. This equates to 1,300 funds per person, all with daily NAV's.

Oversight software has come a long way in recent years and staying ahead of internal parties requirements, such as audit, risk and board-level, along with external regulatory and client aspirations is an enormous challenge for today's asset managers, fund manufacturers and outsourcers alike. FRS dedicate vast resources annually to improving and solving these challenges with the Invest|Pro™ software suite.

Client Type	Staff Count (FTE)	Assets Under Mgmt	Multi Asset Funds	Fund of Funds	Mirror Funds	Schemes / Individual Accounts	Funds per FTE
Pensions Fund Admin	6	GBP £26bn		6,000	1,000	800	1,300
Third Party Administrator – Life Funds	2.5	$3bn		370			148
Life and Pensions Organization	3	€14bn	150	1,925			691
Wealth Manager / International Life Co	4	GBP £12bn		350	150	11,000	2,875

References:

[1] *Central Bank of Ireland, Outsourcing activities in financial service providers (November 2019)*

[2] *PWC, The Asian Awakening - Asset & Wealth Management 2025 report (January 2019)*

[3] *Central Bank of Ireland, Outsourcing - Findings and Issues for Discussion (November 2018)*

[4] *EY, UK Finance Third Party Risk Management Report (April 2019)*

How to govern operational resilience standards both internally and among third-party providers

Moderator

Sara Benwell,
Editor, Fund Operator

Panellists

Mike Tumilty,
Global Chief Operating Officer, Standard Life Aberdeen

Nick Simms, Director, Cornwood Risk Management (former Operational Resilience Director, M&G Plc., and Programme Manager for Pandemic Flu programme, NHS Tower Hamlets)

Professor Gianluca Pescaroli, Assistant Professor in Business Continuity and Organisational Resilience, University College London's Institute for Risk and Disaster Reduction

Amanda Flynn,
EMEA Regulatory Change Manager, J.P Morgan Corporate Investment Banking

POINTS OF DISCUSSION

- *Operational resilience planning is about understanding the critical internal and external partnerships, right the way through the organisation*
- *Investment firms don't command the leverage to bargain with major suppliers on their own so need to act collectively, but within competition rules*
- *It is important to consider the need to go to market against the requirement to manage the risk of every action*
- *Future operational planning will be about building on recent lessons learnt and re-testing for new scenarios*

Sara Benwell: What qualifies as Important Business Services that require the most attention in operational resilience strategies?

Amanda Flynn: The current focus is to establish the right set of criteria for determining if a business service is critical.

As a starting position, business services will be assessed against the Bank of England's criteria set out in the December 2019 Operational Resilience consultation papers e.g. the service has the potential to cause harm to customers, harm to participants and harm to self. Globally, several regulators are just starting on the operational resilience journey and we expect more guidance to be provided. Therefore, we expect the criteria to continue to evolve.

Industry groups likely will have a role in establishing common understanding of what makes a business service critical.

From an individual firm's perspective, the global definition of a critical business service needs to make sense, balanced with regional regulatory needs.

Mike Tumilty: In the asset management space the key business service is technology given that all our critical processes are driven by systems, e.g. Charles River, risk systems, performance systems, client reporting, and so forth. Coupled with that would be telephony and the overarching reliance on broadband to provide connectivity for colleagues. We are also inherently reliant on third party service providers, for example, Citi, State Street, and BNP Paribas for custody and fund accounting.

> THE COMMON ASSUMPTION FOR OPERATIONAL RESILIENCE IS THE AVAILABILITY OF TECHNOLOGY, AND THERE IS A GROWING ATTENTION TO CYBER THREATS TO MITIGATE DISRUPTIONS

Nick Simms: An Important Business Service is something that delivers a specific outcome to an external end user or market participant where disruption could cause intolerable harm – not just inconvenience – to consumers, the market, or the firm itself.

The Investment Association working group identified six high-level generic Important Business Services for asset managers: payments in; payments out; investment; custody; valuation; client and regulatory communications. Each of these was then broken down further.

From experience, it may be appropriate to focus on just one aspect of a business service delivered through one channel, say access to online valuations, and think of other means of delivering the same service, e.g. snail mail, as one of alternative delivery options in a disruption.

Professor Gianluca Pescaroli: Each organisation is unique and every consideration to be taken must consider their operational context. The common assumption for operational resilience is the availability of technology, and there is a growing attention to cyber threats to mitigate disruptions. However, it must be considered that those are just one of the many triggers of possible disruptions. Operational resilience strategies should give more attention to understanding and assessing which invisible utilities that can be the lifeline of other core business services. For example, the satellite infrastructure and its implications for both transactions and Information Communications Technology (ICT). Thus, it is strongly needed to address the common vulnerabilities to their partial or total disruptions.

Sarah: Looking at assigning accountability, for multi-jurisdictional and worldwide groups, what key questions do we need answers on from parent companies and how best to hold them to account on deliverables?

Amanda: The Bank of England consultation paper sets the ownership with the Board and senior managers – and includes several new requirements to demonstrate accountability; for example, in making investment decisions.

We need to understand the accountability requirements from other regional regulators. There are several overlapping existing global regulations in this space (e.g. recovery and resolution, cyber) with further operational resilience regulation expected.

Mike: What is vital here is to have very clear policies and frameworks, which cover the entire firm wherever it operates. That does not mean to say one size fits all, but having overarching policies and frameworks that can be leveraged is really important so minimum standards can be set globally.

Nick: This is difficult, particularly if the parent company or other parts of the group are subject to different regulatory regimes. The US and Basel Committee on Banking Supervision (BCBS), for example, have taken a slightly different approach from the UK regulators. The only way to get round this is for multi-jurisdictional groups to adopt a single, globally consistent approach and to have watertight, enforceable, intra-group contracts spelling out accountabilities and deliverables.

Gianluca: Complementary to the attention to complex issues, organisations should constantly monitor and verify that they are not missing the basics, which in a fast changing operational context may be taken as assumption and become visible just in time of crises. There are two key elements that we need to ensure consistencies across the whole groups, and they may be not rocket science:

1. To what extent are all the basics really done consistently? So, for example, are you really talking the same operational language across the group and the departments?

2. To what extent are the cascading effects of other infrastructure failures are considered consistently and integrated in the existing procedures?

These have now been included in the last ISO 22301:2019 and NFPA1600:19 but are often associated with add on more than being considered in their practical implications. For example, do you have a contract for your generators, or do you have them in place, trained and with a gasoline reserve? Are the critical third-party providers doing the same?

Sarah: How should we determine "severe but plausible" scenarios now and how can we measure such risks?

Amanda: There are several existing mechanisms in place to both: measure risk to firms; and to design test scenarios. The theme is to leverage and build upon these existing frameworks rather than re-inventing or duplicating.

The recent consultation paper throws an interesting new lens on scenario design – in particular, what scenarios are we not planning for? It is early in this analysis, and it is hoped this will help us understand the service resilience limits better.

Before, say, March 2020, would anyone have considered a global pandemic that has infected millions and led to the deaths of hundreds of thousands of people "severe but plausible" or was it "very extreme and barely plausible" and, therefore, outside what we should have been planning for?

Gianluca: I do not believe in "severe but plausible scenarios", because this helps in a limited way to address uncertainties. Moreover, "low probability high impact "does not mean "It won't happen tomorrow". In science and statistics this point is very clear, but this is often missed when translated into decision making. I suggest, start with identification, which can be common vulnerabilities and cascading effects to different threats, assessing which could be the common paths of possible escalations that we may need to address. This is done for increasing the capacity to take decisions in situations of high uncertainties. For example, think about an extreme space weather event and a targeted cyber-attack: the global navigation satellite system may be affected, and the operational implications may be very similar. This could be common to other triggers and threats.

Sarah: What are the new lessons for drafting Service Level Agreements and how has this changed the holding of suppliers to account?

Amanda: There are two lenses on SLAs here: Where clients contract with the Firm for services; and where the firm contracts with third party vendors for services. Both categories are likely to require further thought for Service Level Agreements (SLAs).

> "what scenarios are we not planning for?"

Mike: We constantly scan the operating environment to understand changing risks and events that ccould impact component parts of our business or indeed our whole business e.g. cyber security, political, environmental, social, technology, economic, and so forth. Which could impact component parts of our business of indeed our whole business. We do an annual scenario planning exercise, which simulates a plausible scenario and tests how we as an organisation would respond. We aim to quantify the risks of the scenario, identify the likelihood of it occurring and how things might manifest themselves. We then look at what mitigants we could employ and what other things we may need to consider. These exercises are subject to external assessment from an independent third-party.

Nick: The Financial Conduct Authority (FCA) seems quite clear that firms are not required to measure the risks of any particular scenario occurring but should focus on what to do when – not if - the Important Business Service is disrupted.

We are being asked whether we could stay within our impact tolerances in the case of a "severe but plausible" event but it is not clear what "severe but plausible" means in this context.

There is the potential for this regulation to introduce a new standard of industry expectation – and we would be looking to leverage collective engagement across the industry where appropriate.

Mike: All our big contracts have a very clear and consistent theme with respect to the adoption of contractual breach. This removes ambiguity in the event of who is liable when things go wrong. Contracts are all underpinned by very detailed Service Definition Documents which set out who has responsibility for what in the provision of services. SLA's operate with very clear Key Performance Indicators (KPIs), which are reviewed in some instances daily, weekly, and monthly. We also have in place very clear Service Credit Mechanisms (SCMs), which are designed to remedy underperformance from suppliers. One key thing is that the SLA's are SMART but realistic.

Nick: One of the challenges for many buy-side firms is that they are too small to properly challenge their suppliers. This is true even of the biggest fund managers who are dependent on the big cloud, payments, order management system and custody providers. The only way firms can tackle their suppliers is collectively. This is difficult because of competition rules. We are seeing industry bodies lead

> ONE OF THE CHALLENGES FOR MANY BUY-SIDE FIRMS IS THAT THEY ARE TOO SMALL TO PROPERLY CHALLENGE THEIR SUPPLIERS

in this area. For example, there are initiatives to work with supplier utilities on having a standard set of questions that are posed to providers and can be used as the basis for any follow-ups.

Firms need to fundamentally rethink their procurement practices and their contract terms so that only those suppliers who can meet at least minimum resilience and recovery requirements are even shortlisted for contracts. Too many contracts and associated SLAs talk vaguely about recovery but have no specific requirements and rarely, if ever, mention resilience.

Gianluca: The new lessons are associated with an increased relevance of cascading effects of technological failures, that can impact suppliers both directly and indirectly and must be considered for operational resilience. For example, direct impact to suppliers may be caused by targeted cyber-attacks, or indirectly they may include the consequences of disruptions on other infrastructure sectors, such as a blackout. The complex network system in which we are operating implies a raised value of common scenario and exercises with key suppliers, as well as defining realistic service level agreements derived from joint stress testing.

Sarah: Given the global dynamic of the recent pandemic, has the case grown for removing centralisation of operational support functions or has it grown?

Amanda: There is a difference between centralising functions versus overly concentrating functions. Centralising functions into regional 'centres of excellence' spread across the globe remains useful, particularly to support 'follow the sun' operating models.

But care needs to be taken to ensure that concentration of specific activity is spread across the regional hubs. And that coverage in other regions is available.

While Covid-19 may hold current focus, this same principle applies to other similar risks - political instability, climate events, etc.

Mike: I'm not sure the case has changed but what has been reinforced is that need for functions to utilise common technologies and for those technologies to be deployed on a remote basis. The other thing that the pandemic has reiterated is the need to try and automate more processes that involve manual tasks and activities where possible.

Nick: The pandemic should certainly make asset managers think about how and where they run both their investment and support functions. There are many organisations where the back office is geographically decentralised but the trading and investment decisioning is all in one place. Does that really make sense?

We need to think wider than geography, though. Many firms have concentration risks throughout their investment process, from suppliers, systems, and staff and this needs to be systematically addressed.

Gianluca: The case has grown for a balance between the two solutions. The situation is still evolving and there is the need to achieve the maximum flexibility in the system that should be able to compensate and adapt depending on the scenarios that will arise in the next months. This includes the possibility of concurrency of events, e.g. storms, flooding or extreme space weather happening during the pandemic that could strain further the resources available.

Sarah: According to a FCA report into Cyber and Technological Resilience from November 2018, 91% of disruptive events came in periods of change management. How can we best minimise these threats?

Amanda: Robust change management practises are well known with industry standards in place. Oversight of the implementation of these practises is a key. The identification of critical business services should help focus and prioritise this oversight.

> CHANGE IS THE ONLY CONSTANT THESE DAYS, SO ALL DISRUPTIVE EVENTS COME AGAINST A BACKGROUND OF CHANGE MANAGEMENT

Mike: How we manage change is imperative and how we ensure quality in each stage of the change management life cycle, but testing from both a functional and non-functional perspective is critical. The reputational impact associated with a cyber-attack because of any perceived negligence is massive and to that end, demonstrating that testing has been full and comprehensive is a key mitigant.

Nick: Change is the only constant these days, so all disruptive events come against a background of change management. The challenge is getting the right balance between "good discipline" and go to market. The two biggest financial disruptions in the past decade, RBS/NatWest and TSB, both came from rushed migrations against the clock that weren't thoroughly tested on the exact target platforms and neither had clear and demonstrated back-out plans.

Firms need to take a very good look at their change management processes and ensure that resilience is appropriately embedded from the start, not seen as something that can be added later. We are all aware of new products or processes that were being trialled for one or two customers and suddenly the whole firm or a whole product suite is dependent on them.

Gianluca: Change is an essential part of a dynamic organisational environment and is a constant praxis in the global networked society. We want to maintain flexibility and resilience instead of losing it in the process. This is possible investing in three aspects:

1. Minimise the loss of organisational knowledge that could happen with the change of roles of personnel and the turnout, including the standardisation of training for new personnel to allow and update practices of stress testing

2. Identify, train and exercise the common vulnerabilities to different treats that could be even weaker spots during transitional periods

3. Integrating bottom up perspectives and feedbacks of personnel on the first line that could be aware of invisible points of failures and bottlenecks that need to be preserved during change.

Sarah: **Thank-you to everyone for taking part and sharing your views.**

CLEAR PATH ANALYSIS

TO READ MORE FREE REPORTS VISIT:

www.clearpathanalysis.com

W www.clearpathanalysis.com
T +44 (0) 207 688 8511
E marketing@clearpathanalysis.com
ClearPathAnalys
clear-path-analysis