HTF

OCTOBER 2020

OPERATIONAL RESILIENCE

A research paper by HTF Research



TORI
Experience. The difference.

SPONSORED BY TORI GLOBAL

Operational Resilience

CONTENTS

Executive summary 3
Introduction 4
1. Important business services and impact tolerances 5
- Identification of most important Business Services 6
- Board Approved Risk Appetite 7
- End-to-End Systems and Processes Mapping 7

2. Third Party Supplier Management 8
- Outsourcing and Third-Party Service Providers Disruption 8
- Disruption Issues 8
- Assessment of resilience of third-party service provision 8

3. Linkage between Risk and Crisis management 9
- Resumption of business services plan 9
- Communications Plan 9
- Business Model Review 10
- Operational Resilience review post Covid-19 10

4. Technology and how stable and secure it is 11
5. Operational Resilience Framework 12
- Governance Framework 12
- Ownership of Operational Resilience Framework 12
- Allocation of roles and responsibilities 13
- Operational Resilience Areas 12

6. Management Information and metrics 14
7. Overall strategy 15
- Board Approved Strategy 15
- Board Member Accountability 16
- Senior Level Responsibility if not at Board level 16
- Level of Awareness 17
- Third-Party service providers and scenario tests 17
- Working from home 17

8. Self-assessment and lessons learned 18
- Testing of plans 18
- Lessons learnt most 18
- Testing Operational Resilience Scenarios 19
- Refreshing Resilience Scenarios 19
- Overall Level of Readiness 20

Conclusion 21

About HTF Research

HTF Research specialises in obtaining information which is otherwise Hard To Find. We conduct research among your peer organisations where the information is not available through other sources such as industry forums.

Our executive summaries and peer reviews can help with:

- Strategy best practice
- Budget setting and justification
- Market sizing
- Market understanding

Our researchers are specialists with many years of experience.

For examples and more information please contact info@htfcorporate.com.

Executive summary

This survey was conducted to examine trends in operational resilience within financial services organisations

We first looked at how the Financial Institutions (FI) overall look at Operational Resilience. There is a board approved strategy at 82% of the FI's with 59% of them having an accountable board member. If they do not have responsibility at the board level, then the most common is to have someone with SMF 24 level of responsibility with this typically being the COO. In terms of awareness of Operational Resilience throughout the organisation, 65% had medium with 25% high. Most important business services have been identified by 84% of FI's with the most common criteria being critical client services, PRA definition, and Substitutability. Payments and Trading are seen as the most important services.

Governance frameworks have been implemented by 91%, with Operational Resilience highlighted by 71% of them in this. Board Approved Risk Appetite has been undertaken by 53%, with 58% of FI's having mapped their systems and processes. Continuation or Resumption plans have been developed by 67% of FI's with 49% regularly testing them. A System of Record has been implemented by 51%. Ownership of Operational Resilience Frameworks is 53% in the 2nd line and 40% in the 1st line. A vast majority of FI's (87%) have allocated roles and responsibilities with 79% having developed and tested a Communications plan. Given the effect of Covid-19, 90% have reviewed their Business Model with 72% revisiting the Operational Resilience area.

Areas where lessons have been learnt the most are firstly Technology (85%) and then Third Party (63%). Working from home permanently was very prevalent with 93% having it as part of their plan. Testing Operational Resilience is still at an early stage, and only 30% of FI's are refreshing their Operational Resilience scenarios. Very few FI's are fully ready (7%) with 43% being ready but need improving. The biggest threats to Systemic Failure was seen as Cybercrime (83%) and then Cost Pressures (52%). Third Party disruptions were only seen by 28% during the recent crisis. Assessment of resilience of third-party service provision was carried out mostly by enhanced RCSA programs, with Third Party Service Providers closely involved in scenario tests.

Introduction

This survey examines the approach that Financial Institutions are taking with regards to Operational Resilience, with a focus on readiness for the soon-to-be-introduced regulation and the impact of the recent pandemic on strategy as it relates to Operational Resilience.

The Bank of England and the PRA, together with other regulators around the world, has for some time been focused on end-to-end Operational Resilience. This is not about being able to evidence the recovery of a system out-of-hours in a controlled DR / BCP test scenario. This is about understanding the end-to-end value chain both within the regulated perimeter (banks, insurance companies, fund managers, exchanges, clearing houses etc.) and third-parties that sit outside this perimeter but provide and/or support critical services to these regulated entities. The recently introduced EBA regulation concerning material outsourcing also plays to this.

Ultimately, Operational Resilience looks to understand the complex inter-connected dependencies and potential impact to the real economy. In this respect, Payments, Clearing, Settlement and Custody & Safekeeping are significant areas of interest. Similarly, the continued and indeed accelerated migration to the Cloud and as a result of COVID-19 together with the significant uptick in adoption of Digital services are key considerations.

This next regulatory pillar is fast approaching and will align to other regulatory regimes including the Senior Manager Regime whereby Operational Resilience will become a Board-level accountability, Recovery & Resolution Planning and Regulatory Data Aggregation.

Survey Metrics

This survey was conducted between August 2020 and September 2020. There was a total of 33 participants. This was a global survey that looked at a wide range of large and small Financial Institutions including:

- Banking (Retail, Wholesale, Private)
- Building Societies
- Insurance
- Asset Management

The job titles of the participants were typically:

- Head of Operations Resilience
- Head of Non-Financial Risk
- Head of Operations
- Chief Risk Officer

The research was conducted primarily via an online survey, supported by telephone interviews as required.

Areas covered

The study was split into a number of different sections. The following key areas were examined and analysed:

1. Important business services and impact tolerances
2. Third-party supplier management
3. Linkage between Risk and Crisis management
4. echnology and how stable and secure it is
5. Operations Resilience Framework
6. Management Information and metrics
7. Overall strategy
8. Self-assessment and lessons learned

1. Important business services and impact tolerances

We covered a number of key areas here:

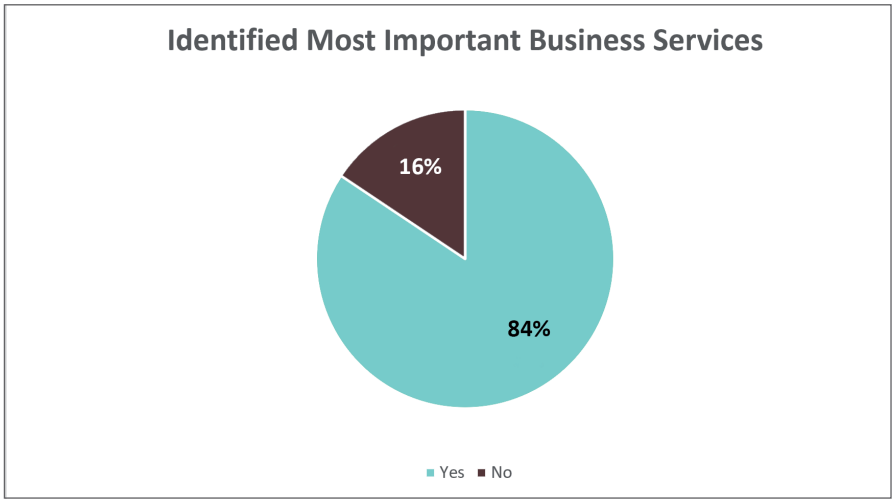
- Identification of the most important business services
- The market and client criteria being used to identify the services
- Which are the most important business services
- Bucketing of differing severity of market and client impacts
- Board Approved Risk Appetite
- End-to-End Systems and Processes Mapping

To achieve Operational Resilience UK regulators have stipulated that firms:

- Identify their important business services that if disrupted could cause harm to consumers or market integrity.
- Identify and document the people, processes, technology, facilities, third parties and information that support a firm's important business services (mapping).
- Set impact tolerances for each important business service (i.e. thresholds for maximum tolerable disruption).
- Test their ability to remain within their impact tolerances through a range of severe but plausible disruption scenarios.
- Conduct lessons learned exercises to identify, prioritise and invest in their ability to respond and recover from disruptions.
- Develop internal and external communications plans for when important business services are disrupted.
- Create a self-assessment framework.

Identification of most important Business Services

The vast majority of Financial Institutions have identified them. Business services are the foundation for Operational Resilience and the operating model should reflect the accountability for the service in its entirety. This may require fresh thinking as the business service will almost certainly cross lines of business, legal entities, geographies and potentially third parties too. Alignment is needed between those having an overall responsibility as SMF24 and those delivering the actual Operations services in supporting functions who typically have accountability for discrete performance of individual service elements, but not all. The operating model must deliver the required ownership and accountability for the Operational Resilience of each of the business services to support SMF24 in managing their overall responsibilities at board level.



Criteria to identify most important Business Services

From the above we asked what market and client criteria are being used to identify those services? The results were very varied, but they included:

- Critical client services (mentioned four times)
- PRA definition of critical processes (three times) with additional criteria
- Substitutability (three times)
- Client harm (three times)
- Reputational Impact (twice)
- FCA's description of an Important Business Service
- Customer and Operations facing services

Most Important Business Services

Following on from the above criteria we asked which were the most important services. Several participants said they categorised them either in A/B or A/B/C. Specific ones mentioned included:

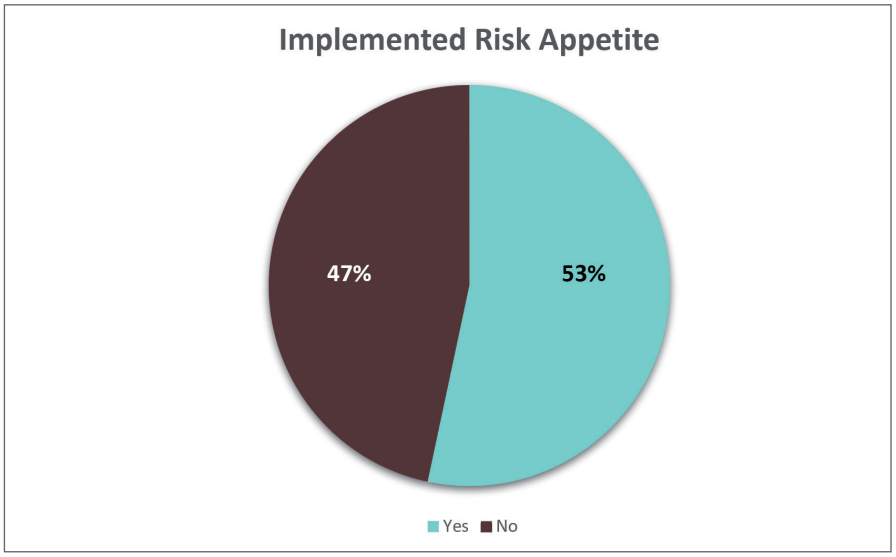
- Payments (seven times)
- Trading (five times)
- Substitutability (twice)
- Critical infrastructure
- Client harm
- Client facing
- Client service delivery

The prevalence of payments is not surprising given its systemic importance and relevance to the real economy. The fact that this rated so highly may also be a result of the Bank's recent scenario testing which focused on payments and specifically the CHAPS and 'Faster Payments' infrastructure.

Bucketing of differing severity of market and client impacts

Looking at the bucketing, there was a wide variety of answers on this but generally they were dealt with under Non-Financial/ Operations Risk Frameworks. Otherwise there 3 to 5 levels of tolerance with some mentioned including

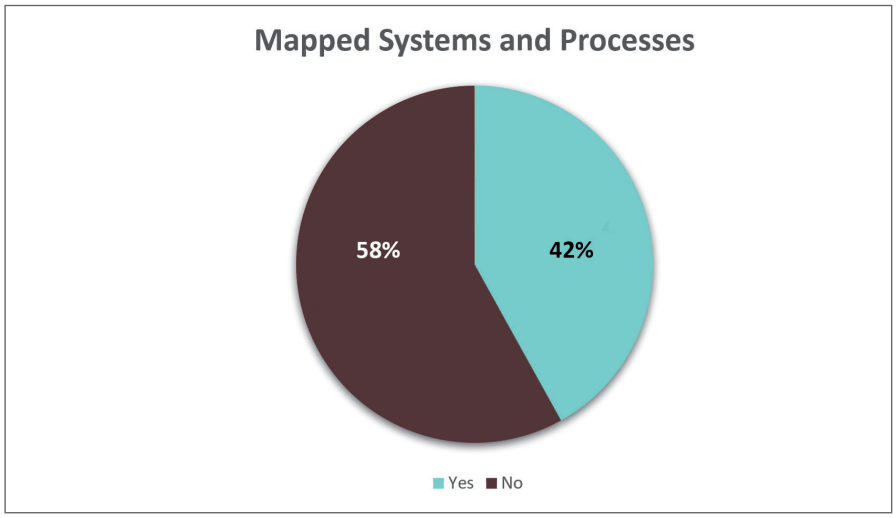
- Acute, Severe, Critical, Significant, Important
- Red, Amber, Green, with various thresholds reviewed annually
- High, Medium, Low



Board Approved Risk Appetite

We examined if Financial Institutions had implemented a Board approved risk appetite and impact tolerance statement with supporting business and function-aligned risk and control exposure metrics.

It appears that this is still an emerging area with a number of Financial Institutions still to implement.



End-to-End Systems and Processes Mapping

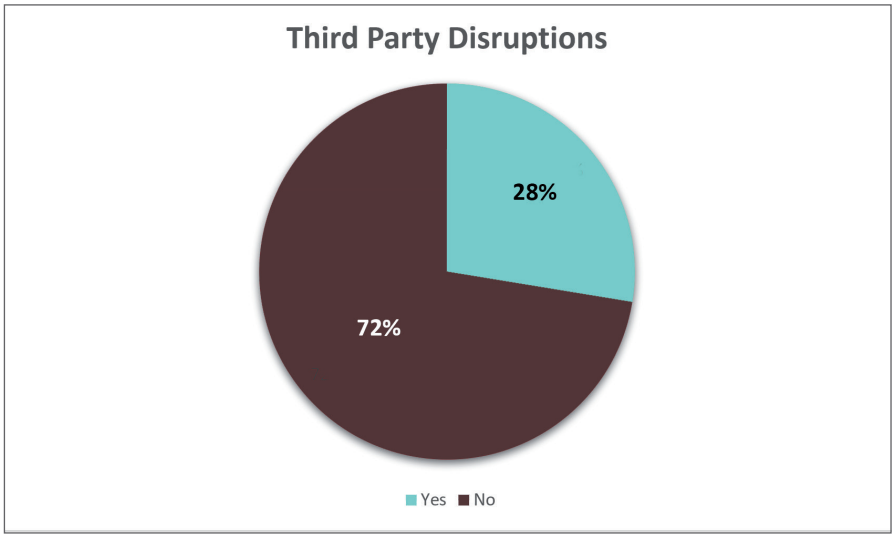
We next asked if Financial Institutions have mapped end-to-end systems and processes that support these business services, including those over which the firm may not have direct control (FMI's, outsourced providers or entities within the same group but in another jurisdiction for example)

This is an area where there has not yet been the focus that is needed. The exercise of mapping systems and processes that support business services in order to identify vulnerabilities in the delivery of important business services within an impact tolerance, will require firms to consider systems and processes over which the firm may not have direct control (for example, third-party service providers and intra Group arrangements).

2. Third Party Supplier Management

The issues covered here include:

- Outsourcing and Third-Party Service Providers Disruption
- Disruption Issues
- Assessment of resilience of third-party service provision



Outsourcing and Third-Party Service Providers Disruption

Whilst Financial Institutions themselves have managed well we asked if any of them have experienced any disruptions from their outsourcing and third-party service providers because of the lockdown? Third-party risk management includes affiliates, other intra-Group arrangements and outsourced services. Accountability for Operational Resilience cannot be outsourced and there must be robust governance and SMF24 oversight of material outsourced arrangements (as also stipulated in the recently published EBA regulatory guidelines).

It was pleasing to see that nearly three quarters of them had not experienced any disruption.

Disruption Issues

In terms of what sort of issues have been experienced and how they have been dealt with short and long term the following were mentioned:

- IT equipment supply
- Loss of productivity at initial stages, issues with technology dependencies with a plan to review strategy to ensure balance of outsourcing v internal model
- Temporary problems with supply chain for plastics for cards. This has now been resolved and contingency is in place.
- Inadequate BCP at third party provider. They recovered the capability themselves and will insource it going forward.

Assessment of resilience of third-party service provision

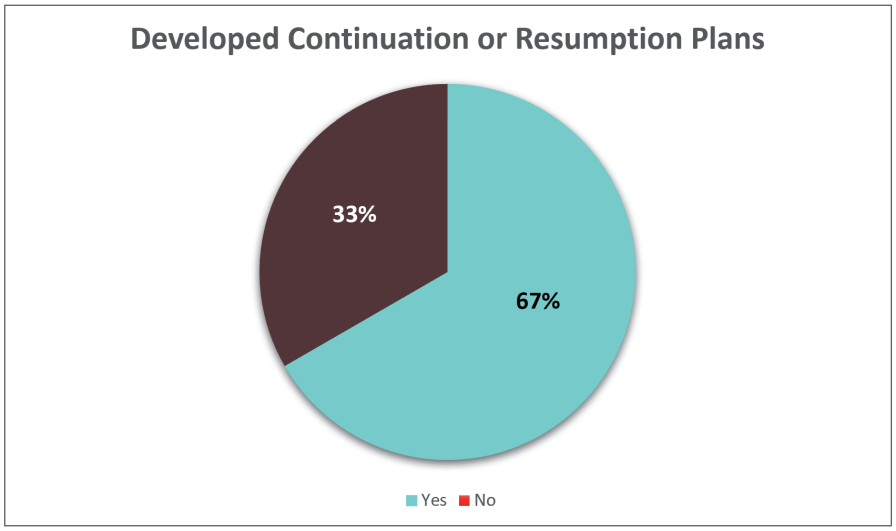
One interesting area we found is how Financial Institutions are engaging the business and the First Line of Defence in the assessment of resilience of third-party service provision as opposed to specialist functions such as Procurement and Information Security. This is being tackled by:

- Enhanced RCSA (Risk Control Self-Assessment) Programs
- Adapted Group Sourcing model
- Enhanced Procurement model
- Directly by the Business/First Line (calling on specialist functions)

3. Linkage between Risk and Crisis management

Here we examined the following:

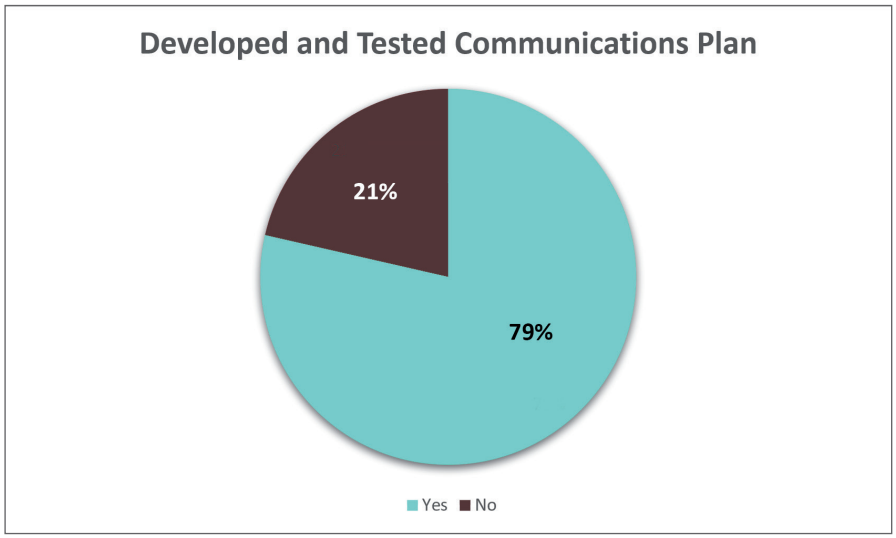
- Resumption of business services plan
- Communications Plan
- Business Model Review
- Operational Resilience review post Covid-19



Resumption of business services plan

We then asked if plans had been developed to enable continuation or resumption of business services when disruptions occurred in accordance with agreed impact tolerances

This was surprising that there are still Financial Institutions who have not developed plans for this. Effective incident and response management requires a clear linkage between Risk Management and Crisis Management plus a feedback loop. As part of this framework, consideration should also be given to tools that support dynamic Business Decision Management (BDM),harnessing Enterprise data and business logic to support real-time automated decisioning where response times are not measured in hours or days and risk vectors can be flexed dependent on potential detriment to the business, customers or market.



Communications Plan

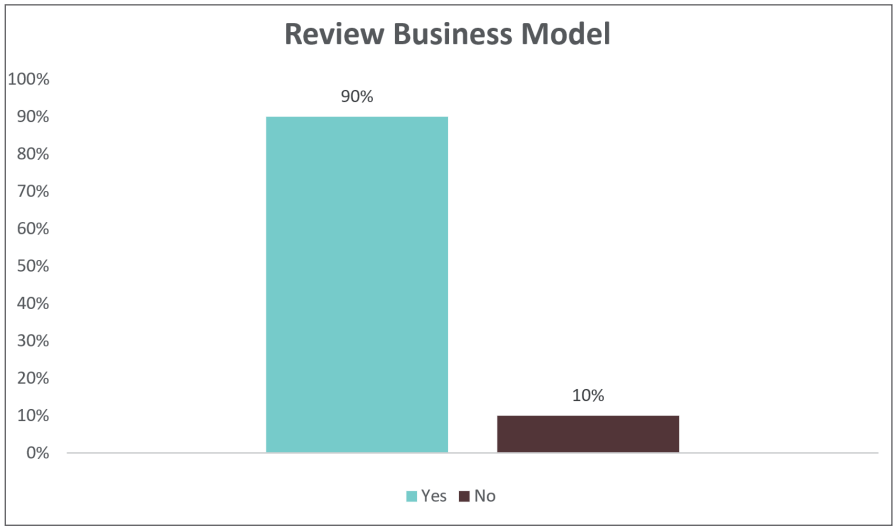
Moving to the area of communications plans we asked if Financial Institutions have developed and tested one in the event of an incident and stakeholder maps to ensure all key parties are communicated with, including third-parties, regulators, internal, media and clients

Whilst it is reassuring to see that most have, it is of some concern that this is not higher.

Business Model Review

Given the disruptive effect of Covid-19, we asked if Financial Institutions are planning to reassess inherent and residual risk in light of Digital adoption, remote working, and Cloud migration (for example):

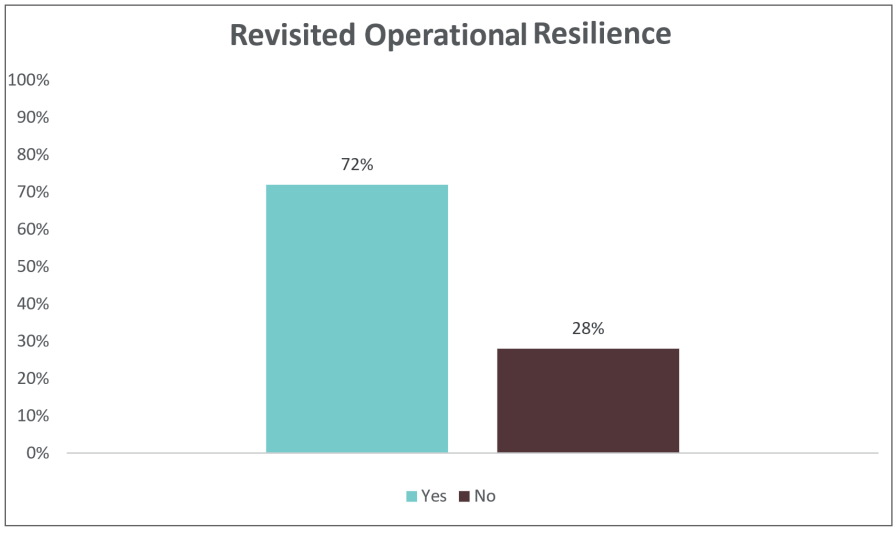
This level of review is to be expected. Across the market financial institutions are re-appraising their Real Estate footprint and re-purposing / reducing where appropriate. This extends to Data Centre strategy given the use of Cloud services to support remote working. It is unlikely that we will see a wholesale return to the way of working pre-COVID. Institutions are reviewing business models at a functional level to determine office versus remote working.



Operational Resilience review post Covid-19

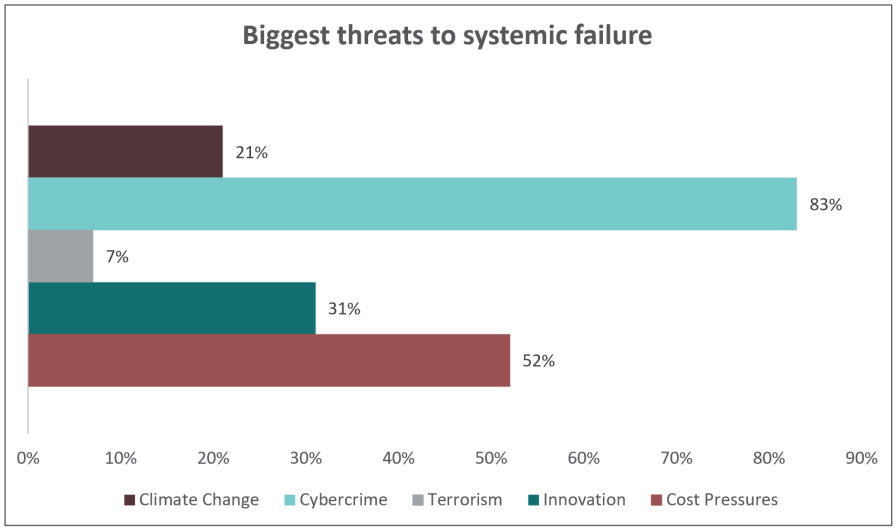
Given how significant Covid-19 has been as an event, we wanted to see Financial Institutions had revisited how they looked at Operational Resilience:

This is not surprising that the vast majority have revisited it.



4. Technology and how stable and secure it is

In this section we focused on what Financial Institutions thought were the biggest threats to systemic failure.



With all the recent Cybercrime incidents it was not surprising that this was the main area. Cost Pressures were next. Although Climate Change was not seen by many, we think this will increase in the future. Other areas that were mentioned included:

- Third Party Risk
- Emerging Risks
- Failure of regulators to directly address concentration risks rather than leaving up to individual firms
- Concentration and reliance on service providers (e.g. AWS)

5. Operational Resilience Framework

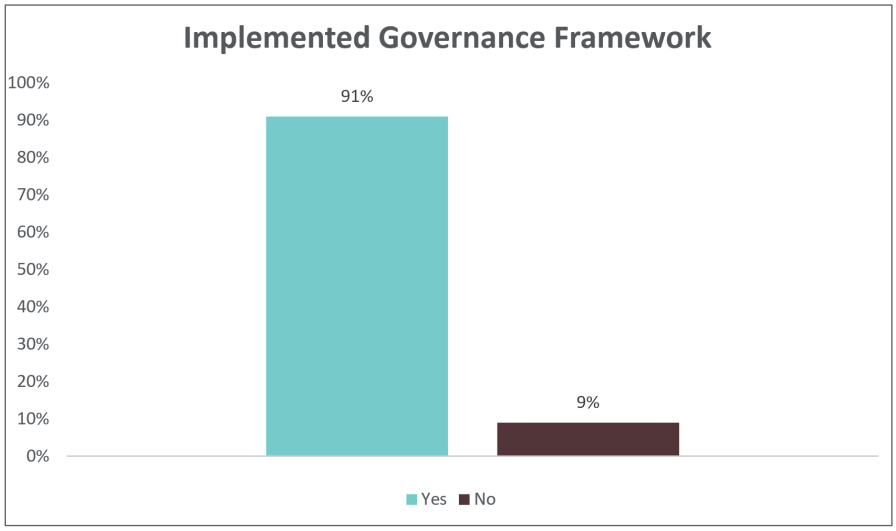
We looked at a number of aspects here including:

- Governance Framework
- Ownership of Operational Resilience Framework
- Allocation of roles and responsibilities
- Operations Resilience Areas

Governance Framework

We examined if Financial Institutions have implemented a governance framework to identify, assess, monitor, and report inherent and residual risks within the Board approved risk appetite:

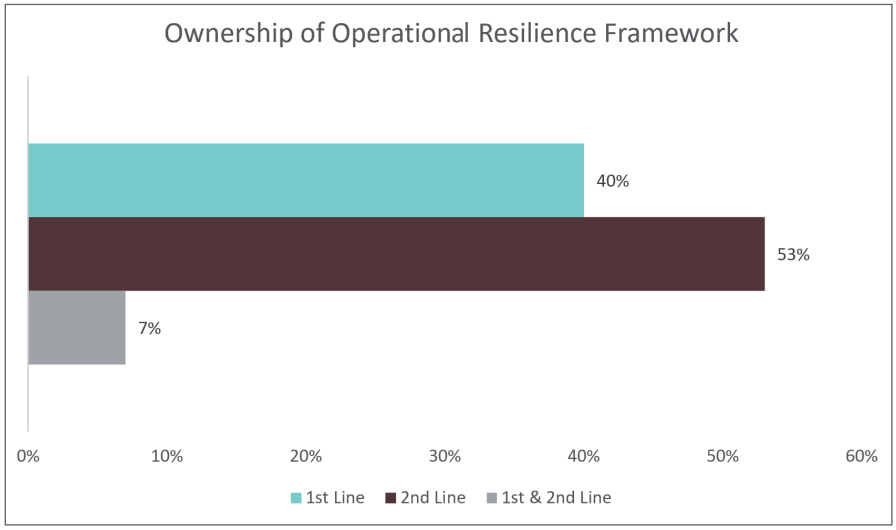
Given the importance of this it was not surprising that most Financial Institutions have implemented it. Effective Operational Resilience combines oversight for a number of key components under a single over-arching governance framework. The Operational Resilience framework must be subject to continual review, test and challenge to create a dynamic continuous feedback loop. This ensures business critical services can be delivered within impact tolerances during periods of stress and crisis without causing detriment to clients, financial impact to the business or increasing systemic risk to the wider market.

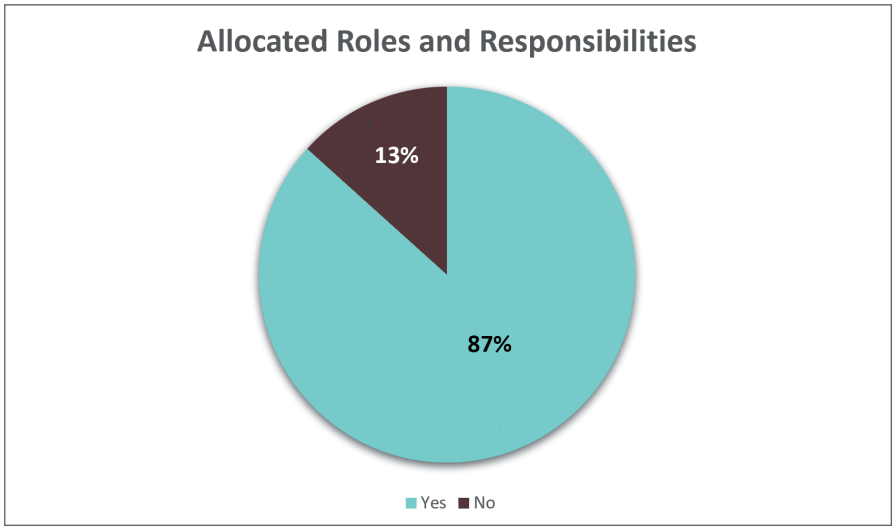


Ownership of Operational Resilience Framework

We now explored where the ownership of the Operational Resilience framework occurred (1st or 2nd line?)

Financial Institutions are split into where this should reside.

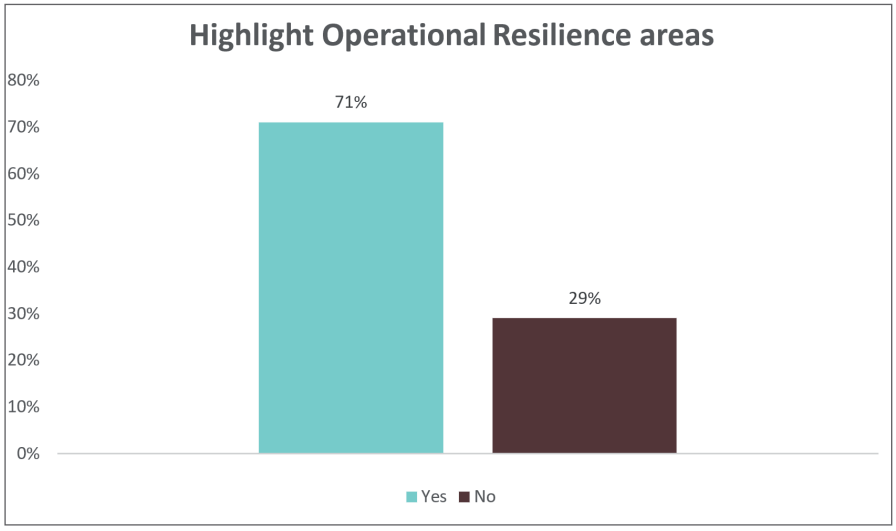




Allocation of roles and responsibilities

This next section looked at if Financial Institutions have allocated roles, accountabilities and responsibilities including third parties, for responding to incidents:

Not surprisingly most of the Financial Institutions have implemented this.



Operational Resilience Areas

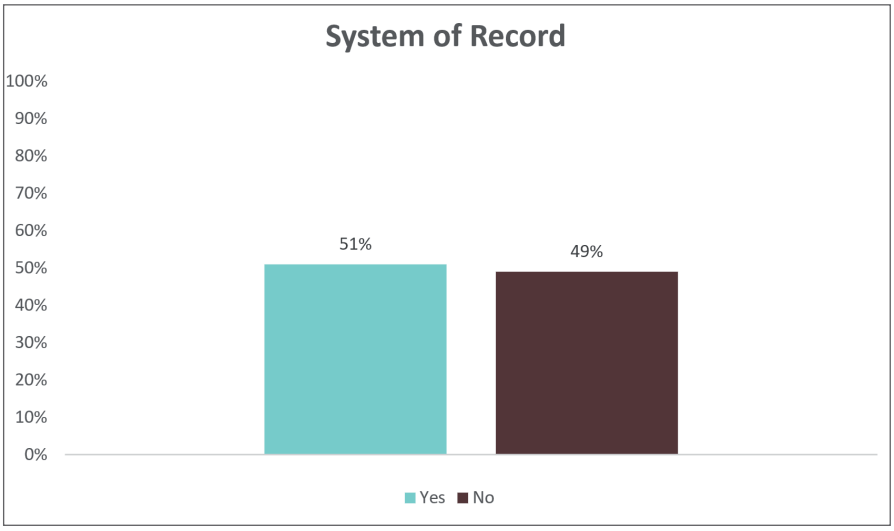
Finally, we determined if this specifically highlights Operational Resilience areas:

This showed that some Financial Institutions still have a way to go to focusing on Operational Resilience within their framework.

6. Management Information and metrics

Looking at where information is kept, we asked if the Financial Institutions have a system(s) of record to support Operational Resilience.

Again, this was surprising that nearly half do not have one. Regulators will expect Operational Resilience to be supported by a system of record. This support may be available from existing systems, databases or a dedicated solution may need to be considered which will ideally integrate to existing frameworks and information. Key considerations are set out below.



1) Functionality

- An 'Operational resilience module' which could either be standalone or integrate with a GRC or other existing systems
- A library of relevant business services with the ability to score their materiality against: Consumers, Markets, Firm Safety and Soundness and Financial Stability
- A library of resources (people, process, tech, facilities, third parties, info) with the ability to link to important business services
- Ability to set multiple impact tolerances for each important business service (e.g. 24-hour duration)
- Ability to map end-to-end important business services and required resources to identify potential vulnerabilities
- Scenario testing to identify vulnerabilities to remaining within tolerance.

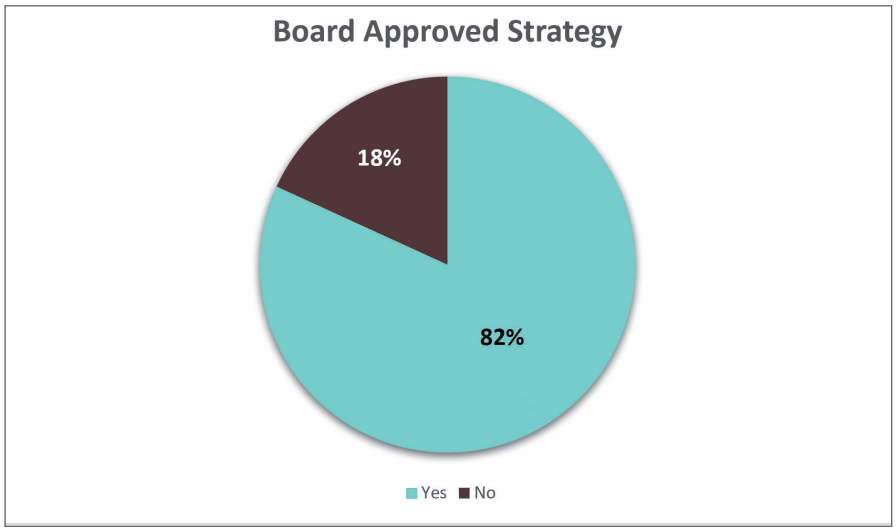
2) Reporting, Monitoring & Management Information

- Ability to link important business services to existing or new key metrics to act as warning indicators if the ability to recover within impact tolerances may be threatened
- Reports and MI including dashboards to provide summary and detailed oversight of the status of SLA's Operational resilience
- Creation of important inputs required for the annual self-assessment to be signed-off by the Board - a standard report can be designed with the required information to be extracted from the system

7. Overall strategy

This section focuses on overall strategy looking at a number of focus areas:

- Board Approved Strategy
- Board Member Accountability
- Senior Level Responsibility if not at Board level
- Level of Awareness
- Third-Party service providers and scenario tests
- Working from home



Board Approved Strategy

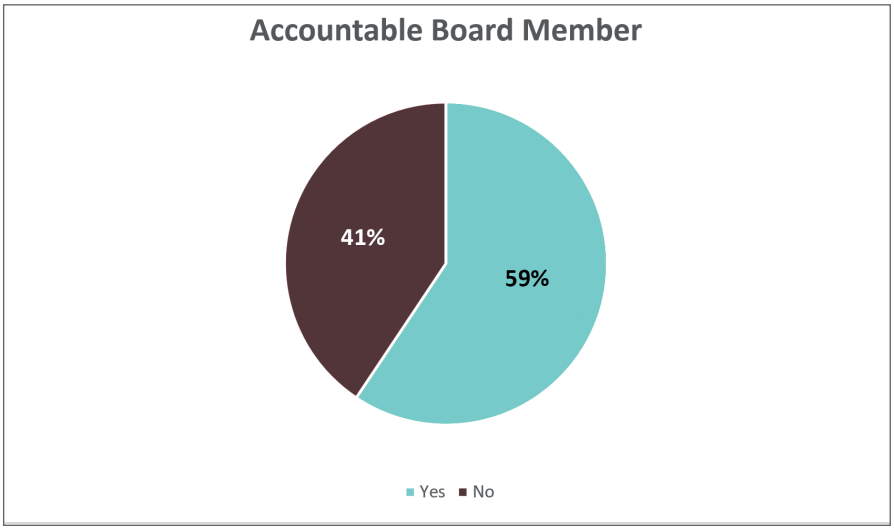
We asked if Financial Institutions have a Board approved strategy to build Operational Resilience, in line with business objectives and the risk environment.

The results show a good percentage; however, this is to be expected with recent events as Financial Institutions realise that Operational Resilience must become part of the DNA of the firm. To achieve this change requires a clear and practical vision allied to an achievable implementation plan, sponsored by the Board, to deliver in a realistic timescale. The result of the change must be to equip the Board with the governance and oversight capability required to practice and demonstrate effective management of operations resilience across the most important business services offered to customers and clients. The strategy must also trigger, and then maintain, an organisation-wide adoption of resilience as a core value in service design, Operational delivery and in the capability to respond to adverse events as and when they occur.

Board Member Accountability

We next looked at whether Financial Institutions had identified a Board member with accountability for Operational Resilience.

Given the importance of Operational Resilience that is seen in this survey it was surprising that this was not higher. Operational Resilience should build on components already in place to deliver a holistic, inter-connected governance structure. Data must be curated to align MI to important business services, allowing the Board and Senior Management to effectively challenge the organisation. The Board and key stakeholders must work together to plan and respond to scenarios, taking in to account the inter-dependencies that transcend the organisation model.

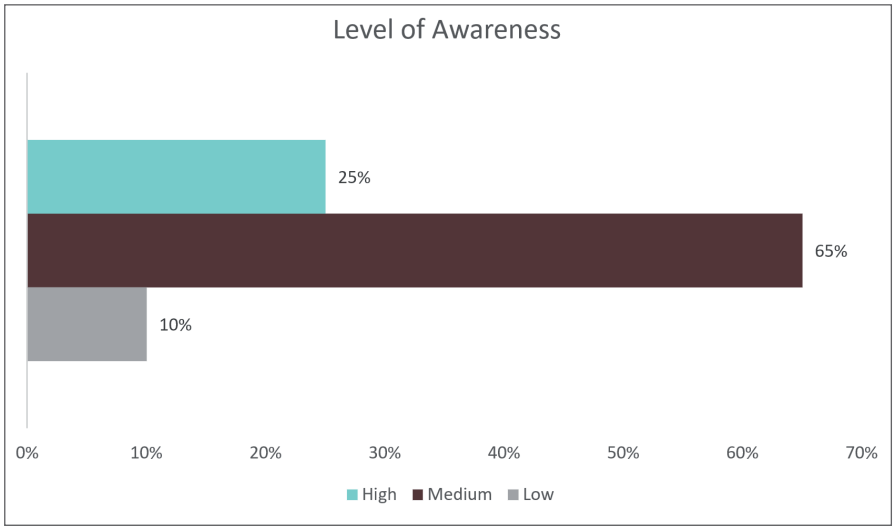


Senior Level Responsibility if not at Board level

Here we asked if there is not someone accountable at the board level, is there someone who is under the SMR regime who is responsible and if so who? Generally, the answer was someone with SMF 24 level of responsibility (7 specifically mentioned this) along with a couple of SMF 4's. Specific roles mentioned included:

- COO (6)
- CRO (2)
- CEO (1)
- Head of Business Unit (1)
- CTO (1)

Accountability for Operational Resilience should reside with the SMF24 executive to drive Operational Resilience top-down across the organisation. It should also be noted that accountability for material outsourcing as defined by the EBA, cannot be outsourced. The CEO is accountable and should delegate this accountability through the SMCR regime to the SMF24. It is a critical executive role.



Level of Awareness

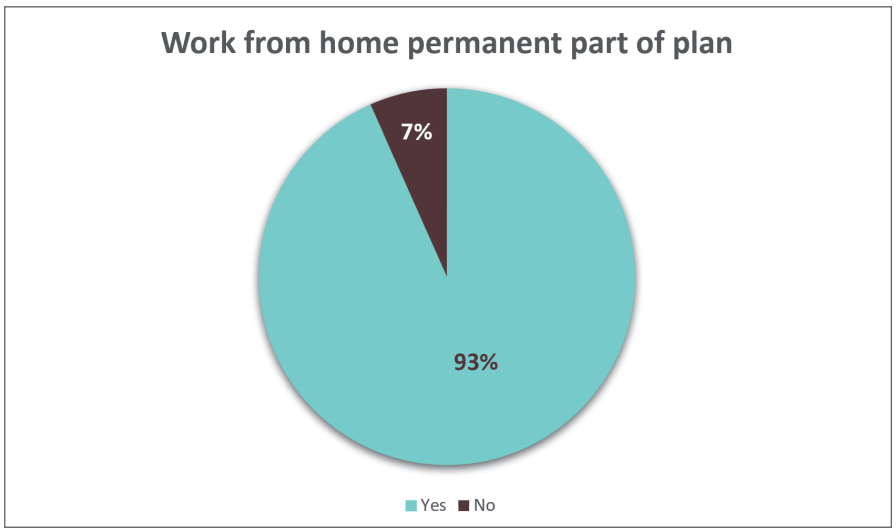
Next, we examined what is the level of awareness through the whole organisation (not just senior management) on Operational Resilience.

Whilst there were a relatively low number of Financial Institutions with a high level of awareness, we expect for this to increase going forward. A Communications strategy is key as is training and awareness. Ultimately, Operational Resilience is a mindset and as such must be embedded in ways of working, culture and behaviours. Similarly, thinking needs to reorientate to client service and outcomes. This is a very different approach to BCP and DR.

Third-Party service providers and scenario tests

Finally, we looked at how Financial Institutions are engaging with third-party service providers to be part of scenario tests. Although a lot of people said that this is still being defined there were a few strategies:

- Include them in Crisis Management exercises
- Through partnership with joint exercises, both physical and tabletop exercises
- Key third party suppliers will be asked to participate in desktop scenarios, as well as providing evidence of their own testing.



Working from home

One of the hottest areas to emerge from the Covid-19 event is working from home. We looked at if this is now a permanent part of Financial Institutions resilience plans.

Not surprisingly most respondents said it was and it will be interesting to see if this is still the case over time.

8. Self-assessment and lessons learned

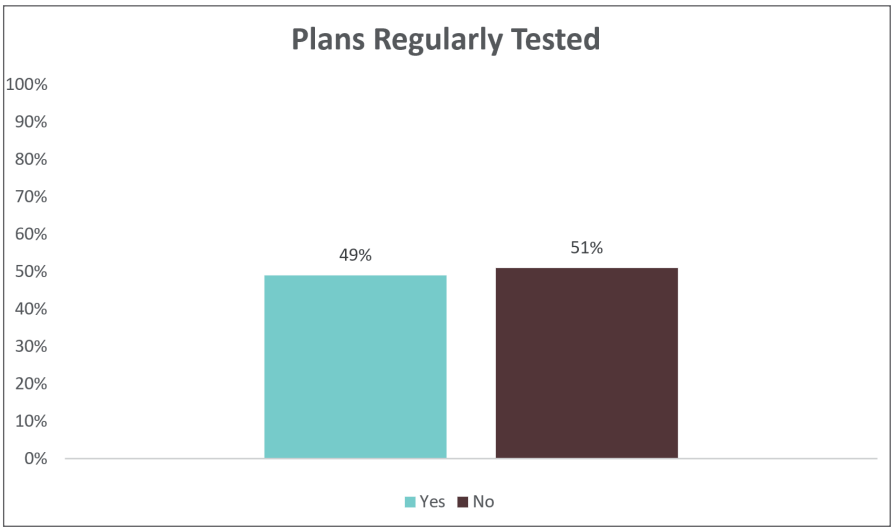
This final section looks at the different areas of self-assessment and lessons learned. If covers the following:

- Testing of plans
- Lessons learnt most
- Testing Operational Resilience Scenarios
- Refreshing Resilience Scenarios
- Overall Level of Readiness

Testing of plans

It is important these plans are regularly tested so we asked if they are and if the outcomes form part of a self-assessment programme.

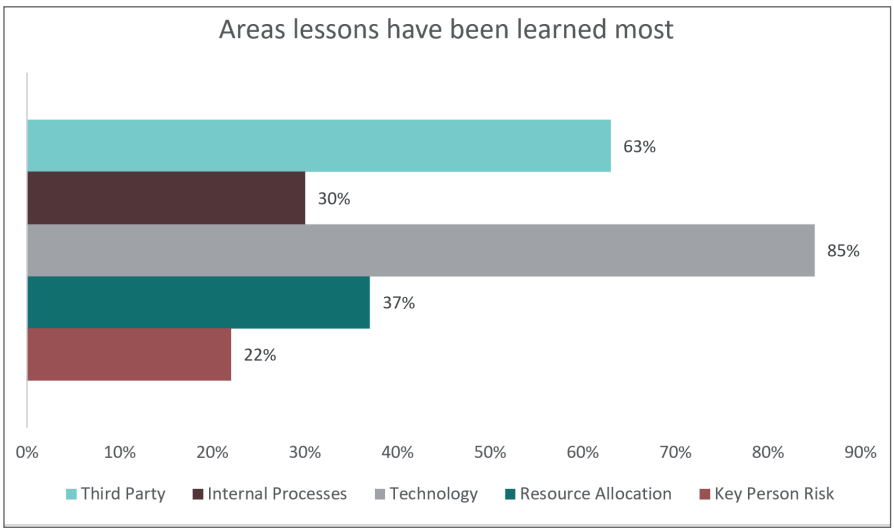
It was surprising that nearly half were not tested.



Lessons learnt most

Next, we wanted to see in which areas lessons have been learnt the most.

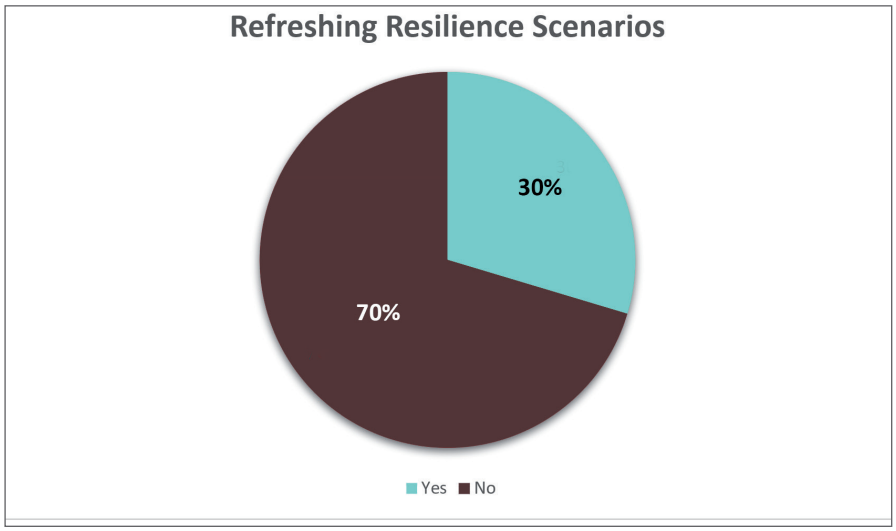
As expected, technology is the front runner with the other significant one being third party reliance/exposure.



Testing Operational Resilience Scenarios

Whilst a lot of Financial Institutions have Operations Risk Scenarios, we asked what measures if any are being adopted to test them (use of software such as Chaos Monkey and/or development of gamification techniques for example). The vast majority had nothing will only a few mentioning a plan or methodology:

- Will be using scenario and what if based workshops
- Once the important business services are identified, those will be stress tested via scenario analysis, leveraging existing playbooks
- Chaos Monkey has been in place for some time. Increasing use of scenario analysis.
- Internal scenario gaming
- Live testing



Refreshing Resilience Scenarios

To ensure that resilience scenarios remain severe and plausible we asked if Financial Institutions have a framework in place for systematically generating and/or refreshing them.

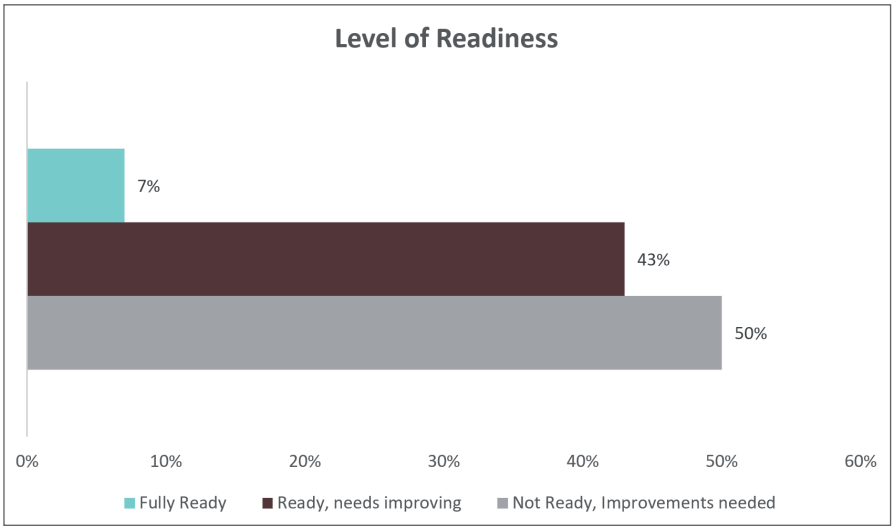
This was quite surprising that very few Financial Institutions have this in place.

Overall Level of Readiness

Given all the above we asked for Financial Institutions to assess what their overall level of readiness is to conform (attest and evidence) with Operational Resilience?

Given the recent big changes because of Covid-19 it was not surprising that very few were fully ready. They are still waiting for the regulations to be finalised. Currently areas that could be improved included:

- More regular scenario testing
- End to End client journey testing
- Business Continuity
- Resilience and embedded recovery with third parties



Conclusion

Whilst Operational Resilience is seen as a key part of a Financial Institutions strategy, there is a strong regulatory drive in this area as well. The deadline for responses to the current Bank and PRA consultations on "Building Operational Resilience: Impact tolerances for important business services" and the PRA consultation on "Outsourcing and third party risk management" will, in line with the FCA, be extended to 1 October 2020. The current working assumption is that regulations will come in to force during Q2 next year.

All regulated firms need to take time to review and understand the Regulators' proposals and what they will mean for their business and respond where appropriate before the Regulators decide upon the final policy. Embedding Operational Resilience is complex given the fact that business services often extend across Lines of Business, legal entities, geographies and third parties. The case for action is now.



TORI
Experience. The difference.

HTF

HTF Research
19 Shaftesbury Court
2 Alderney Mews
London SE1 4JR

info@htfcorporate.com
www.htfcorporate.com

HTF and the HTF logo are trademarks or registered trademarks of HTF Group in the United Kingdom and in other territories. Other company, product and service names are the property of their respective owners. This publication is issued for general guidance only. Copyright © 2020 HTF Research.