# Adopting cross-industry resilience practices; a guide for financial services

# Adopting cross-industry resilience practices; a guide for financial services

The need to plan and prepare for operational disruption within the financial services industry has never been more important. Advancements in automation and artificial intelligence, growing cyber risk, increased outsourcing, economic disruptions such as Brexit and climate risk have all made this need more acute. Historically, firms have focused on preventing disruption, but increasingly regulators are requiring firms to assume disruption will occur and have plans in place to ensure continuity of service.

While media coverage of operational resilience focuses on major incidents or outages within financial services firms, the national headlines throughout 2019 have also highlighted that operational resilience is a key focus for a number of other industries. Telecoms outages, energy supply interruptions and service pressures in the NHS are just a few examples. Throughout this paper, we will investigate how other sectors approach resilience and what lessons the financial services industry can learn from them, focusing on the following questions:

- Who is responsible for ensuring resilience?
- What services do firms need to ensure are resilient?
- How resilient does a firm need to be?
- How can firms assess resilience?
- What happens when it all goes wrong?
- How can firms assess the impacts of a resilience incident?
- What does good resilience testing look like?
- What role can the regulator and industry play?

## Summary of key elements of the UK authorities' discussion paper on operational resilience

In July 2018 the Bank of England (BoE), Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA) published a joint discussion paper on an approach to improve the operational resilience of firms and financial market infrastructures[1], which is summarised below:

### Business service focus

- Focus should be on ensuring resilience of firms' most important business services as a whole
- Firms need to understand how individual systems, processes, people and assets can impact the resilience of their business services
- Focusing at a business-service level should drive the right decision-making and investment
- Resilience investment should focus on the risk it is mitigating

### Planning for failure

- Working to prevent disruption is not enough. Instead, firms should assume that disruption will occur, and put in place workarounds, back-up plans and/or recovery options
- Risks are often identified only when something has gone wrong
- The resilience of the overall financial system is dependent on the connection between the underlying services offered by firms

### Impact tolerances

- Firms should set impact tolerances for the operational resilience of their business services
- Impact tolerances may be expressed by specific metrics (e.g. customers impacted)
- Tolerances should be expressed clearly and are separate to risk appetites or recovery time objectives (RTO)
- These will then allow for testing and measurement in order to meet regulatory requirements

### Supervising resilience

- In the future, there will be greater supervision and regulation of operational resilience
- A future supervisory approach would likely cover:
  - Sector-wide work, such as stress testing
  - Assessment of how firms set and use impact tolerances
  - Analysis of systems and processes
  - Assurance of how resilience is governed

The authorities are expected to publish further detail on their vision for operational resilience and their policy proposals for enhancing operational resilience standards in a series of consultation papers in Q4 2019.

[1] Bank of England, Prudential Regulation Authority, Financial Conduct Authority (2018), *Building the UK financial sector's operational resilience*

## What does being resilient involve?

In order to address changing regulatory requirements, financial services firms must better understand the connections between their systems, processes, people and premises, and how the resilience of these components impacts the overall resilience of the services they provide to end users. Moreover, firms need to have mechanisms in place to monitor resilience, respond when problems arise and determine when additional investment in resilience is required. Rather than introducing a new framework around operational resilience, this requires firms to embed resilience within existing operational capabilities. These capabilities need to work in unison to allow an organisation to offer resilient services to its customers and other interested parties. At a high level, firms must demonstrate the following seven key elements:

1. Clear **ownership and accountability** exist for operational resilience, which includes understanding the critical people, processes and systems that underpin a resilient service. The board should actively weigh up the costs of an operational resilience incident against the financial cost of investing to prevent this
2. **Operational processes and locations** are designed to support resilience during disruption. This includes areas such as Incident and Crisis Management, and Business Continuity Planning
3. **Business and IT changes** are managed in a way that supports resilient outcomes
4. The **technology systems, processes, data and infrastructure** in place are sufficiently resilient to maintain service during disruption, and support fast and effective recovery
5. Proportionate **information security** capabilities are in place to protect against adverse cyber security events
6. The resilience risk relating to **third-party suppliers and partners** is understood and adequately managed, with suppliers assessed on how they manage risk at the point of selection as well as on an ongoing basis
7. The organisation has a **culture** that values behaviours supporting resilient outcomes, and **people** with sufficient skills and knowledge to maintain resilience

# Who is responsible for ensuring resilience?

The PRA's Senior Managers & Certification Regime (SM&CR) places individual accountability for operational resilience on the person (or persons) who fulfils the Senior Manager Function 24 (SMF 24). However, in their discussion paper the UK authorities also highlighted that they expect resilience to be the responsibility of the board. This is consistent with other industries, for instance, the energy and utilities sectors, where a firm's board is ultimately responsible for ensuring that risk management policies are defined and business services continue in the face of a disruption. For a number of financial services firms, this will involve ongoing education sessions for the board and senior management around what resilience is, and their role in ensuring it.

However, accountability doesn't stop at the top – accountability for resilience needs to be embedded throughout the organisation. In the energy sector, the single focus on ensuring a continuous flow of energy and 'keeping the lights on' helps unify staff and creates a culture where everyone feels accountable for the resilience of that service. Daily and weekly team meetings are centred around performance of the service, with displays in offices and warehouses showing how long it has been since the last resilience incident. This encourages everyone to feel responsible for mitigating and resolving disruptions. The same is also true in the telecoms industry, where their singular purpose is maintaining network availability. A unifying purpose doesn't have to mean a singular purpose. In the aviation sector, ground handlers, traffic controllers and pilots all have multiple but unifying purposes around ensuring passenger safety and delivering an efficient transport experience for customers. As financial services firms move towards defining their business services from the perspective of the end user, this unifying purpose will develop and support embedding a resilient culture.

# What services do firms need to ensure are resilient?

The discussion paper published by the BoE, PRA and FCA requires firms to understand the end-to-end services they provide and what can impact the resilience of these services. One option firms can use as a starting point to accomplish this is customer journey maps. Within the aviation industry, Heathrow Airport mapped out the main stages of the passenger journey at the airport to assess resilience across the whole user experience. This enabled them to identify the various teams that would impact the resilience of the passenger journey, define the interaction model between them and work through the response of each team during a disruption.

It is not sufficient for firms to look at their services in isolation; they must also consider the interdependencies between their services to fully understand the resilience of a service. Yorkshire Water provides an interesting case study for this. In addition to identifying the stresses that could directly impact their systems, they also identified where stresses could indirectly impact systems through an interdependent system.

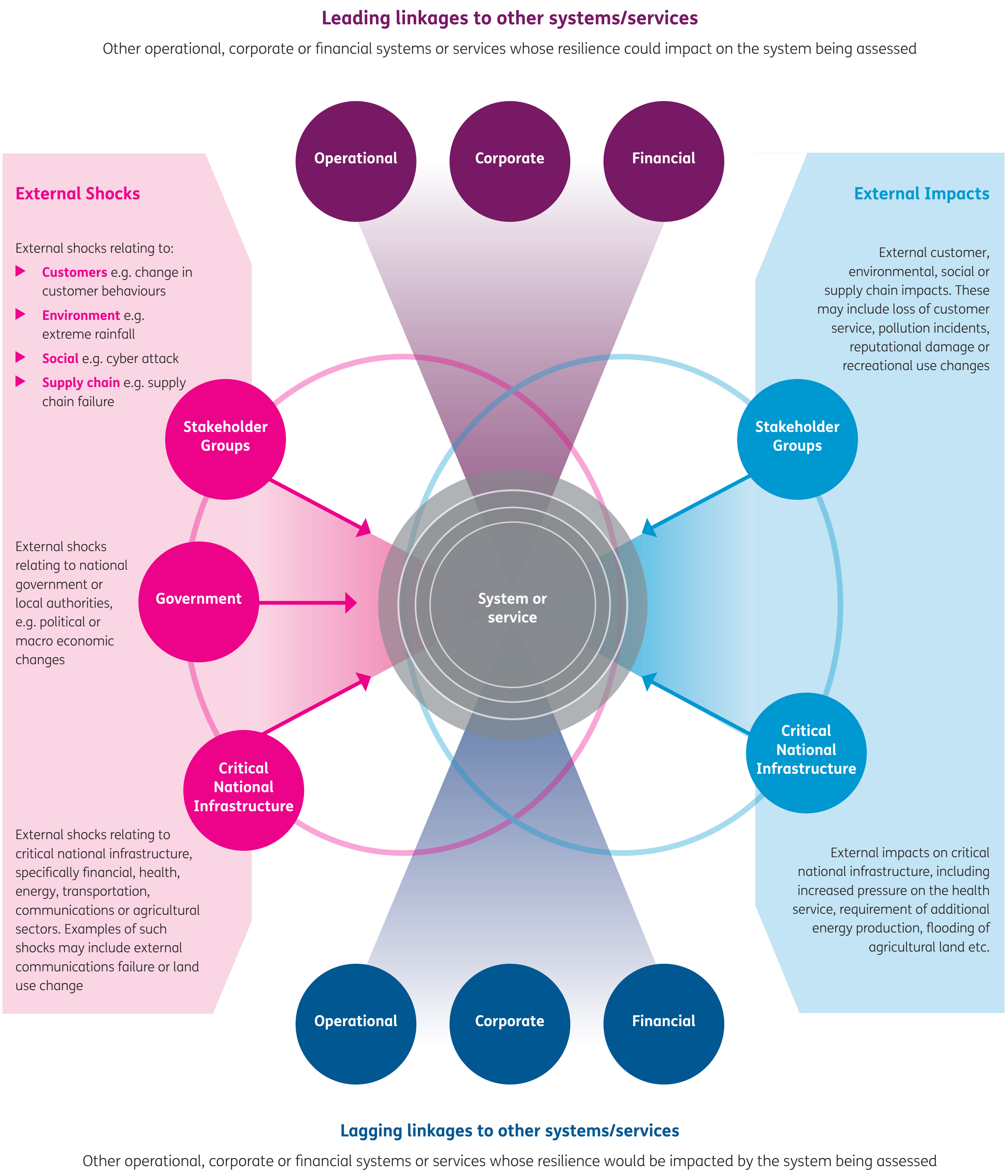
As set out in Figure 1 opposite, for each of their services, Yorkshire Water documented:

- External shocks relating to stakeholder groups, government or critical national infrastructure that could impact the system in question
- Links or interdependencies between the system and other financial, corporate and operational systems/services within Yorkshire Water
- Possible external impacts of any resilience issue with that system, either to stakeholder groups or to critical national infrastructure

Yorkshire Water considered both leading and lagging interdependencies. For instance, when assessing water resources, Yorkshire Water identified land management as a leading interdependency, such that problems with land management could result in a problem with water resources. It also identified water distribution as a lagging indicator, such that problems with water resources could result in issues with water distribution. Understanding how their systems link together as a whole enables Yorkshire Water to better comprehend, and therefore prepare for, the impacts of a resilience incident.

This same approach can be used by financial services firms to understand the shocks that could impact their services both directly and indirectly, and how they can manage these shocks.

## Figure 1: Stylised illustration of the interdependence map used by Yorkshire Water



**Leading linkages to other systems/services**

Other operational, corporate or financial systems or services whose resilience could impact on the system being assessed

**External Shocks**

External shocks relating to:

- **Customers** e.g. change in customer behaviours
- **Environment** e.g. extreme rainfall
- **Social** e.g. cyber attack
- **Supply chain** e.g. supply chain failure

External shocks relating to national government or local authorities, e.g. political or macro economic changes

External shocks relating to critical national infrastructure, specifically financial, health, energy, transportation, communications or agricultural sectors. Examples of such shocks may include external communications failure or land use change

**External Impacts**

External customer, environmental, social or supply chain impacts. These may include loss of customer service, pollution incidents, reputational damage or recreational use changes

External impacts on critical national infrastructure, including increased pressure on the health service, requirement of additional energy production, flooding of agricultural land etc.

**Lagging linkages to other systems/services**

Other operational, corporate or financial systems or services whose resilience would be impacted by the system being assessed

# How resilient does a firm need to be?

It will be a major change for financial services firms to stop looking at the probability of an incident occurring and to start assuming and planning for failure. Historically, the same has been true in the energy industry, where high capacity, triple redundancy of data centres, quadruple redundancy for applications, and a robust control environment meant that resilience incidents rarely arose. As such, it was hard to make the case for investment in ensuring resilience against scenarios that were not crystallising.

UK financial services regulators have left it down to firms to determine the appropriate level of resilience that they should maintain. Firms have to balance the cost of investing in resilience against the impact from a resilience incident if they fail to do so. In the energy sector, firms rely on customer panels for help. Focus groups are asked questions around how stable an energy connection they want, the acceptable level of planned and unplanned interruptions to their service, and the value they would place on increased reliability. These panels are held annually, sometimes more frequently, and help firms understand the resilience demand from customers.

A similar approach is used in the water industry with independent groups of customer representatives and other stakeholders, known as customer challenge groups (CCGs). The regulator mandates the use of a CCG, whose roles and responsibilities include reviewing and providing feedback on firms' resilience plans. Water companies publish details of the membership of their CCGs, the response of the CCGs to their business plans, and details on how they are addressing any concerns raised by the CCGs.

Clearly, consumers are not the only drivers or influencers over firms' resilience levels – the regulator will play a large part in guiding firms as to whether their resilience levels are sufficiently justified. In the same way that both OFGEM and OFWAT review and challenge firms on their levels of resilience investment and their justification for this, we can expect that the UK financial services authorities will hold firms to account about how they arrive at their decisions around resilience.

### Resilience as a differentiator

In the telecoms industry, network resilience is not driven by consumer input but is seen as a differentiator and an area on which firms compete to gain market share. Companies such as uSwitch, Tech Advisor and Which? regularly publish information on firms' network reliability and performance, including how that reliability changes across the country. RootMetrics, an IHS Markit company, goes further and provides half-yearly reports on performance and reliability across the big four players for 16 different metro areas in the UK, alongside interactive coverage maps for each provider's call performance across the country.

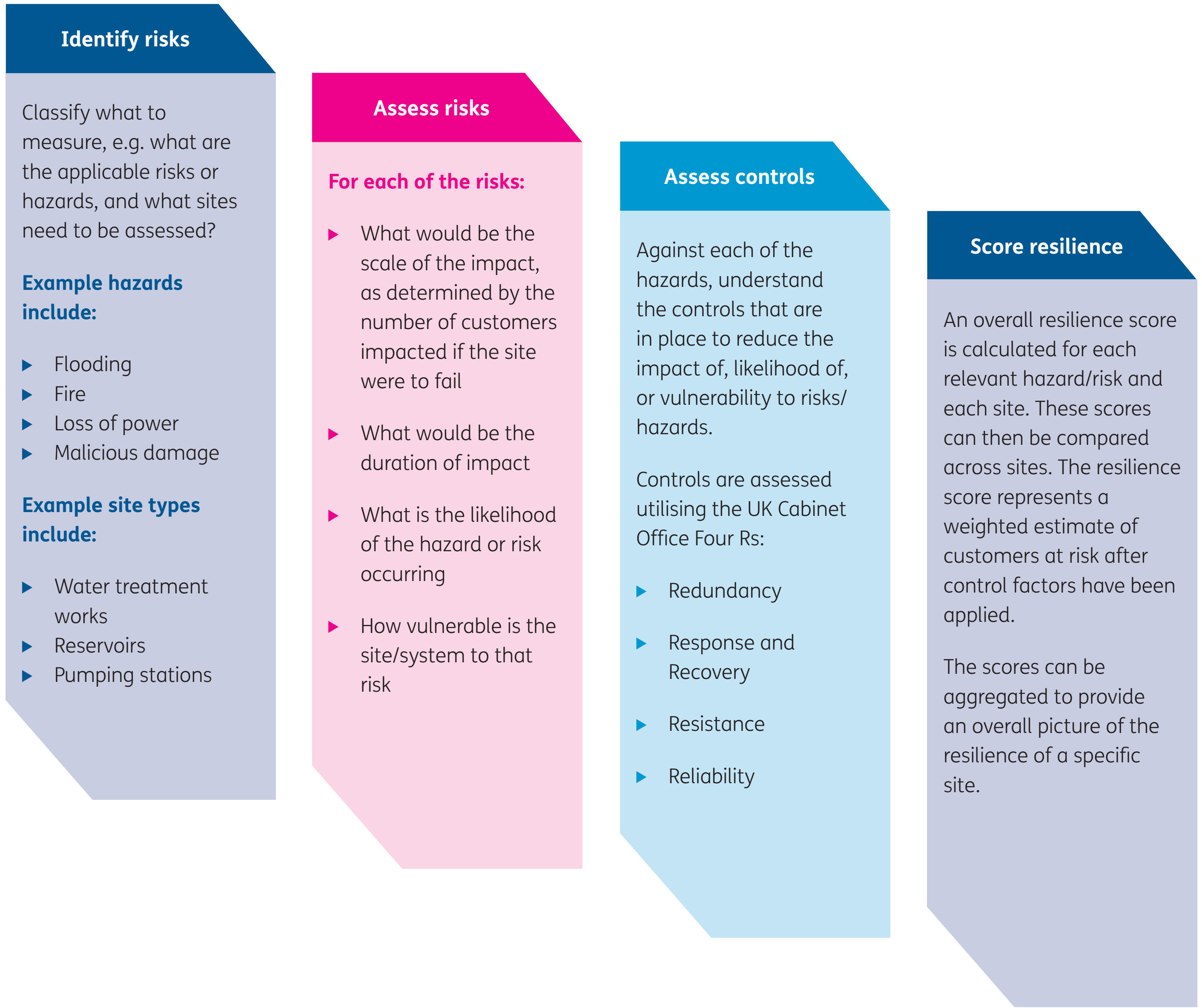
This access to information, and the fact that the new Text-to-Switch service has made it easier than ever for consumers to switch telecoms providers, means resilience will continue to be an important factor in market competition. Likewise, the introduction of the Current Account Switch Guarantee in 2013 and the increased use of switch incentives may be an indicator that resilience will prove to be a similar source of competition in banking going forward. In the future, the size, duration and handling of IT incidents may all prove to be sources of data that consumers consider when deciding on who to bank with, and whether to switch their account.

But resilience can be more or less important to different people. Some firms have capitalised on this, creating premium products targeted to those who value resilience more highly. Vodafone's dedicated internet access product is specifically designed for businesses that want a faster and more reliable service, and are willing to pay for it. In the financial sector, banks already offer premium services to customers who meet certain conditions, with benefits including dedicated relationship managers and 24/7 customer service, free travel insurance, preferential rates or perks such as free Wi-Fi or discounts on restaurants. In that context, resilience differentiators on premium financial services products might not be that hard to imagine.

# How can firms assess resilience?

Firms need to understand their current resilience maturity in order to determine if it is within or outside appetite, and whether further investment is needed. Assessing how resilient a firm's services are is no small feat, as it requires an understanding of all the components that impact on the delivery of the service, from people to processes to systems to premises.

In this regard, financial services firms can learn from the water industry, where significant effort has been spent in developing a clear and structured approach to measuring the resilience of their various sites and services, as outlined in the diagram below[2]. The principles behind how water companies tackle their resilience assessment are very much aligned to how financial services firms already assess their operational risks, i.e. identify the relevant risks, assess or quantify inherent risk, assess controls, assess residual risk. However, it is not an approach financial services firms apply consistently when it comes to assessing their resilience.



**Identify risks**

Classify what to measure, e.g. what are the applicable risks or hazards, and what sites need to be assessed?

**Example hazards include:**

- Flooding
- Fire
- Loss of power
- Malicious damage

**Example site types include:**

- Water treatment works
- Reservoirs
- Pumping stations

**Assess risks**

**For each of the risks:**

- What would be the scale of the impact, as determined by the number of customers impacted if the site were to fail
- What would be the duration of impact
- What is the likelihood of the hazard or risk occurring
- How vulnerable is the site/system to that risk

**Assess controls**

Against each of the hazards, understand the controls that are in place to reduce the impact of, likelihood of, or vulnerability to risks/hazards.

Controls are assessed utilising the UK Cabinet Office Four Rs:

- Redundancy
- Response and Recovery
- Resistance
- Reliability

**Score resilience**

An overall resilience score is calculated for each relevant hazard/risk and each site. These scores can then be compared across sites. The resilience score represents a weighted estimate of customers at risk after control factors have been applied.

The scores can be aggregated to provide an overall picture of the resilience of a specific site.

[2] Arcadis & United Utilities (2017), *Measuring Resilience in the Water Industry*; Northumbrian Water (2018), Business Plan Appendix 3.6: *Resilience Assessment Final Report (PR19 Too Critical To Fail Sites).*

Resilience assessments are much further developed in other industries, as firms increasingly look at more effective ways to both visualise and engage with resilience data. A good example of this is Southern Water, which has developed zonal resilience maps that visualise the level of resilience across various zones or sites in the network and show which sites are most critical (based on the expected impact from a hazard occurring). Similarly, Northumbrian Water has developed a resilience dashboard that shows the level of resilience across individual sites, including the key hazards and the level of controls in place. Data visualisation tools are something we already see financial services firms looking to employ in areas such as operational risk, and they could be expanded to also cover resilience.

Assessing the resilience of services that rely on third parties has proved challenging for financial services firms. Energy transmission networks and distribution companies manage this risk by limiting their reliance on third parties and by closely managing them. This is done through carefully monitoring service level agreements (SLAs) with third parties and working closely with them to ensure that, while services may be outsourced, knowledge is not.

Collaboration is also employed by the NHS, with winter resilience plans developed in tandem with partners and providers, including ambulance providers and local authorities. Financial services firms can learn from these examples by fully understanding their third-party network, clearly defining resilience objectives in SLAs, closely monitoring performance against SLAs and ensuring that they retain the capacity and capability to take back outsourced services if they need to (or transfer easily to another provider). However, firms need to go further and also consider potential systemic risks if the industry as a whole is concentrating around the same few providers, and to engage with regulators to discuss these issues.

### *It's about monitoring, not just measuring*

Understanding the resilience of a service and the potential risks is not enough – firms also need to monitor actual resilience on an ongoing basis.

The OFWAT report into the freeze/thaw incident in Q1 2018[3] noted that part of the problem was that major supply problems were not picked up early enough by some companies, and real-time data on network issues was lacking. The firms that performed better, notably Northumbrian Water, United Utilities, Wessex Water and Yorkshire Water, were highlighted as using real-time information and monitoring systems to identify and manage issues.

Northumbrian Water announced earlier this year that it was going a step further, partnering with BT to deliver a smart-water project. Through sensors in its pipe network, Northumbrian Water will capture and process data on how the network is functioning, including real-time data on water flow, pressure and quality. Similarly, in the energy industry, National Grid monitors gas flow in real time. Real-time data enables firms to anticipate issues before they arise, and proactively take action to avoid them escalating, rather than being on the back foot.

Financial services firms have increasingly been exploring the use of real-time data in the context of risk management, for example, for surveying markets and detecting money laundering or payment fraud. Firms should explore what existing data they can bring together and leverage to monitor resilience, and the gaps where they need to invest in developing new data.

[3] Figures taken from OFWAT (2018), *Out in the Cold: Water Companies' Response to the 'Beast from the East.'*

# What happens when it all goes wrong?

Even when firms invest in enhancing controls and plan for disruption, there is still the possibility of an incident disrupting their services. The important thing in these circumstances is not only how such incidents are handled, but also how lessons learned are used to drive through resilience enhancements going forward.

### Incident communications

A positive example of how to handle a resilience incident is aluminium producer Norsk Hydro. In March 2019, hackers targeted Norsk Hydro with a ransomware attack, impacting 22,000 computers across 170 sites and 40 different countries. As a result, 35,000 employees were forced to use pen and paper to keep things going. The attack also came at a challenging time for the company; just days before, the CEO had retired, and the new CEO was not scheduled to take up his role until two months later. Unlike other firms that have faced the same situation, Norsk Hydro chose not to pay the ransom, relying on the entire workforce, and many long-retired workers, to band together and get things up and running. While the incident certainly cost the firm in terms of productivity and revenue, their open and transparent response has been highlighted as the gold standard across the industry, and their reputation has benefited. Norsk Hydro's CFO held a press conference the morning after the ransomware attack, informing people that most IT systems were impacted and that the firm was switching to manual processes. Over the next few days, weeks and months, the firm continued to provide frequent and detailed updates – via their website, social media and press conferences – about the business units impacted, the status of the investigation and the progress on restoring systems.

In contrast, customers of Lloyds Banking Group were vocal about their frustration at the lack of communication following the IT outage in January 2019, and the same has been true of similar incidents at other banks. Financial services firms should make sure that, when undertaking resilience planning and testing, they also consider their communications plans, taking lessons from Norsk Hydro. Firms should determine what the right communications strategy looks like for them; a bank whose customers predominantly visit branches will need a very different strategy than an online-only bank whose customers largely use their mobile application. The key premise, however, remains the same – like any good relationship, it is about open, honest and regular communication.

### Continuous improvement cycles

Firms need to keep enhancing their resilience and learn lessons from resilience failures or incidents. Root cause analysis is a method used by many industries for investigating failures, and it is often used in the financial services industry for complaints investigations. However, it has not been consistently employed to learn from resilience incidents.

Root cause analysis has been heavily employed in the aviation industry, including to investigate aeroplane crashes, and an understanding of the technique is essential for complying with airline safety management and audit programs. The '5 whys' technique is often employed in root cause analysis and involves exactly what the name suggests: asking 'why' 5 times in order to get to the root cause of a problem. This is a simple technique which, in tandem with cause maps, can help create a structured analysis that is easy to understand.

Analysis needn't be firm specific. In the case of industry-wide incidents, firms can collaborate in order to jointly assess the causes and learn lessons. A good example of this is the water industry's response to the freeze/thaw incident; in addition to the regulator investigation, water companies also came together to discuss lessons learned and potential interventions.

It is not sufficient to merely investigate how and why incidents happened; firms need to then take that analysis and incorporate the lessons into their resilience plans going forward. Following the OFWAT report on the freeze/thaw incident, Southern Water responded by improving detection and forecasting of events, and also by ensuring that they would be better equipped to respond if a similar situation arose. To this end, Southern Water drastically increased their available bottled-water supply stocks, as well as increasing the supply of stocks that can be called upon within four hours and within 24 hours.[4]

The best way to ensure lessons are taken on board is by presenting the outcome of the root cause analysis to senior management at board level and discussing potential actions the firm should take on the back of the analysis.

# How can firms assess the impacts of a resilience incident?

Following action by the FCA and the Competition and Markets Authority (CMA), and a voluntary commitment by banks and building societies, current account providers in the UK now supply more information on the services they offer customers. This includes details on how quickly they open accounts, how quickly they provide customers with a debit card and how quickly their customers have access to internet banking. However, when it comes to operational incidents, management information (MI) is limited to the number of incidents, and whether these incidents impacted telephone banking, mobile banking or internet banking.

In contrast, MI on resilience incidents in non-financial services industries is far more detailed. In addition to equivalent metrics on the number of outages, electricity network operators also monitor the customer impact of operational incidents, with metrics around the number of customers whose supply was interrupted and the number of customer minutes lost (i.e. how long customers were without electricity). The benefit of using customer minutes lost as a measure of operational resilience is how straightforward the metric is to report and compare. Firms must report this measurement to the regulator, OFGEM, at least once every year, so the regulator can easily compare the level of resilience among different network operators within the UK.

The water industry uses a similar metric for supply interruptions that looks at the average number of minutes lost per customer for interruptions that lasted three hours or more. Water companies must regularly report data on supply interruptions to the regulator, OFWAT, as well as maintain records of the timing and duration of supply interruptions, with details on the location of properties affected. This industry-wide metric is supplemented with bespoke metrics for each water company around the number of outages, mains repairs, sewer collapses, etc., as well as metrics that measure the impact of a degraded service rather than just loss of service (e.g. metrics around the average time properties experience low pressure).

Telecoms firms also monitor a number of metrics around network coverage and the quality and speed of the network. More recently, firms have considered a less mechanistic approach to measuring the impact of resilience incidents, instead measuring the impact of incidents on the customer experience. This includes looking at the implications of a network issue for customers, and the correlation between network issues and customer complaints.

We would encourage financial services firms to think about equivalent metrics to measure not just the number of incidents but also the customer impact of resilience disruptions – for instance, the number of minutes for which a customer was unable to access their money or submit a claim, or the average response time to an incident.

[4] Southern Water (2018), *Freeze Thaw Action Plan and Response to OFWAT.*

# What does good resilience testing look like?

Financial services firms have long used scenario testing to check that business continuity and disaster recovery plans are credible and realistic. However, is there more firms can do to test and plan for resilience?

Energy and utilities firms employ failure modes and effects analysis: a structured approach to breaking down a process into its component parts in order to establish potential points of failure and the impact of those failures, including to the customer. Unlike scenario testing, thinking through potential failure modes (i.e. what could go wrong, and the consequences) helps firms to actively consider multiple points of failure, rather than just the obvious ones. Firms can then use this analysis to prioritise which scenarios require full resilience plan tests.

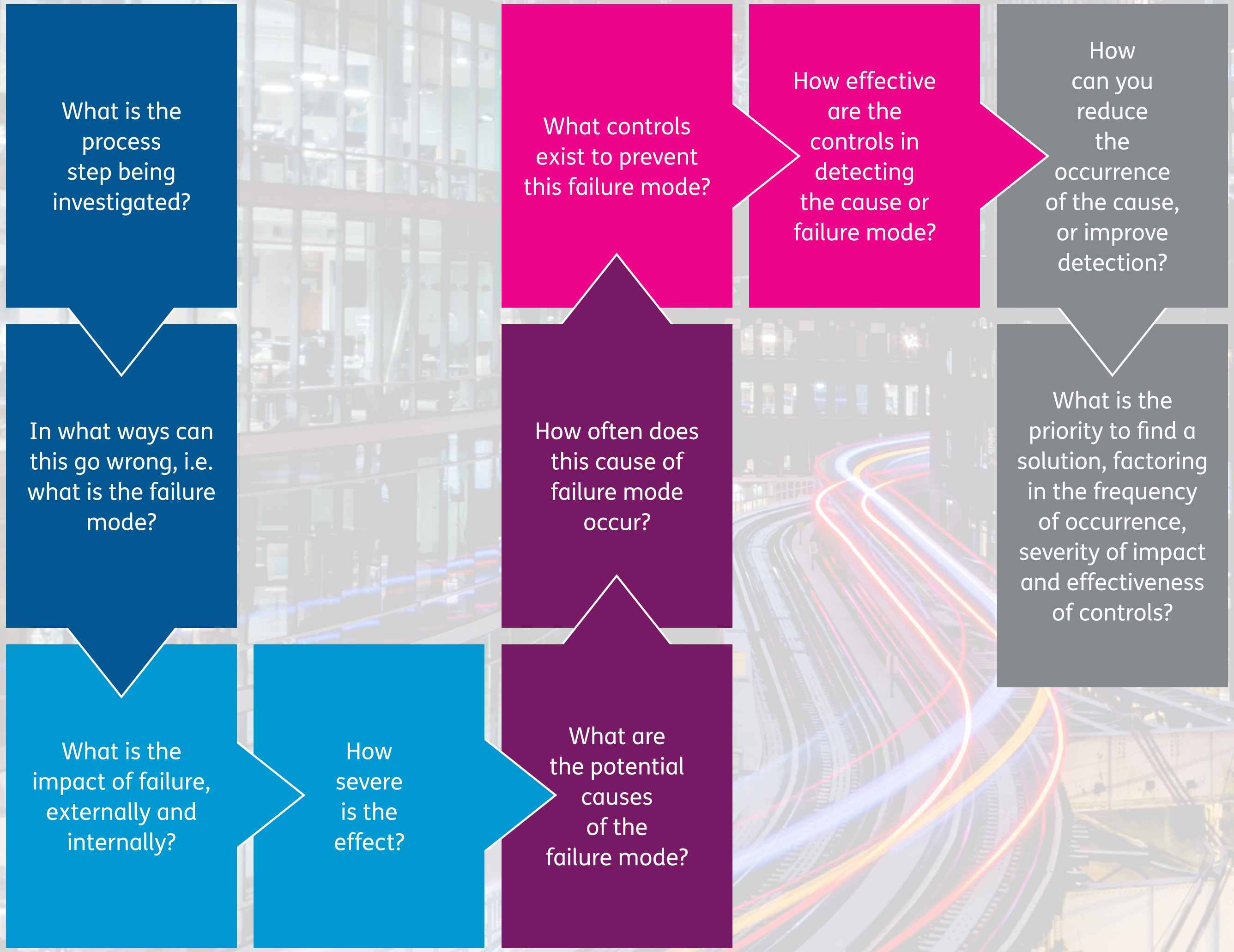
Financial services firms need to leverage their own experience and the experience of others in the industry in identifying potential failure modes and scenarios. But firms also need to challenge their own thinking in order to identify potential new avenues for failure. Industry associations and the regulators can be one source for such a challenge, but they could also play a role in identifying scenarios common across the industry. For instance, in the health industry, Public Health England has developed the Off the Shelf Exercises (OTSE) library, which provides exercise frameworks that can be used by NHS-funded providers, Public Health England and other key local partners, to help them review and enhance their resilience plans. The exercises were written in partnership with subject-matter experts and include a range of scenarios around chemical incidents, communicable disease outbreaks, fuel disruptions and winter pressures, among others. The exercises are reviewed periodically and new ones considered, so that the library remains fresh and relevant. Generic scenarios can't replace the need for firms to think through the specifics for their own organisation but can nonetheless be a useful starting point.

When it comes to scenario testing, very few scenarios tend to be fully played out in practice; instead there is often reliance on desktop walkthroughs. In addition, tests tend to involve a limited group of people. In the healthcare industry, training for failure is commonplace. NHS organisations are required to have training for all staff who have a response role in an incident, focusing on the specific roles and requirements of an individual. To this end, NHS organisations undertake a training-needs assessment to identify the types of training required by various staffing groups, including the frequency, length and delivery method for the training. All staff are trained on basic emergency preparedness, resilience and response principles, with more detailed training provided as required. For instance, in its review of winter 2017/18, the NHS outlined how it had provided intensive training to frontline staff in order to improve patient flow during high-volume winter periods, including specialist input from clinicians and social care experts.

The same is true in other industries. Southern Water provides training on the use of Arlington tanks for field operators, to help ensure ongoing water supply during an extreme weather event. In the airline industry, as part of both the initial application and the renewal of a flight crew licence, applicants are examined on abnormal and emergency procedures such as engine failure, cabin pressure failure and incapacitation of flight crew members. Applicants are also subject to Upset Prevention and Recovery Training (UPRT), which aims to provide the flight crew with the competencies to both prevent and recover from situations in which an aeroplane unintentionally exceeds the parameters for line operation or training (aeroplane upsets).

With these examples in mind, financial services firms should think about whether further training is needed across a wider group of personnel, so that, if the worst does happen, they are prepared.

## Figure 2: Failure modes and effects analysis


What is the process step being investigated?
In what ways can this go wrong, i.e. what is the failure mode?
What is the impact of failure, externally and internally?
How severe is the effect?
What are the potential causes of the failure mode?
How often does this cause of failure mode occur?
What controls exist to prevent this failure mode?
How effective are the controls in detecting the cause or failure mode?
How can you reduce the occurrence of the cause, or improve detection?
What is the priority to find a solution, factoring in the frequency of occurrence, severity of impact and effectiveness of controls?

# What role can the regulator and industry play?

In the financial services industry, only recently have regulators started to lay out more prescriptive requirements around operational resilience. In contrast, regulators in other industries have published an abundance of regulations on the standards they expect firms to follow and the level of investment that is needed in resilience. Of note is the Network and Information Systems Regulations (NIS Regulations) which came into force in May 2018 and looked to bolster cyber and physical resilience of network and information systems for the provision of essential services and digital services across EU member states.

Regulators in other industries work closely with firms to ensure that they meet service requirements, scrutinising their business and mitigation plans. For example, NHS England requires local integrated care systems to submit formal winter plans in September, covering resilience arrangements from December until Easter, with more detailed plans required to be submitted in December. The NHS provides guidance on what these plans should cover, including priorities. Similarly, OFWAT undertakes an annual assessment of water companies' business plans across a number of criteria, including how they are securing long-term resilience. The regulator sets out the factors that a high-quality plan should demonstrate, namely:

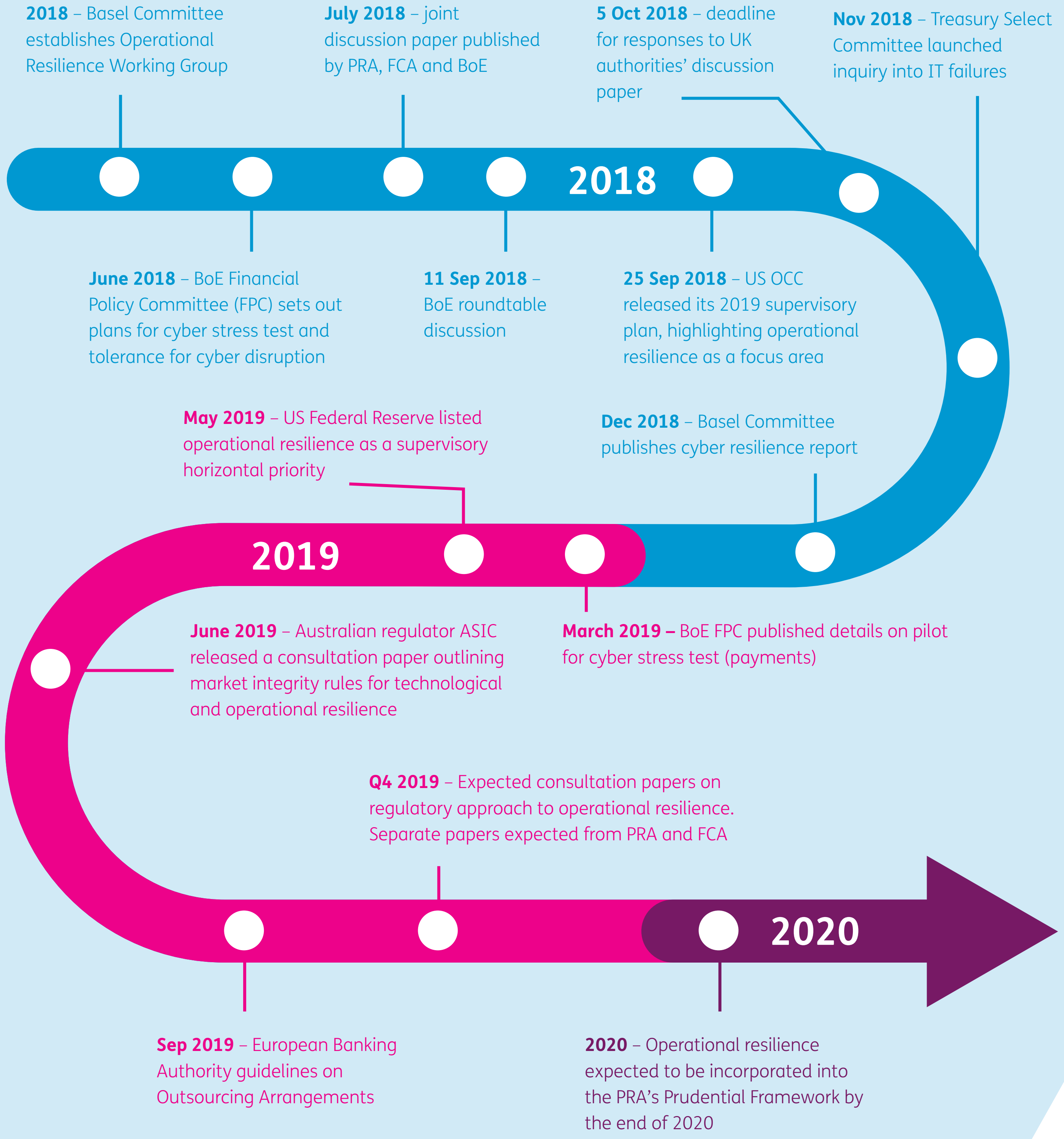
- The company has assessed long-term resilience in the round in accordance with the resilience planning principles
- The company will take an organisation-wide, integrated approach to appraising all the diverse risks to the resilience of services and interdependencies across areas
- The company will provide clear evidence that they have objectively assessed the full range of resilience management options
- The company's proposals will reflect customer preferences and will be supported by commitments made to customers
- The company will develop a plan that delivers long-term resilience in the round, which provides the best long-term value for money for customers
- The company will provide robust evidence that customers are not paying twice for resilience, given the funding provided in previous price controls

OFWAT couples this assessment with a carrot-and-stick approach, whereby the regulator reviews the supply interruptions for each water company and ranks them in order. The firms that perform worst are penalised financially, while those that perform best are rewarded through an allowance in their regulatory return. A similar approach is employed in the energy industry, whereby OFGEM rewards firms that outperform their targets on customer interruptions and customer minutes lost, and penalises those that underperform.

Within financial services, regulatory scrutiny and clear standards to assess firms against will be critical for ensuring that firms focus on resilience sufficiently. It is not just regulators that can provide a benchmark to firms – industry associations as well as joint regulator and private sector groups can also play an important role in setting the resilience standards to which firms should aspire. For instance, the operational risk association, ORX, recently collaborated with 44 of their members to develop a new operational risk taxonomy for financial services firms. Similarly, the FX Global Code and UK Money Markets Codes were both developed through joint initiatives between central banks and private sector participants.

Since the BoE, PRA and FCA published their discussion paper last year, a number of financial services industry associations have been working with their members to collectively try to address the evolving requirements on operational resilience. This includes UK Finance, the Investment Association and the Association of British Insurers. While we encourage this behaviour, the cooperation could go further. Cross-country collaboration is something we see in regulated networks, and it enables firms to learn from best practice in other jurisdictions, as well as to avoid inconsistent approaches across jurisdictions.

## A selection of recent and forthcoming regulatory developments in relation to operational resilience for financial services firms



**2018** – Basel Committee establishes Operational Resilience Working Group

**June 2018** – BoE Financial Policy Committee (FPC) sets out plans for cyber stress test and tolerance for cyber disruption

**July 2018** – joint discussion paper published by PRA, FCA and BoE

**11 Sep 2018** – BoE roundtable discussion

**25 Sep 2018** – US OCC released its 2019 supervisory plan, highlighting operational resilience as a focus area

**5 Oct 2018** – deadline for responses to UK authorities' discussion paper

**Nov 2018** – Treasury Select Committee launched inquiry into IT failures

**Dec 2018** – Basel Committee publishes cyber resilience report

**March 2019 –** BoE FPC published details on pilot for cyber stress test (payments)

**May 2019** – US Federal Reserve listed operational resilience as a supervisory horizontal priority

**June 2019** – Australian regulator ASIC released a consultation paper outlining market integrity rules for technological and operational resilience

**Sep 2019** – European Banking Authority guidelines on Outsourcing Arrangements

**Q4 2019** – Expected consultation papers on regulatory approach to operational resilience. Separate papers expected from PRA and FCA

**2020** – Operational resilience expected to be incorporated into the PRA's Prudential Framework by the end of 2020

## Summary

Regulatory requirements around operational resilience are changing. This report highlights a number of areas where financial services firms can leverage lessons from other industries to help them respond to this changing environment. The key lessons can be summarised as follows:

### Who is responsible for ensuring resilience?

Across other industries, a firm's board is ultimately responsible for ensuring that risk management policies are defined and business services can continue to be provided in the face of a disruption. However, accountability doesn't stop at the top; rather, accountability for resilience needs to be embedded throughout the organisation. The key is to have a single unifying purpose. Defining business services from the perspective of the end user should help provide this unifying purpose for financial services firms going forward.

### What services do firms need to ensure are resilient?

Customer journey maps are a starting point to help firms identify the services that they provide to their clients and what might impact the resilience of those services. However, it is not sufficient for firms to define their business services and the impact of disruption to those services in isolation. Firms also need to understand the links between their various services in order to understand how shocks may spread across services.

### How resilient does a firm need to be?

Customer panels can be an effective mechanism to calibrate the level of desired resilience. Resilience levels may vary by customer type or location, and may even be a source of differentiation or competition for firms.

### How can firms assess resilience?

Firms can leverage experience from managing operational risk to assess their overall resilience, but should also use newer data visualisation techniques to bring resilience assessments to life and make them user-friendly. In assessing the resilience of services, firms need to understand how third-party providers impact on their resilience, and where potential systemic risks exist due to a limited number of providers.

### What happens when it all goes wrong?

Despite planning, there is always the risk that an incident may occur that disrupts the provision of services. Firms therefore need to have in place a clear strategy to manage resilience incidents and provide open, honest and regular communication in a way that works for their customers. Firms also need to undertake root cause analysis to understand why resilience incidents occurred, and update their resilience plans accordingly.

### How can firms assess the impacts of a resilience incident?

Financial services firms need to consider moving away from traditional resilience metrics and instead look to measure the customer impact of resilience disruptions – for instance, the amount of time that a customer was unable to access their money or to submit a claim.

### What does good resilience testing look like?

Failure modes and effects analysis can be employed to make sure that firms don't just focus on the obvious scenarios but really consider possible failure points in their services. Regulators and industry bodies can also play a role by providing firms with a common set of industry-wide scenarios for testing. However, no amount of testing can replace the need for regular training, so that staff understand their roles and know how to respond if an incident happens.

### What role can the regulator and industry play?

Regulators can play a strong role in driving up resilience standards, both through oversight and challenges but also through incentives and penalties. Industry bodies can also help drive collaboration.

## About Baringa

Baringa Partners is an independent business and technology consultancy. We help businesses run more effectively, navigate industry shifts and reach new markets. We use our industry insights, ideas and pragmatism to help each client improve their business. Collaboration is central to our strategy and culture ensuring we attract the brightest and the best. And it's why clients love working with us.

Baringa launched in 2000 and now has over 600 members of staff and more than 60 partners across our five practice areas of Energy and Resources, Financial Services, Products and Services, and Government and Public Sector. These practices are supported by cross-sector teams focused on Customer & Digital; Finance, Risk and Compliance; People Excellence; Supply Chain and Procurement; Data, Analytics and AI; Intelligent Automation and Operations Excellence; and Technology Transformation. We operate globally and have offices in the UK, Germany, Australia, US, and the Middle East.

Baringa Partners have been voted as the leading management consulting firm for the second year in the Financial Times' UK Leading Management Consultants in the category energy, utilities and the environment. We have been in the Top 10 for the last 10 years in the small, medium, as well as large category in the UK Best Workplaces™ list by Great Place to Work®. We are a Top 50 for Women employer, and are recognised by Best Employers for Race.

### We'd love to hear from you

opresilience@baringa.com

Headquarters: London (UK) | Belgium | Ireland | Germany | Australia | Singapore | UAE | USA |