Managing Risk, Leveraging Technology and Building Resilience for the World's Official Institutions

An insight on the vital importance of data integrity and the robustness challenge

ORC
Operational Risk Consulting Limited

STATE STREET.

As data continues to grow in importance, official institutions today face increased complexity in operating models and require heightened diligence.

State Street partners with Operational Risk Consulting to explore these challenges and engage in a discourse to navigate them.

The Vital Importance of Data Integrity and Security

Oliver Berger
Head of Official Institutions, Europe, Middle East and Africa,
State Street

The clear trend in data management across institutions today is to choose consolidating providers, partners and systems to reduce complexity.

Official institutions globally are seeking benefits from this, which include reducing the costs associated with data and repurposing resources towards core areas of business. But the advantages go beyond savings and efficiencies. Data management has now become a core area of business. It is part of organizations' digital transformation efforts, enabling them to use data across their areas of operation to better serve their stakeholders.

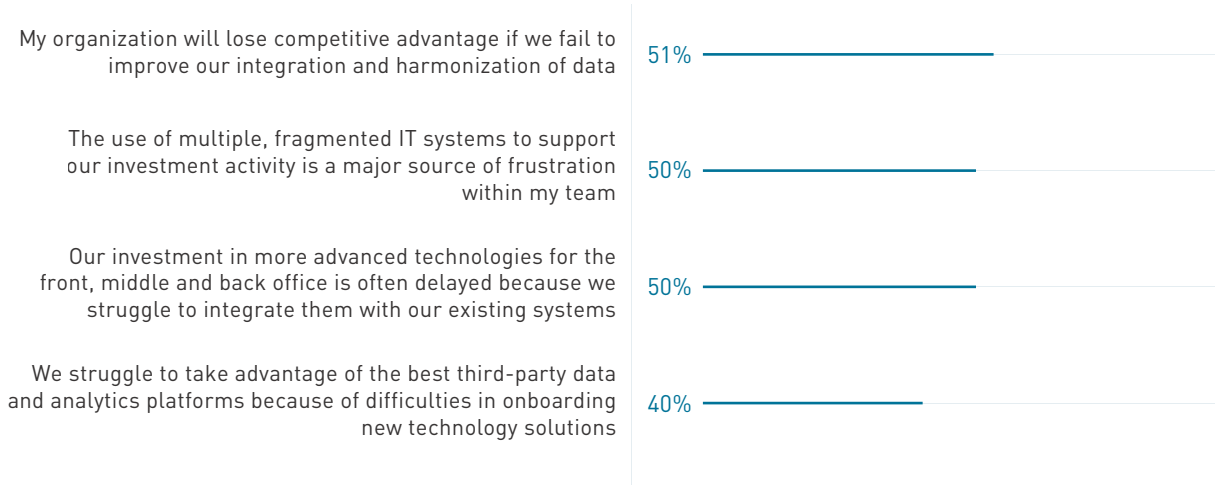
Research shows that institutions increasingly recognize the importance of data to the effective running of their operations. More than half (51 percent) of global respondents to State Street's 2019-20 Growth Readiness Study[1] said, "My organization will lose competitive advantage if it does not improve data integration or harmonization."

However, the challenge with poorly integrated or siloed data is both internal and external. While 50 percent of respondents claimed that multiple or fragmented IT systems to support their investment operations was the major source of their frustration. Other 33 percent said they had difficulty integrating with third-party data systems.

These challenges associated with unsuitable legacy systems and processes are felt across organizations, with 50 percent warning: "Investment in more advanced technology for front, middle and back office is delayed by integrating it with existing systems."

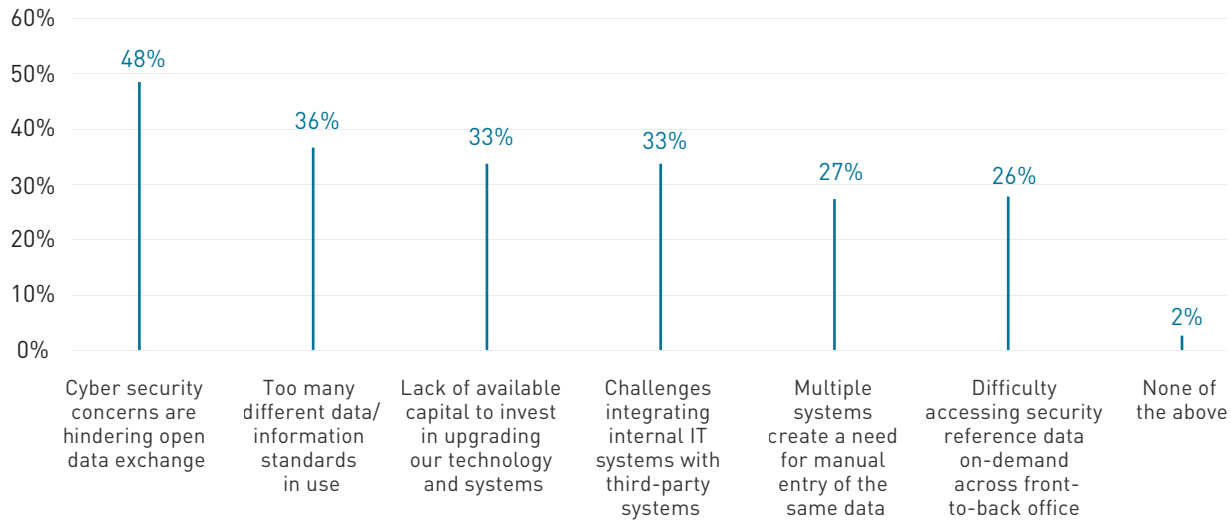
[1] State Street engaged Longitude Research to field a global survey of 523 industry executives from 20 countries, during November and December of 2019. Respondents spanned senior executives in investment, operations, distribution and C-Suite roles, representing institutional asset owners, asset managers and insurance companies.

Figure 1: The Importance of Integrated Data



Source: State Street Growth Readiness Study 2019-20

Figure 2: 'Biggest Barriers' to 'Adopting More Efficient Data Practices'



Source: State Street Growth Readiness Study 2019-20

This has led to a focus on technology investment and partnerships that better enable a holistic view of a firm's internally generated and externally sourced data, as well as an ability for it to be accessible across operational areas in suitable formats for multiple functions.

Cloud technology was the top area of emerging technology investment for respondents, while 39 percent said they have a 'data lake'[2] in place and a further 36 percent are currently migrating to one. However, this process remains nascent, with just 10 percent saying their data lakes were 'enabling new business applications'. The remaining 29 percent of lake users were just using theirs to augment 'existing processes' with 'new analytics'.

The events during the last year, in particular the restraints on investment performance and portfolio liquidity placed on investors by the market crisis generated by COVID-19, have amplified the importance of this trend. The performance and efficiency advantages conferred by data management and analysis-led digital transformation were hit home by the crisis and organizations have responded by increasing their investment in data systems and processes.

In the 2020-21 State Street Growth Readiness Study[3], when asked what had grown in priority as a result of the crisis, respondents cited cyber security (35 percent) and 'risk analytics and scenario analysis tools' (34 percent) as their top choices. 'Liquidity risk management tools' and 'investment analytics tools' (both 28 percent) were also significant increased priorities.

The importance of partnerships to institutions' data ambitions was also highlighted by recent events. The biggest 'positive' for respondents, from the crisis, was the 'knowledge for which we can trust our technology vendors or third-party providers to support spikes in capacity demands'. These relationships are only going to grow in importance as organizations' data needs grow more sophisticated.

Nearly three quarters (74 percent) of respondents said, "The use of alternative data sources[4] in investment analysis has become a bigger priority for my organization as a result of COVID-19." However, a similar number of respondents (70 percent) acknowledged, "We are more likely to use an external provider for alternative data analysis than to build our own in-house infrastructure for this." While 53 percent conceded, "My organization does not have the necessary big data processing and artificial intelligence tools in place to make the best use of alternative data sources."

35%

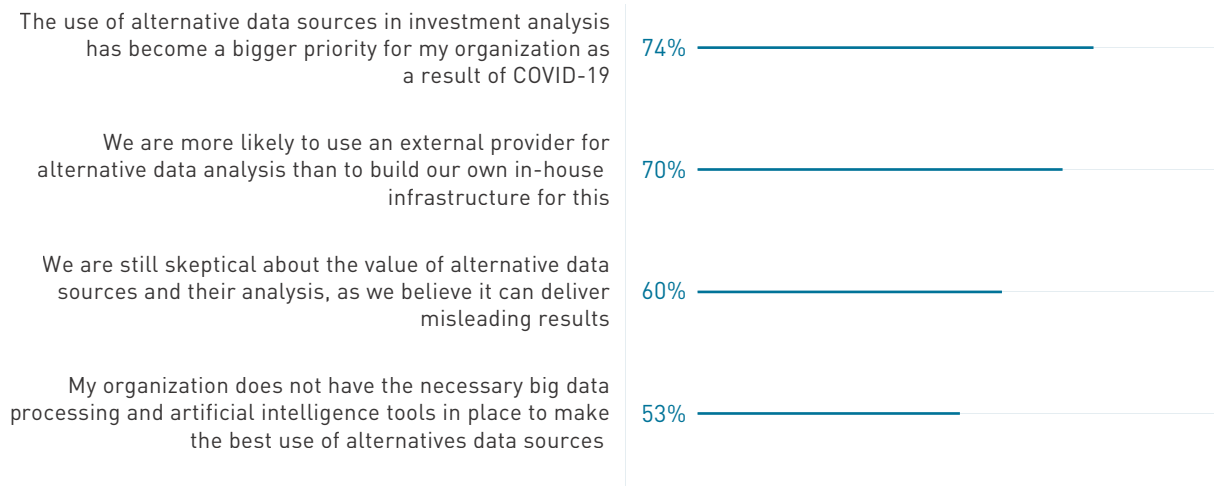
of asset owners cited cyber security as their priority as a result of the COVID-19 pandemic.

[2] A data lake was defined in the survey as: "All data is consolidated into a central data store, where it can be accessed simultaneously and in real-time by many different applications."

[3] State Street engaged Longitude Research to field a global survey of 618 industry executives from more than 20 countries, during September 2020. Respondents spanned senior executives in investment, operations, distribution and C-Suite roles, representing institutional asset owners, asset managers and insurance companies.

[4] Eg., Satellite images, social media posts, foot traffic and transaction data

Figure 3: Plans for Increasing Sources of Data for Investment Management



Source: State Street Growth Readiness Study 2020-21

Cyber security is one of the most consistently important functions of investment institutions' technology investment, according to State Street research.

In addition to the aforementioned data indicating that it was the biggest growing priority for technology investment, post-pandemic, it was also the most important outcome for technology investment in the previous year's survey and second most important in the 2018-19 edition of the study.

The 2020-21 State Street Growth Readiness Study shows that the move to widespread remote working is unlikely to be confined to the immediate circumstances of the crisis. Approximately two thirds (65 percent) of respondents said they expected "all or most" of their employees to continue working from home permanently. As more conversation and information sharing is done remotely, the need for increased attention to cyber security and improved information protection protocols grows.

Operational Risk Consulting Introduction: The Robustness Challenge

Nigel Morriss
Managing Partner,
Operational Risk Consulting

"If you always do what you've always done, you'll always get what you've always got." The grammar is not ideal and the quotation's origins may be contested, but the message is one of timely importance. Whether the statement is accurately ascribed to Twain, Einstein, or Ford, is of little significance compared to the value of its inherent call to periodically re-evaluate and change.

A Shifting Landscape

If the world has learned anything during the COVID-19 pandemic, surely it is that despite humankind's overwhelming achievements and advances, sometimes we have no control over the sheer force of external events. While fundamental, wholesale change to existence may not be required in response to developing situations, 'adaptation' most certainly is.

Organizations must be prepared for change. This includes Sovereign Wealth Funds (SWFs) and other institutional asset allocators.

When developing their operating models, official institutions must accept a fundamental premise that what was fit for purpose in the past may no longer meet the demands of current or future challenges.

The unique complexity faced by official institutions requires heightened diligence when considering whether their operating models sufficiently mitigate the scale and type of challenges faced. The risk universe, fund size and composition, and organizational structures of official institutions starkly differ from those of other asset allocators or investors, requiring a more prudent approach to manage the risks associated with their operating models.

The Operating Model Challenge

Investment operations standards must change periodically to keep pace with developments in portfolio diversification, environmental objectives, infrastructure, service provider consolidation, technological advancement, data needs, emerging risks and regulatory requirements. The key challenges faced by official institutions investors today can be defined within two broad categories: data integrity and systems and cyber security and operational robustness.

Let us consider each of these themes in the context of the Basel Committee on Banking Supervision's definition of operational risk as being the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This time-honored parameter consistently acts as a yardstick by which operating model considerations and their practical implementation should be measured. When reviewing their operating models, official institutions must be mindful of the risks associated with either not changing at all or changing at the wrong pace or in the wrong direction. The good news is, solutions are available and, if carefully planned and applied with robust governance, prevention is certainly better than cure.

Data Integrity and Systems

Official institutions are huge consumers of data – data integrity is paramount for them. Yet data is good only when accurate and has no benefit if incomplete or inaccurate.

Given their scale and complexity, official institutions face several data-related challenges:

Data Aggregation

Official institutions often struggle with multiple data sets from various vendors and sources. Data is often fragmented by asset class or by liquid and illiquid strategies, with some data more readily available and accurate than others. The ability to view accurate, aggregated data has long been an obstacle, with some official institutions having to consolidate data and assemble a top-level view. A single source of trusted data is the target end-state.

Data Management

Given the volume and disparate sets of data official institutions work with, data quality can sometimes be compromised. Official institutions perform a critical overlay role as users of investment-related data and, with the increasing complexities associated with global and regional investments across the spectrum of asset classes, can find themselves acting as data checkers.

Data Locale

Some official institutions require their data to be stored locally. This can limit their access to global data warehousing services and requires them to develop bespoke local data storage solutions.

Investment Systems

Official institutions are major users of powerful in-house investment systems. These are hugely complex, both in how they are implemented and how they run on an ongoing basis. Challenges may arise through incomplete or inappropriate configuration, as well operational knowledge to maintain.

Cyber Security and Operational Robustness

2020 was the year 'operational resilience' became everyday parlance in the investment industry and investment operations teams were placed in the spotlight. The vital role investment operations plays in developing and administering an official institution's operating model as well as the overall success of the organization's objectives, was perhaps better appreciated than ever before. After all, a funds' investments and the return they generate are only as good as the operational infrastructure supporting them.

The added strain placed on operations by the COVID-19 pandemic has also attracted the unwelcome attention of cyber criminals. More broadly, over the last decade, the understanding of cyber security and protection against the threats posed by cybercrime have become common aspects of life. This has made it critical for official institutions to consider the significance of cyber security and operational robustness. The same high standards taken by official institutions to protect against the increasing cyber threat landscape need to be passed on to their third and fourth parties to reduce vulnerabilities in the wider eco-system.

The need for an official institution's operating model to be founded on a framework of appropriate controls and processes, complimented by a system of robust challenge and oversight, is now more imperative than ever. Despite that, investment operations teams grapple with several challenges that test operating model robustness.

Internal Framework

Implementing an agile, robust operating model is a considerable undertaking. True collaboration with third-party vendors yields enhanced results when both parties work in tandem. Challenges may arise; however, when internal frameworks require development or official institutions and service providers are not strategically aligned and have divergent practices, technology platforms or other operating model limitations.

External Relationships

Official institutions require not only technical and data solutions, but also client service, relationship management and counterparty operating models that appropriately support their ever-evolving needs. Of all the institutional investors, official institutions, perhaps need true, strategic partners the most. Their mandates and investment schedules are more prone to change as they must evolve to match policy decisions. With change a constant factor, cracks can occur when service providers and partners do not offer the degree of holistic support required. These can develop into fissures if left unnoticed or unattended.

Partner Oversight

Appropriate monitoring of external vendors is critical to a well-controlled, robust official institution's operating model. Whether it is external investment manager operational due diligence, custodian selection and monitoring or periodic review of key counterparties, an ongoing third-party oversight framework is a critical yet complex constituent of an organization's operating model, and can help protect an official institution from immeasurable risk.

COVID-19 Implications

The global pandemic has challenged conventional ways of working. Though necessary and appropriate, such wholesale changes to client support structures, operating models and day-to-day service delivery frameworks require increased oversight and constant re-evaluation of the emerging risk landscape. The pandemic has affected the entire gamut of the operating models of organizations supporting official institutions. This in turn, has placed huge responsibility on official institutions to understand and manage these external risks, as well as their own internal COVID-19-related risk implications.

A Conversation on Data Integrity and Systems for Investment Institutions

Riccardo Lamanna
Head of Global Exchange,
EMEA, State Street

Stephen Johns
Head of Alpha Data Services,
EMEA, State Street

Nigel Morriss
Managing Partner,
Operational Risk Consulting

James Redgrave
Moderator, Head of EMEA
Insights, State Street

Drivers of Change

James: Let's start by talking about what the main factors are that drive investment in data management and new data operations for investment institutions.

Nigel: When you think about the factors influencing data management, you have to appreciate that the investment world is inherently a different place now to what it was even 5 or 10 years ago. The complexity of investments has increased significantly in line with the changing needs of investors. Official institutions tend to invest across the spectrum of asset classes, resulting in data complexity and the need for accurate information to be able to report on those positions, whether they're liquid or illiquid across their portfolios. In response to that complexity, we see the need for a suitable investment data solution, a system that provides essentially a front-to-back offering across these diverse and complex investment strategies.

Stephen: I echo what Nigel described. A slightly different angle on the same view is that I think we're really seeing that technology and data need to be part of an official institution's competitive edge. Earlier it was, "Do you have great fund managers? Do you have great processes around fund management activity?" However, now very fundamental to that question is technology and access to data, and not just institutional data. It includes market data, index constituents, curves, environmental, social and governance data, etc. You're bringing in new instruments that are very data-hungry to drive the decision process. So, it's where we see technology and then specifically the management of data as a key part of the competitive edge that these investment organizations are looking for.

Riccardo: Data is fundamental for the investment process that we have at the moment, but one thing to really understand is how you get all these data together to make them usable. I would say that there are two very distinct processes when you look at data. One process is to put yourself in the position to manage your investment activity and to collect data in a structured way, with efficient systems and technology. Second, you then generate valuable information that are used for subsequent analysis, for either reporting purposes or to find specific themes that can be part of or affect your investment process. So, there is a cycle. You need to process the data and then enter into the analysis that you need to do, both from an administrative point of view as well as from a value-added point of view. To do all of this, you need new technology, data management and the availability of the data in a system that can host a large quantity of data in an efficient way, i.e. the cloud.

"The complexity of investments has increased significantly in line with the changing needs of investors. Official institutions tend to invest across the spectrum of asset classes, resulting in data complexity..."

— NIGEL MORRISS

Data Systems and Infrastructure

James: So, data is becoming increasingly important across a very wide variety of business areas. But, I also hear that data systems must be interoperable: data is being used by multiple functions within an organization as well as inputted into systems run by third parties, coming from a variety of sources. What is it that investment institutions are doing, both in terms of reorganizing their own internal operations and systems, and also in terms of working with partners and other organizations, to get the benefits of this more efficient and widespread use of data?

Stephen: There's been a very distinct evolution in the industry. Nothing's fundamentally changed in the importance of data. Data has always needed to be accurate and timely, but what we have seen is the subsequent development of the relevant investment technologies. Official institutions have moved from needing to place reliance on a single point of data to needing aggregated data. Multiple financial services need to utilize golden sources of data to ensure lineage and data flow through a connected eco-system is hydrated and accurate. This needs to be the flow from the front office and the investment decisions through the middle office investment accounting and to the fund accounting in the back office, and all other services that need to hang of this cyclical flow.

The investment and technology industries have developed and changed over the last few years. The introduction of fintech has added to the changes. I see a clear drive for official institutions to harmonize the information they receive, to look to one golden source of data they can use to make critical strategic investment decisions. There's also been a clear realization among official institutions that the power of the systems that they have internally and the data that they are consumers of is imperative.

Riccardo: With technology and infrastructure, data is key, but we first need to ingest, clean, make them transparent for official institutions and for their applications to consume. Similarly, we need to let third-parties' applications and services enrich and consume data. The key is to create an open and interoperable platform, where different parties (service providers, fintech, software providers) can link to, to deliver additional information and insights. At State Street, we have developed and implemented this platform to provide front-, middle- and back-office functions, in an open and interoperable manner. Other providers can access it and integrate with it to provide added value to their clients.

Nigel: I think it's clear that we're now in a period of harmonization. There's been a fundamental shift from a 'them and us' approach, where different entities were vying for opportunities to be the data owner. Now, with this complete holistic architecture that we are describing, with these advances in technology, we can provide and facilitate interoperability. It's what many investors have been looking for, because it facilitates that complementary set of benefits between the resources of global corporates with established and powerful platforms and smaller entities, like fintech and other data providers, that are able to connect into that architecture.

New Technology

James: Now, all of you have touched on technology and its role in driving some of these improvements in data management and use of data. Perhaps we could go into a little bit more detail about the types of new and emerging technology, which are making a difference here. Things like artificial intelligence (AI) and cloud. How are those things improving – and how are they set to continue to improve – the data landscape for institutions?

Stephen: I think a combination of technology evolutions is taking place. On the one hand, there are emerging fintech players and on the other, there are large, established players. Then there's collaboration between those two categories. You look at Amazon and Microsoft and there is your cloud capability. There's a huge progress with cloud and the speed with which you can establish some of the services and connectivity to drive architecture change.

One comment specific to official institutions: traditionally, some SWFs have been reticent to use cloud-enabled services. They want to have the data directly in their architecture, to have a box and that box needs to run in their data center where they can see it and control it. There's now an acceptance that this isn't the route they will necessarily take as it is not as secure as a provider that's doing this very carefully and putting a lot of time and effort into the security around it.

Then I think, there are other technology advances that allow the normalization and the aggregation of data, where you've got emerging technologies coming very quickly and giving a very powerful offering. Snowflake, for example, is enabling a next step in data sharing. There's a lot of scope for different types of technology organizations to provide offerings such as data dictionaries, lineage tooling and data catalogues. This is critical to the service in which a client and then a provider can deliver an interactive data service where the client still has full visibility of their data assets and feels in control. For example, take a piece of data that's appearing in an online factsheet. You can see and make sure it's the piece of data you wanted to use. You see that data journey all the way through the data flows, through the investment process, all the way to appearing in a factsheet. So, it's very exciting at the moment to see what's going on around the technologies available to help these kind of data services we're talking about and how State Street is building technology ecosystems to deliver data services upon.

Riccardo: The technologies, either already available or being developed, must satisfy three requirements: integration, integrity and intelligence. We need to integrate the data and that is what we are doing with sophisticated data management services and structures. We maintain the integrity and security of information using cloud technology. We should underestimate that the amount of data that we collect and store now is much higher than it was only 5 or 10 years ago. For example, State Street, as a security services provider, receives transaction records from clients which may be 50 to 60 data elements long. What we used to do in the past was to cut out everything

that we didn't need to perform the function that we were paid for like matching, settling and booking the transaction. What we do now, which is the real value of the new technology, is store all data elements and classify them intelligently to make them consumable. The cost of the storage of the data is not as expensive as it was before. So, we store this massive amount of information and secure in the cloud to let artificial intelligence and analytics, which is the third 'I', do their job efficiently. This is made available if you have good integration and storage.

Nigel: I think this is a brilliant way to articulate an approach to data – this journey of integration, integrity and intelligence. In any entity that owns the assets, operations is the gatekeeper of data.

They must ensure all data, which come from custodians, fund administrators and a myriad of different entities, is absolutely accurate before it is passed on to the investment team. Of course, this is the role of each provider, but the asset owner's operations team must still act as an overlay before passing on this information to the investment team. The investment team needs to act on it promptly and make some potentially significant investment decisions off the back of the data that it receives. When so many data sets are being consumed and aggregated, those enhancement processes and protocols are of critical need. Think of the nature of these asset owners that we're talking about here. They, like many institutions in the world, are responding to a set of challenges such as the world has never seen before. Strategic decisions of huge importance need to be made daily. As the evolution rate is fast within these organizations, they need to be able to move quickly. Therefore, it becomes imperative that they have access to quality data.

James: Regarding the rate of evolution in this area and how quickly institutions are changing as the circumstances around them and the technology changes, what's going to develop in the relationship between the institution and the provider? What do you see the future looking like compared to the point to which it's evolved today?

Nigel: I think we must start with the premise that if we build today, we have to build for the future. Build the house today that you need for today but allow for extensions to be added to grow the property. When we've talked about fundamental shifts in people's thinking in this area, it isn't just thinking about their relationship with custodians and fund administrators. It's clear to me that as prescient, highly sophisticated investors, official institutions are looking to continue to work with all these parties, but also to harmonize those relationships when it comes to data. Several entities have asked me how they can utilize AI and there are many different levels of complexity to where and how it could be harnessed in financial services. Investors are willing to engage in those conversations about how they can be educated about it. I would also say that core data and system offerings that are already available were developed hand-in-hand with major clients. Take them on the journey when planning for the future. Don't try to go off and do it independently. Open up a critical dialogue between data users and consumers.

Stephen: I agree. For example, we've worked with a SWF over the last couple of years that had their books of business separated across four providers. They were all running custodian and fund accounting processes, so that their assets were separated. That was good for them in the past. Those providers have a rich relationship that's not going to necessarily change, but they now need to pull that data together. It's no longer acceptable to that organization to have four separate books of business. This is where the data service comes in. We can stitch it all together. So, that's a step that we see becoming a reality. Some of the things we've already talked about are automatic checks of data through its lifecycle. I think we're going to see that shift into AI. Now, can we have some of the platforms themselves flagging insight rather than having lots of human intervention? I think this foundation of the data architecture – standardization and aggregation – is now going to be the platform that AI and insights can really grow upon.

Riccardo: I think it's very important to understand that we use AI on a day-to-day basis in our processing. We collect data, transform it into usable information and through the use of AI, we anticipate issues. We can see when trades are not being matched properly and we try to anticipate an issue with certain securities depository or a certain broker. This helps our clients with liquidity management. One other way in which a provider like us is using AI is in trend analysis based on data we collect while providing our services to identify macro trends and provide valuable information to our clients. Clients want us to take risks, to make investments, to consider their needs and integrate them in our systems and offering. When something really special comes out, we develop it with the client and take it as an opportunity to create a solution that could be made widely available. This has proven to be more powerful than single way development.

Stephen: Technology and business knowledge are really coming together. We have data scientists, data architects, but they really have to understand the clients, the financial processes that they're dealing with and that's something that I've seen develop in recent years.

"I think this foundation of the data architecture – standardization and aggregation – is now going to be the platform that AI and insights can really grow upon."

— STEPHEN JOHNS

A Conversation on Cyber Security and Operational Resilience

Dan Money
Head of Operational Resiliency,
EMEA, State Street

Neill Newman
Head of Information Security,
EMEA, State Street

Nigel Morriss
Managing Partner,
Operational Risk Consulting

James Redgrave
Moderator, Head of EMEA
Insights, State Street

Resilience Best Practices

James: I'd like to talk about resilience and best practices for setting up a resilient set of operations. What to do at the very beginning to make the best possible start, in operational resilience with a particular focus on technology and cyber?

Dan: The first key element of resilience is identifying your critical business services. That can be areas that hit market stability or firm viability or the consumers. The second aspect is to map that end-to-end and identify what your key dependencies are. What are you dependent on to deliver those services? Third, you can then set metrics or tolerances in terms of disruption to those services. Fourth, you need to develop some way to measure them in real time and assess any forward-looking impacts that are coming up. The fifth element is to test it, either through scenarios or through looking at incidents that you've seen.

Neill: From a cyber perspective, Dan mentioned understanding what your critical services are and that means understanding the people and process elements – the technology element is not just about technology. Forgetting people or process and their resiliency can be a detriment if you are trying to recover in a certain situation. The other piece is about how you recover. It's also important to have an understanding of what you would do when it goes wrong and how you respond to recover those services back to deliver to the clients or to the regulators.

Nigel: You also need to think about robustness. When we talk about robustness, we mean how models need to be built and whether you've got something that's been carefully designed and implemented with resilience in mind. When there is an event and resilience is required, you can bounce back – ensuring you bounce in the right direction. We have to go back to the basics and just like building a house, the foundations need to be strong. Also, all other elements of the build, which are integral to the overall integrity of the structure, are critical. I think the Basel Banking Commission gave the simplest definition of operational risk. It's fundamentally building to protect against the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events. It really does cover such a vast area of considerations.

Dan: It's a great point about the robustness and the foundational elements. Are we set up in the right way? Or have we built things piecemeal when we needed to look at it end-to-end, holistically and from an efficiency perspective? I think sometimes people look at how we need to do it from a regulatory perspective, but we also need a best practice perspective. It's also going to give you some good business outcomes from putting that lens on it.

Neill: Yes, this isn't a one-time exercise, it's continuous. While you can design, plan and be ready for certain events, there are other things that are happening inside an organization. Organizational change, structural changes, business strategy changes that lead to changes in your resilience. So, while you can design something at the start that is resilient, over time the natural changes in an organization can make those systems less resilient.

Nigel: There is no one-size-fits-all. There are some gold standards but what one has to do with a best practice standard is take it in the relevant circumstances to which it needs to be applied. As long as there's no compromise to the black and white rules, it needs to be applied specifically to the task at hand – to the financial institution, to the client, to the investor that you're working with and to the jurisdiction that they're in. With operating models and their robustness, there's nothing that should be static. Technology changes at a rapid pace. Data systems change. Regulation has taken on an entirely new meaning in everybody's lives. As an example, a few years ago many board members wouldn't have known the real implications of cyber security. Now this is a board-level discussion where risk management and many areas of business must be involved to ensure appropriate ongoing resiliency. Perhaps that's because the threats to organizations – financial and non-financial – have grown to where there are not just criminal enterprises but state actors.

Monitoring Resilience and Recovery

James: I want to move on to this idea of an ongoing process. Once you have your best practice standards in place, you have to ensure that you maintain them. What are the best ways of doing this?

Neill: From a cyber perspective, it's about understanding what you have and spending time looking into those processes. Have you got a continuous measurement and how well is it doing? It may be that a particular service line is more important than another one. So how do you get visibility and how do you measure to make sure that you're delivering what is expected by the customers, in some cases regulators, and ultimately for the value of the shareholders? How do you ensure continuous improvement – updating the organizational changes or threats that you face in each one of those areas.

The other element to overlay onto that is governance. It's all well and good asking the IT guys, "Are the systems okay?" They say, "Yes, they're all good." But how are you overseeing that? How are you challenging that? How do you know you're getting the correct information? So, there's a process of validation and challenge that is also required.

Nigel: Go deep is what I would say. I understand the risk landscape that an organization may be exposed to and how it can manage that risk. We have to understand that risk is inherent. It's there in the financial organizations that we work and deal with. So, to be able to truly identify the risk landscape and manage it on an ongoing basis, you have to go end-to-end across the organization and beyond, depending on third parties. We look at investment structures or those frameworks that are in place to support investment structures: custody; compliance frameworks; risk management; audit functions; investment controls or investment support controls that support the lifecycle of assets and asset administration; data continuity frameworks; and then third-party management.

James: What does an organization need to have in place in terms of recovery when something happens that really puts pressure on their operations and systems, to the point of failure?

Neill: There are many things that will be thrown at you that you have not considered for whatever reason, whether that's through lack of planning or an abnormal event that nobody has considered before. In those situations, what you need is clear communications with the right people and they can vary. It obviously will include senior management, but it could include your legal teams, external communications teams, IT, or business operations. It's choosing the right people at the right time to bring into those conversations. The second thing is not panicking and logically understanding what has happened. In that information void during a particular event, you can actually make what seemed to be good decisions but turn out to be drastically bad decisions. Then, of course, after the event, learning from it.

Nigel: We've talked about things going wrong, but I always like to call out the near misses too. In the operational risk management frameworks that Dan has mentioned a near miss is often the same as an actual error or loss event – you're just lucky that it didn't transpire. We have to treat it the same because there was a control failure. Therefore, we promote straight-through processing automation. We get very nervous when things slide out into the manual realm. But when they do, you need a framework of appropriate signatories signing off something that can be supported consistently in an error-free way. The right controls and ongoing oversight must be put in place to support that. Plan it with the people in mind because it's people who are chosen specifically based on their deep experience and their knowledge.

Dan: The other thing that we focus on in incident management is to try keeping things to a standard and try not to do too many ad hoc things, because that's when you're introducing risk. Try and maintain standard processing, standard procedures, standard controls as far as possible so that you're not introducing new risk into what is already probably an out of the ordinary incident.

Technology Enhancing Resilience

James: We've talked about the potential for risk that cyber introduces into the resilience sphere. I'd like to talk a little bit about how technology can create opportunities to generate better resilience and due diligence. Both internally and in terms of your external relationships, how can technology better promote the practices we've been discussing?

Neill: One area that is incredibly important as you get into the technology space is standardization. If you have a technology footprint or an operational footprint that is complex, that is messy, that is non-standard, then quite clearly, the complexity of that will lead to more failures and therefore a less resilient system. So, understanding what you have, simplicity and standardization are the ultimate aims. It's difficult to achieve that, but the more you can do to standardize your technology and your operations, the easier it is to understand when something is wrong.

Dan: We have built a tool that helps us with process mapping and looking to link together taxonomies because all the information is already there, but can you identify the key repositories of your dependencies or third parties, people or locations? If you can use technology to link those together and allow you to analyze them from an ongoing vulnerability point of view, then that can be a very powerful tool.

Neill: It also helps bridge the gap between what has culturally and historically been the divide between business operations and technology. Business operations understand the business process. The technologists understand the nuts and bolts. But it's where they interface and what the implications are for each other, that it can become blurred. If you have that end-to-end process map for operations – the systems that they're operating on, the technologies that they're operating on, the physical location of those pieces of infrastructure, the servers, the networks, firewalls, etc. You can then truly understand the risk that you are managing and that's the ultimate goal.

Nigel: There's a growing theme here of regulatory concern around organizations understanding the risk that their third parties are exposed to and information technology risk. I think we'll begin to see growing momentum from the regulators in ensuring that we look at the technology space, because it does promote resiliency. You can't afford to have interruption to business as usual. You need those prices. You need those data feeds. You need that cleaning and cleansing tool facility. You need to be able to aggregate that data. I think technology can and does provide opportunities and it does promote resiliency, but it all goes back to understanding. Do you truly have a clear line of sight into what the underlying processes and controls are that your third parties have?

Neill: That kind of assessment comes back to how risk averse you are in your diligence. If you go that extra step, your third parties typically rely on another third party; a fourth party. Do you go the extra mile with the fourth party and if that fourth party is relying on a fifth party, and so on? You can quite clearly see the sprawl that would create and the complexity that is probably too difficult a problem for any one organization to objectively measure. There's a level of pragmatism that has to be taken into account because, while in an ideal world you would understand everything, the practicalities mean that you can't. It's about understanding where that line is and making the right decision.

Third Parties and Due Diligence

James: That brings us on to third parties. Presumably, you need an ability to do due diligence on your third parties' due diligence. You obviously can't check all their suppliers and providers, but you can check the systems that they have in place to check them. It's like a hall of mirrors, from one position you can see all the way down.

Dan: Exactly. Your due diligence on them – a key aspect of it – is how do they conduct due diligence over their key suppliers? Have they identified their key suppliers? What checks are they doing over that chain of outsourcing elements that you invariably see in operating models today?

Neill: You can split operational risk of resilience into two camps. One is the areas where the variables are controllable. For example, with an interest rate fluctuation, you know what the interest rate is going to vary between two fixed things whether that's zero to negative, whether it's positive, depending on what the economic circumstances are. But it's a very – I hesitate to use the word simple – but it's a controlled situation where the variables are minimal. If you then move into a lot of IT risk the number of variables involved are significant and sometimes almost impossible to quantify. Therefore, in the first situation where you've got a bounded problem, you can usually get to a robust answer within a degree of accuracy. When you get to some elements of cyber security and IT security and operations, the variables are so vast, it's very difficult to actually pinpoint that, 'This is the risk.' You can measure the impact of a cyber event, for example. But calculating the likelihood of those situations occurring is difficult. So those organizations that treat cyber risk as something we are absolutely able to quantify 100 percent in order to make decisions on resiliency and so forth start to fall apart when you start talking about the likelihood of these events occurring. I think there's an evolution or a maturity that needs to occur that understands and respects the complexity. It is not an excuse; it's just the nature of the problems are different in the cyber world.

Dan: Certainly, the view of some of regulators is they're now saying they want you to assume failure of key dependencies and then analyze what that would mean to you. I think that it's a move from the likelihood question to, 'Things will go wrong and often beyond your control.' If they go wrong, how will you deal with that? In our scenario testing that we're doing now, we stopped trying to build scenarios. We just say this has failed. It's failed for these many days. How would you deal with that? It takes that likelihood element away from it in terms of your testing of your key dependencies.

"I think there's an evolution or a maturity that needs to occur that understands and respects the complexity. It is not an excuse; it's just the nature of the problems are different in the cyber world."

— NEILL NEWMAN

About State Street

State Street Corporation is one of the world's leading providers of financial services to institutional investors including investment servicing, investment management and investment research and trading. State Street partners with official institutions, sovereign wealth funds, central banks and other official institutions globally to help address their biggest challenges.

About Operational Risk Consulting

Operational Risk Consulting or 'ORC' is a UK-based specialist risk management advisory firm, which advises institutional asset owners on managing the operational risks associated with investing. ORC's key objective is to help raise investment operations standards.

For more information, visit:

statestreet.com/ideas

STATE STREET.

State Street Corporation
One Lincoln Street, Boston, MA 02111

www.statestreet.com

Disclaimer

The material presented herein is for informational purposes only. The views expressed herein are subject to change based on market and other conditions and factors. The opinions expressed herein reflect general perspectives and information and are not tailored to specific requirements, circumstances and/or investment philosophies. The information presented herein does not take into account any particular investment objectives, strategies, tax status or investment horizon. It does not constitute investment research or investment, legal, or tax advice and it should not be relied on as such. It should not be considered an offer or solicitation to buy or sell any product, service, investment, security or financial instrument or to pursue any trading or investment strategy. It does not constitute any binding contractual arrangement or commitment of any kind. State Street is not, by virtue of providing the material presented herein or otherwise, undertaking to manage money or act as your fiduciary.

You acknowledge and agree that the material presented herein is not intended to and does not, and shall not, serve as the primary basis for any investment decisions. You should evaluate and assess this material independently in light of those circumstances. We encourage you to consult your tax or financial advisor.

All material, including information from or attributed to State Street, has been obtained from sources believed to be reliable, but its accuracy is not guaranteed and State Street does not assume any responsibility for its accuracy, efficacy or use. Any information provided herein and obtained by State Street from third parties has not been reviewed for accuracy. In addition, forecasts, projections, or other forward-looking statements or information, whether by State Street or third parties, are not guarantees of future results or future performance, are inherently uncertain, are based on assumptions that, at the time, are difficult to predict, and involve a number of risks and uncertainties. Actual outcomes and results may differ materially from what is expressed herein. The information presented herein may or may not produce results beneficial to you. State Street does not undertake and is under no obligation to update or keep current the information or opinions contained in this communication.

To the fullest extent permitted by law, this information is provided "as-is" at your sole risk and neither State Street nor any of its affiliates or third party providers makes any guarantee, representation, or warranty of any kind regarding such information, including, without limitation, any representation that any investment, security or other property is suitable for you or for others or that any materials presented herein will achieve the results intended. State Street and its affiliates and third party providers disclaim any warranty and all liability, whether arising in contract, tort or otherwise, for any losses, liabilities, damages, expenses or costs, either direct, indirect, consequential, special or punitive, arising from or in connection with your access to and/or use of the information herein. Neither State Street nor any of its affiliates or third party providers shall have any liability, monetary or otherwise, to you or any other person or entity in the event the information presented herein produces incorrect, invalid or detrimental results.

No permission is granted to reprint, sell, copy, distribute, or modify any material herein, in any form or by any means without the prior written consent of
State Street.

3545351.1.1.EMEA.INST Expiration date: April 30, 2022