THE INVESTMENT ASSOCIATION

OPERATIONAL RESILIENCE

Business Services & Beyond

December 2019

ABOUT THE IA

The Investment Association is the trade body that represents UK investment managers, whose 250 members collectively manage over £7.7 trillion on behalf of clients.

Our purpose is to ensure investment managers are in the best possible position to:

- Build people's resilience to financial adversity
- Help people achieve their financial aspirations
- Enable people to maintain a decent standard of living as they grow older
- Contribute to economic growth through the efficient allocation of capital

Our members help to grow people's savings in a wide range of ways, including through authorised investment funds (schemes where several investors 'pool' their assets and invest in a professionally managed portfolio), pension funds, and stocks & shares ISAs. The UK is the second largest investment management centre in the world and manages over a third (37%) of investments across Europe.

Investment Association (IA) members hold in total over one third (35%) of the value of UK publicly listed companies. We use this collective voice to influence company behaviour and hold businesses to account.

More information can be found at **www.theia.org**

FOREWORD

OPERATIONAL RESILIENCE IS A MAJOR FOCUS WITHIN THE INDUSTRY AT PRESENT AND WILL CONTINUE TO DEFINE OPERATIONAL RISK AND BUSINESS CONTINUITY AGENDAS. THERE HAS BEEN A MARKED REGULATORY SHIFT FROM TRADITIONAL RISK MANAGEMENT AND BUSINESS CONTINUITY PRACTICES TO ENHANCED BUSINESS RESILIENCE. THE COMPETITIVE ADVANTAGE TO INDIVIDUAL FIRMS OF BEING OPERATIONALLY RESILIENT AND THE KEY ROLE IT PLAYS IN THE WIDER MARKET'S OVERALL FINANCIAL STABILITY CANNOT BE OVERESTIMATED.

This publication contains the conclusion of our work on Business Services. The IA convened a Working Group of more than twenty firms on the topic which worked over the last few months with Baringa Partners LLP to help investment management firms in the process of defining their important business services. This is a critical first step on the road to achieving compliance with evolving regulatory expectations on Operational Resilience and enables firms to look in more depth at the dependencies on people, facilities, IT and outsourcers, and then at setting appropriate impact tolerances.

There is a clear benefit for firms to understand what their important services are and look to improve their efficiency and customer outcomes, as well as being compliant with the regulations. Over time, with increased levels of outsourcing, automation and offshoring, firms and even front-line staff may have lost contact with the knowledge of exactly how their functions are delivered. Operational Resilience can help with this by clearly documenting process flows and dependencies.

We are seeing regulators across the globe moving in a similar direction to the UK, which provides an opportunity for staff in multi-national firms. There have been regulatory developments on similar themes in the US, Singapore, European Union and Australia recently.

However, as a relatively new concept overall, firms will need to build out their capabilities by identifying the new skills that will be required and investing in their staff.

The IA has recently published its Talent Strategy to support members to attract, develop and retain a high quality workforce fit to respond to the changing world of work and the working environment. Investment20/20, our industry careers service focused on diversifying the talent that joins our industry, provides access to graduates and school leavers to fill the new roles that will be created.

We will soon publish our work plan on Operational Resilience, a guide to how the IA is supporting its members through policy work, events and training.

The IA is committed to supporting its members through this process and engaging with the regulators to ensure that the prescribed obligations are proportionate and appropriate to the investment management industry.

Stay up to date with our activity via
www.theia.org/operational-resilience

Pauline Hawkes-Bunyan
Director, Business: Risk, Culture & Resilience

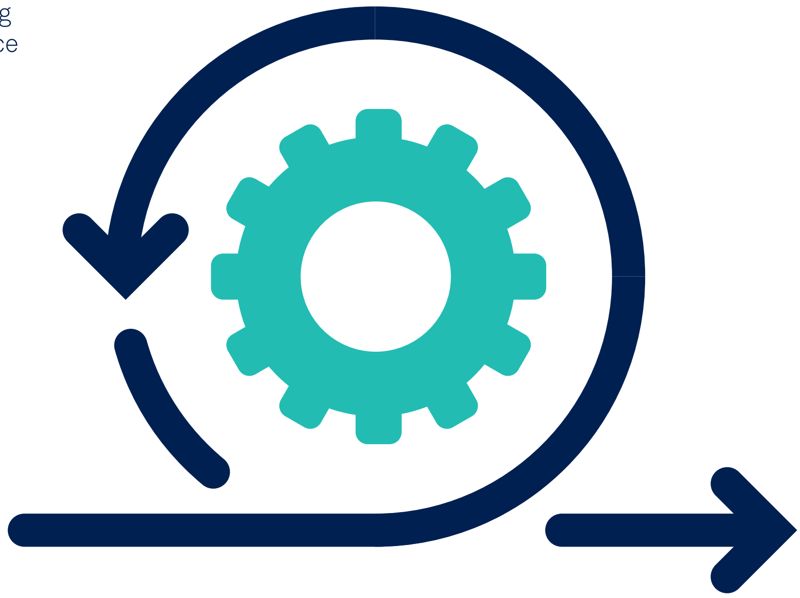
BACKGROUND

THE LEGACY OF THE FINANCIAL CRISIS ALONG WITH HIGH PROFILE INCIDENTS IN OTHER SECTORS AND THE GROWING RELIANCE ON TECHNOLOGY WITHIN FINANCIAL SERVICES HAVE PLACED OPERATIONAL RESILIENCE HIGH ON THE REGULATORY AGENDA. AT THE HEART OF OPERATIONAL RESILIENCE IS A FOCUS ON PROTECTING CONSUMERS AND RESTORING TRUST IN THE INDUSTRY.

In the 2018 Discussion Paper, the regulators highlighted the need for a step-change in operational risk management across financial services and detailed key principles firms should follow when building Operational Resilience:

- Firms should aim to minimise customer harm in the event of operational disruption. A customer focussed culture should be embedded across firms and be led by Boards and Senior Managers.
- A business service is defined as a product or service that a firm or financial market infrastructure (FMI) provides to its customers. Firms will need to define their most important business services which will vary by firm or FMI.
- Once business services have been identified, mapping the service end-to-end will help firms to understand the full value chain, including services provided by third parties and identify potential single points of failure. This will support firms identifying potential points of failure and taking appropriate measures to ensure that the service can still be delivered through quick recovery or substitutability.
- Impact tolerances describe firms' and FMIs' tolerance for disruption, under the assumption that disruption to a particular business service will occur. Impact tolerance is expressed by reference to specific outcomes and metrics. Such metrics could include the maximum tolerable duration or volume of disruption, the criticality of ensuring data integrity or the number of customers affected. Impact tolerances are different from risk appetite, in the sense that they assume a particular risk has crystallised, but they will inform the risk appetite of a firm or FMI's Board and Senior Management.
- Firms need to be able to demonstrate their resilience by testing the effectiveness of incident response plans by exercising operational disruption outage scenarios. Firms should then use lessons learned from these exercises to build upon incident response plans and inform future resilience control measures.

Rather than being a regulatory tick-box exercise, ensuring effective Operational Resilience is to the benefit of firms, enabling them to make improved, informed, investment decisions, better prepare for change and adapt quickly in the face of disruption. The regulators will be looking to see that firms embrace this approach throughout their supervisory activities.



REGULATORY PRIORITIES

In 2018, the Bank of England, PRA and FCA published a joint Discussion Paper, 'Building the UK Financial Sector's Operational Resilience'.

The Discussion Paper outlines that **operational disruptions have the potential to harm customers and market participants, threaten firm viability and cause instability in the financial system**. As such, there is a need for firms to become operationally resilient.

To safeguard against operational disruptions, the message from the regulators is that firms must prepare for the inevitability of a disruption.

The key regulatory priority is mitigating the impact of disruptions on consumers through:

- Effective Board oversight
  - Recognise the importance of elevating Operational Resilience to a position of high priority on the Boards' agenda;
  - Provide all Boards with appropriate training to enable fully informed decision making;
  - Create an appropriate governance structure so that Operational Resilience controls and decisions are effectively challenged across the three lines of defence;
  - Assign relevant responsibility and accountability to senior manager(s) and ensure there is widespread awareness of individual responsibilities;
  - Establish an unambiguous chain of command.
- Business services continuity planning
  - Marked shift from preserving the interests of shareholders to an emphasis on mitigating the impact of disruption on consumers;
  - In particular, being able to continue delivering important business services to customers e.g. ensuring continuation of core investment operations;
  - The resilience of underlying systems and processes should still be considered and their role in the delivery of important services should be mapped in order to prepare appropriate substitutes and/or recovery methods.
- Setting impact tolerances
  - Prepare for disruption to key business services by assessing the maximum tolerable limit a firm can withstand;
  - Each service should have a set impact tolerance and necessary recovery time. The firm should determine these themselves and be able to explain to the regulator the process behind determining each impact tolerance.
- Understanding of supply chains and outsourcing arrangements
  - Clear understanding of key business services, people, systems;
  - In particular Boards and Senior Managers need to identify any reliance on critical third party service providers and have measures in place to ensure the continuation of important business services in the event of an outage;
  - Where possible firms should engage with third parties, especially unregulated third parties, to ensure that they are familiar with the firms' expectations and that their resilience approaches are aligned.
- Embedding a resilience culture
  - Recognising operational disruptions are a question of 'when' rather than 'if' helps firms become better prepared and ensuring that everyone across the business knows this and that they play a key role;
  - Embedding a culture of resilience will encourage continuous improvement.
- Effective and timely communications
  - Internal and external plans in place.

DEFINING AND MAPPING BUSINESS SERVICES

Business services, and in particular, ensuring that firms continue to provide the most important business services to customers in the face of disruption, is a key regulatory focus.

"THE SUPERVISORY AUTHORITIES BELIEVE THAT AN OPERATIONALLY RESILIENT FIRM OR FMI WOULD HAVE IN PLACE: A CLEAR UNDERSTANDING OF THEIR MOST IMPORTANT BUSINESS SERVICE OR SERVICES; A COMPREHENSIVE UNDERSTANDING AND MAPPING OF THE SYSTEMS AND PROCESSES THAT SUPPORT THESE BUSINESS SERVICES, INCLUDING THOSE OVER WHICH THE FIRM OR FMI MAY NOT HAVE DIRECT CONTROL."

Joint FCA, Bank of England and PRA Discussion Paper

In response, the IA created the Operational Resilience: Business Services Working Group, focussing on member priorities. This Working Group has sought to provide clarity and guidance on identifying and mapping important business services, which are both areas expected to be part of the FCA's Operational Resilience regulations.

Defining the 'most important' business services

A fictional firm, aiming to be broadly representative of members' business models, was created to help the group walk through the identification process. The high-level functions of the firm were first identified. They represented a collection of services, and were not distinct in their own right.

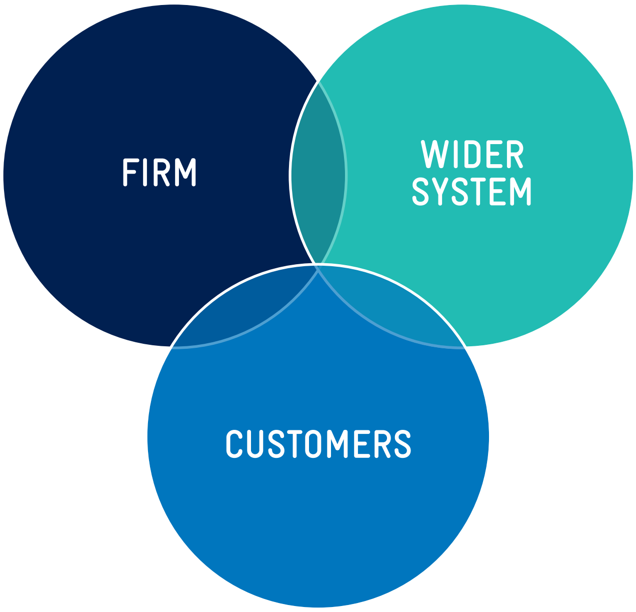
The sample overarching services identified (investments, payments in/out, valuation, custody and client and regulatory communications) were deemed to be the fundamental functions underpinning the delivery of investment services to the end consumer whether that is a retail or institutional client.

An additional collection of services, which we identified as 'Internal Support Services', was also included, even though it didn't provide any customer-facing output because it underpinned the delivery of a number of other services, such as Human Resources, the Technology Management capability, Treasury, Corporate Security etc, and was therefore critical to the firm's operations.

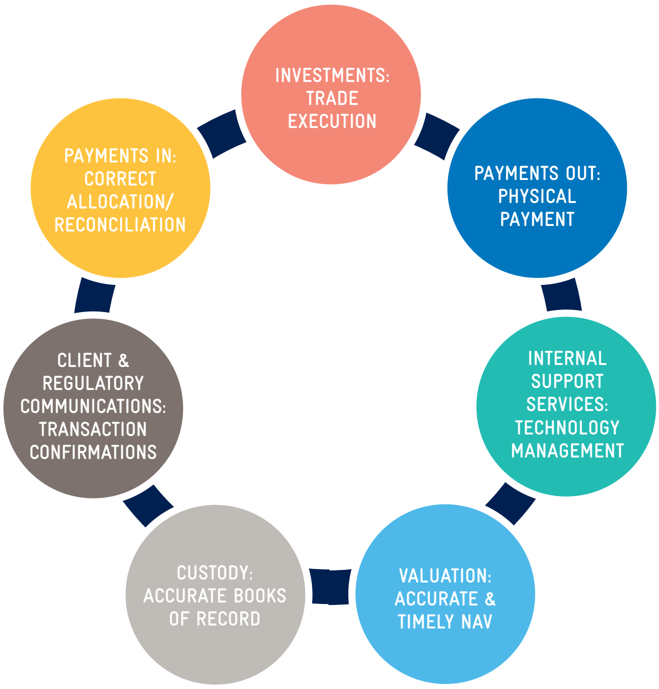
These seven high-level services were then individually assessed and broken down into lower-level services. For example, Payments Out was broken down into four distinct services:

- Physical payment
- Liquidity & ability to realise value from assets
- Access to payment systems
- Appropriate referencing/other explanatory output to recipient

Out of this group, the most important business service was selected using a scoring criteria of the impact on the customer, firm and threat to wider market/financial stability, should that service be disrupted.



Those that met this criteria were the following, which the fictional firm then adopted as its seven most important business services:



It is important to be aware that there may be more than one important service involved in the delivery of the overall function, but for the purposes of this fictional firm we have only selected one.

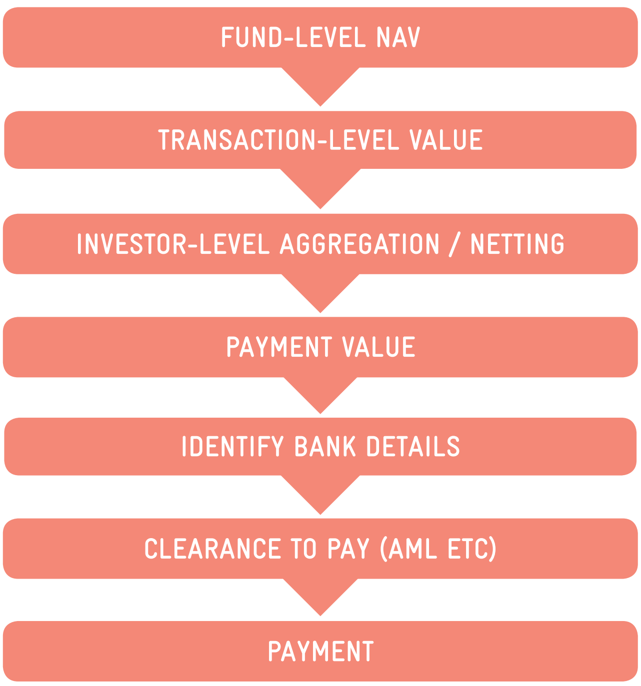
An in-depth overview is available on the Operational Resilience Expert Page of the IA website **www.theia.org/campaigns/operational-resilience**

Mapping business services

Once the key business services had been identified, by taking an end-product perspective the systems and processes involved in delivering this service could be mapped. The approach taken was to:

- Identify main systems and processes involved in contributing the output and any underlying dependencies
- Identify what is critical to the continuing delivery of the service
- Maintain awareness of third parties involved in the value chain and any interdependencies
- Understand the services and underlying systems needed to keep the business running on a day to day basis and therefore deliver the entire important service
  - Understand the digital dependencies involved in delivering a business service for instance internet connectivity and IT systems
- Identify single points of failure across services such as underlying IT software
- Maintain a holistic perspective to ensure the end-to-end provision of the services critical to the firm and its customers are accounted for

Using the Payments Out example again, the process flow was identified as



The dependencies and underlying functions were identified as

- **IT systems** of the Accounting book of record, the Transfer Agent and the potential payment platforms and banking providers
- **Outsourcers** of Custody, Accounting, Transfer Agency
- **Facilities** across the globe of these entities and internal departments
- **People** and staff of the sub-teams within these departments

Now that the firm had identified its important services, replicated the above end-to-end mapping process for each of them and understood the dependencies at every stage, the firm was in the position of understanding its business service provision from the end consumer's perspective.

We used the example of a fictional firm in order to facilitate discussion in the group, break down the differences in operating models and explore the area with relatable examples.

Firms should replicate the process against their own operating models, customer types and products, in order to identify the correct business services relevant for them.

With thanks to Baringa Partners LLP for their help with the Business Services Working Group.

RESILIENCE FRAMEWORK FOR FIRMS

There is no one-size-fits-all approach to resilience. Proportionality is advocated as the application of Operational Resilience strategies will vary according to firm size, structure, products, services, interconnectedness and market impact.

Utilising existing documentation and processes, such as governance and operational risk frameworks, and business continuity plans forms a useful foundation to build an approach for implementing Operational Resilience holistically across the firm. There are certain factors that are important when going through the process of embedding operational resilience into firms and this framework is intended to summarise these elements.

Board engagement

- Defined governance arrangements with person(s) identified as responsible for Operational Resilience with sufficient seniority and a clear mandate.
  - Under SM&CR, Operational Resilience is owned by the SMF24(s) for enhanced firms. Core firms should also look to appoint a senior individual.
  - The role of identifying and mapping business services should be clearly set out to an individual or team with clear Board and/or Senior Management oversight.
- Appropriate oversight from the Board to ensure the holistic application of Operational Resilience rather than managing key services in silos.
  - This will require engagement across the business and communication across teams and locations to ensure the firm takes a services/ consumer focussed approach.
- Technical expertise at Board or Senior Manager level to provide effective challenge across the three lines of defence.
- Setting a top-level example helps establish a resilience culture.

Defining and mapping important business services

- Clear understanding of the most important business services to customers.
  - This may require communication and/or engagement with customers to determine what services they value most.
- Customer at the heart of determining 'important' business services – what services do they most rely on; what will impact customers the most in the event of an outage?
- In addition to knowing what services are important to customers, firms need to maintain awareness of the services that if disrupted could affect firm viability as well as trigger systemic consequences for the wider market and economy.
- Mapping systems and processes looking at:
  - **Technology** – knowledge of key underlying IT systems. This is especially important during the change management process.
  - **People** – who are the key individuals associated with the service throughout the value chain, where does responsibility lie?
  - **Outsourcers** – and associated concentration risks of many firms relying on a small number of crucial suppliers.
  - **Facilities** – from what premises are services delivered, across which jurisdictions? How will processes/approaches vary overseas?

Establish impact tolerances for each important business service

- An impact tolerance can be defined as: a firm's tolerance for disruption in the form of a specific outcome or metric.
- Impact tolerances can be assessed using a variety of metrics:
  - The maximum tolerable duration or volume of disruption;
  - Number of customers affected by a disruption to an important business service;
  - The maximum length of time a key business service could be unavailable.
- Establishing impact tolerances helps set a risk appetite to prepare firms for disruptions and ensure a firm can recover within a certain time period to minimise disruption for customers (e.g. substituting a service can rectify delivering the service to a customer but you may allow longer to rectify the initial system internally).
- Once business services have been identified and mapped, the next stage is to identify the potential risks and threats that could impact the provision of this service.
- Identifying potential vulnerabilities and the impact on the provision of a business service to its customers, gives firms the data and means to prioritise investment and resource allocation.

Scenario testing

- End-to-end testing of severe but plausible scenarios such as counterparty default and operational failure to gauge the extent to which a firm can continue to provide its business services.
- It also helps to inform and calibrate a firm's impact tolerances and help identify areas for improvement.
- Table-top exercising is also a good way of testing incident response plans, learning lessons and then implementing improvements.

Business continuity plans

- Work under the assumption disruption will occur and plan for it based on gathered data.
- Test that plans are able to continue to operate during a disruption e.g. substituting key services.
- Identified decision makers with knowledge of responsibilities and accountabilities – there should be representatives involved across the business/value chain to ensure the whole service is accounted for.
- It is important to recognise the risk of a critical third party service provider outage and to mitigate accordingly.

Effective communication

- External –
  - Keep customers and other stakeholders, such as suppliers informed
  - Protect firm reputation
- Internal –
  - Upward and timely reporting measures in place
  - Effective Management Information to inform decision-making
  - Ensuring individuals know what to do/share with their teams, direct customers, third parties etc.

Continuous improvement

- Build upon and continue to test a firm's resilience to ensure it can maintain its business-as-usual activities as much as possible during an incident.
- Apply lessons learned from previous incidents and testing to continually improve responses and overall resilience.

AWARENESS OF RISKS

Understanding the risks and being aware of the ever changing threat landscape helps inform effective resilience and focus on a firm's vulnerabilities. In particular, it is essential to map risks and how they are linked to the value chain of key services.

Growing dependence on technology

- Technology brings both opportunity and the potential for disruption
- Introduces new risks, attack vectors and vulnerabilities
- Race to gain the competitive advantage in adoption of new technologies that can help streamline services can lead to insufficient testing and consideration of the risks involved in implementation

Change management

- Change management is widely recognised as one of the foremost causes of operational incidences
- This can include new products and services, or upgrading technology
- Tested exit strategies in place can help mitigate against the risks associated with changing to a new service provider, for example

Cyber attacks

- Denial of service attacks, hacking attempts and a plethora of other cybersecurity issues pose a real risk to the continuing delivery of key services to consumers and as such need to be sufficiently mitigated against
- Internal security is frequently the weakest link
- Important to increase technological expertise at Board level
- Ensuring that IT resilience is not delegated solely to the IT team as it underlies everything.

Nature and scale of the business

- Adequate financial resources and capital to account for losses
- Appropriate systems and controls in place monitoring risks

Rising interconnectedness

- Increases risk of contagion within wider financial system if one firm faces disruption
- Where third parties are connected to customers, poses additional threats with increased access points that could inadvertently cause residual disruption
- Impact on financial stability in the event of a concentration risk issue crystalising e.g. a major commonly-used system goes down

Climate change risks

- Physical risk to infrastructure e.g. extreme weather such as flooding
- Transition risks e.g. transition to lower-carbon economy

Outsourcing and third parties

- Reliance on third party service providers for important services poses risks regarding data protection and data loss
- Knowledge and management of access and audit rights
- Lack of substitutability in event provider goes down to be able to continue to provide important services
- Integration issues between legacy systems and using new providers such as the cloud
- Effective management oversight of not just third party service providers but the fourth and fifth parties involved in the provision of the service and the risk of one of these going down

Higher customer expectations

- Expectation of round-the-clock service provision poses new challenges for firms
- Higher demand for customised services results in added pressure to deliver these and also raises the profile and reputational consequences for firms when a service faces a disruption

CYBER RESILIENCE

CYBER RESILIENCE IS A KEY AREA TO BE CONSIDERED WHEN BUILDING OVERALL OPERATIONAL RESILIENCE AND A KEY FOCUS FOR THE REGULATORS, AS HIGHLIGHTED IN THE FCA 2019-20 BUSINESS PLAN.

As IT underpins almost every single service and process within investment management firms and is at risk of failure or attack from an ever changing threat landscape, firms need to take appropriate control measures and have suitable response plans in place. Even if important IT processes/services are outsourced they should still be considered as any other internal dependency in the delivery of an important service.

Cyber Resilience should therefore also be a Board-level priority and have the appropriate governance measures in place to ensure that cyber risk is properly managed and that Boards and Senior Managers can make informed business and investment decisions.

Further information on the IA's Cyber Resilience work including the IA's Cyber Resilience Work Plan and guidance on building Board engagement and governance can be found on the IA's Cyber Resilience Expert Page **www.theia.org/industry-policy/positions/cyber-resilience**

RESILIENCE 'BY DESIGN'

Implementing continuous improvement and having a resilience 'by design' model helps firms prepare for future incidents. It is important to embed a resilience methodology into new systems and processes from the outset to prepare for outages and ensure that the service can be restored and/or substituted effectively in the event of a disruptive incident.

Effective resilience can be seen as the ability to:

PREPARE

Put control measures in place to prevent disruptive incidents.

Be aware of the threat landscape in order to develop appropriate resilience measures to mitigate the potential impact of new and emerging threats.

DETECT

Having appropriate monitoring capabilities to be able to detect incidents.

Encourage staff to report unusual events, and slowed or disrupted technology incidents.

RESPOND

Have plans in place to ensure the firms' ability to react promptly when incidents do occur.

Ensuring the firm still has the ability to continue to provide critical investment operations during an outage either through substituting the disrupted channels or rapidly restoring them.

Maintain effective communication channels both internally and externally to customers and key stakeholders.

RECOVER

Return to normal operations in a timely fashion as stated in impact tolerances.

ADAPT

Learn from incidents and adapt systems, processes and response plans to help prevent repetition and/or improve the firms' response and recovery.

TALENT AND SKILLS GAP

In order to address and implement effective Operational Resilience, it is essential for investment management firms to recognise that the people working for them are a foundational pillar of managing risk. Staff at all levels across the business need to have a clear understanding of their personal responsibility with regard to Operational Resilience, and they must have the knowledge and skills to prepare for incidents, build resilience and respond to problems when they occur.

As an emerging and evolving concept, there is inevitably a shortage across the industry of skilled and knowledgeable staff.

The IA has developed a Talent Strategy setting out how it will support members to attract, develop and retain people with the skills, knowledge and competencies the investment management industry needs. The strategy covers the career arc from entry point to executive level and has been developed following extensive discussions with IA members about current and future skills needs. It is structured around three key themes – attraction, advancement and environment – all of which are relevant for building Operational Resilience skills into the talent pipeline.

ATTRACTION

Early careers initiatives form an important part of IA members' attraction strategies. The IA is building on its successful work in supporting members to source and develop a more diverse pool of talent by expanding **Investment20/20**.

The IA will be carrying out a feasibility study into two new routes into the industry via **conversion courses** – a master's programme and a foundation programme – to help individuals from a non-STEM degree background or other sectors transition effectively into investment management.

The IA will continue to engage with government on the future of the **Apprenticeship Levy** so that members can unlock funding for training on essential new skills.

ADVANCEMENT

The IA already delivers a **technical training and events** for IA members, and will look to add focussed training on Operational Resilience to its programme.

It is important that **Board members** have the technical expertise to provide effective challenge. The IA will continue to develop its **online resource for iNEDS**, which offers essential information, support and training as well as events for facilitated networking.

ENVIRONMENT

The IA has completed a substantive piece of **consumer market research** to help develop an industry narrative explaining the role of the investment sector in a way that resonates with the general public. This seeks to address IA members' concerns around the public's perception and lack of understanding of the industry, and the effect this has on their ability to attract necessary talent.

IA members are aware of the need to anticipate future changes in the industry, including the impact that technology and innovation will have on working practices. The IA is producing **research on the changing world of work**, specific to the investment management sector to enable our members to anticipate and prepare for future skills needs and new ways of working.

It is now generally accepted that diversity of thought will create a rich pool of resource, which should serve to mitigate against the risk of 'groupthink' and enhance decision making and innovation which have an important role to play in supporting firms' Operational Resilience. The IA has supported members to progress their D&I agendas and the wider culture journey through thought leadership and sharing best practice.

Investment20/20

Investment20/20 is the industry's talent and career service that provides a 12 month trainee programme for a broader group of people to access our sector. Alongside the trainee programme, Investment20/20 delivers an extensive outreach programme and pre-employment initiatives that develop the confidence, skills and knowledge of young people enabling them to start a career in our industry.

Find out more at **www.investment2020.org.uk**

FUTURE WORK PLAN

To support members with the development and implementation of Operational Resilience over the coming years, the IA is developing an Operational Resilience Work Plan.

The plan will provide an overview of the key industry priorities associated with Operational Resilience and give detail of the IA's upcoming strategy, policy work, operational work, training and events. The direction of the plan is determined by the IA's Operational Resilience Committee, consisting of senior industry representatives.

In addition to the work already done on Business Services and Process Mapping, the IA aims to support members by forming Working Groups to look at key areas:

CONSULTATION PAPER RESPONSE

The development of the IA's response to the questions and themes contained in the Consultation Paper to ensure accurate representation of industry specific views to the regulator.

SETTING IMPACT TOLERANCES

Supporting member firms in setting, monitoring, testing and adjusting impact tolerances for their key business services.

SUPPLY CHAIN & OUTSOURCING RISK

Creating member guidance on the identification, management and monitoring of supply chain & outsourcing risks that may impact a firm's resilience.

TESTING & ASSESSMENT

Helping firms demonstrate their resilience via the development of effective incident response plans to plausible operational disruption outage scenarios.

In addition, the IA will be engaging closely with key individuals across the membership, including **SMF24 Senior Managers** to gather an industry view of Operational Resilience Plans and identify key challenges requiring IA support.

The IA will continue to work closely with **regulators** to represent investment management industry views through ongoing meetings and roundtable discussions and encourage the regulators to adopt a proportionate supervisory approach.

THE
INVESTMENT
ASSOCIATION

The Investment Association
Camomile Court, 23 Camomile Street, London, EC3A 7LL

www.theia.org
@InvAssoc

December 2019