CAPCO

TAKING THE TEMPERATURE:

HOW TESTING IS ESSENTIAL TO OPERATIONAL RESILIENCE

TAKING THE TEMPERATURE: HOW TESTING IS ESSENTIAL TO OPERATIONAL RESILIENCE

> *Testing leads to failure, and failure leads to understanding.*
>
> **Bert Rutan,**
> **designer of the Virgin Starship and**
> **winner of the Ansari X Prize.**

Testing is vital to prove that a system works or an object performs as expected and it can also be used to better understand the properties of that system or object and how it responds to changes to its environment. In an operational resilience setting, all these considerations are relevant when assessing how prepared an organisation is in coping with disruptive events. The new UK Operational Resilience regulation[1,2] puts significant emphasis on testing to give boards and executives confidence that their firms are resilient.

We see the key questions that UK regulators are looking to have answered by conducting testing are:

1. **Scenario testing.** How do important business services (IBSs) cope with severe but plausible events (based on the information captured in the process maps). Are impact tolerances breached?
2. **Process map accuracy.** How accurate are the back-up plans in the process map as this impacts the accuracy of scenario testing?
3. **Effectiveness.** How effective are the incident response capabilities of the firm in terms of information flows, decision-making and carrying out the necessary actions to address the disruption?

In this paper, we investigate how firms should approach each of these questions and what is required to answer them effectively. It is also worth noting that the UK Financial Conduct Authority policy statement on operational resilience[2] lists both scenario testing and testing as distinct topics to be covered as part of a firm's annual self-assessment.

SCENARIO TESTING

UK regulations require firms to remain within impact tolerances for each of their IBSs when severe but plausible events are experienced. Given that some of the most significant disruption is caused by relatively innocuous events, such as misconfigured data centres, we define as 'severe' those events that could have a severe impact on clients, market stability or the soundness of the firm if no mitigating action is taken. The regulators indicate that 'plausible' covers those events that have already been experienced by or impacted organisations globally. This is helpful in limiting the number of potential scenarios in scope.

Guidance put out by the US Federal Reserve Bank of New York[3] in October 2020 mentions that testing should be carried out semi-independently of the teams tasked with maintaining delivery processes. We view this as a sensible way of ensuring the effectiveness of any testing. We would see scenario testing as being the responsibility of the central operational resilience team or the operational risk function. It is worth noting that the Hong Kong Monetary Authority in their Supervisory Policy Manual[4] proposed that it should be the responsibility of the board to select the scenario to be applied. This underlines the importance of the selection of scenarios to be applied.

Firms should select scenarios that cover a range of incident types in line with the FCA's guidance (SYSC 15A.5.6)[5] (see below). Firms can apply the same event to multiple IBSs and we anticipate that, as firms carry out scenario testing over time, they will work through the possible disruptive events that they face.

1. Corruption, deletion or manipulation of data critical to the delivery of important business services
2. Unavailability of facilities or key people
3. Unavailability of third-party services that are critical to the delivery of its important business services
4. Disruption to other market participants, where applicable
5. Loss or reduced provision of technology underpinning the delivery of important business services.

In the UK consultation papers, there is an example of an IBS that is tested across four different events to assess its resilience. We believe that four scenarios is about right in terms of surfacing issues given the number of IBSs that firms have identified.

We recommend that firms adopt a three-phase approach to scenario testing, as illustrated below:

Three-phase approach

Creating the scenario. The starting point is to select the event that will be applied for the test. We recommend that firms maintain a material risk inventory that includes possible events that the firm sees as having the potential to disrupt services and that this is maintained within operational risk as the golden source. This ensures that the areas that need to be prepared to respond to events (BCP, cybersecurity, physical security, etc) are all aligned. This also answers the question of what events the firm has considered and for which preparations have been made. This inventory needs to be specific enough to allow plans to be made. For example, in the case of a cyberattack, it would need to list the exact nature (e.g., a distributed denial of service (DDoS) attack) and for physical events it should cover the location as well as the nature (e.g., a hurricane in Florida.) This is the logical extension of the horizon scanning that operational risk should coordinate on a regular basis.

Assessing the impact on each element. Once the scenario has been decided, the next step is to identify how it will impact each element of the delivery process, at a granular level using the information in the process maps, as well as how long recovery would take for each element. Understanding the length and extent of possible disruptions by reference to external events, not just in financial services but across all industries, creates a neat proxy for potential outage or unavailability in firms' own scenarios. These disruptions can test resilience far beyond actual events experienced by a firm.

End-to-end review. Once the impact on each of the elements in the delivery process is known, the end-to-end impact can be calculated and compared to the impact tolerance with an assessment as to whether the test is a pass or fail.

The scenario testing is based on the information in the process maps including the recovery and failover plans/timings. Currently, it is typical for firms to rely heavily on SMEs to run scenario tests.

Execution

As part of their policy statement on operational resilience the PRA expect that firms will become more sophisticated in their approach and indicate three increasing levels:

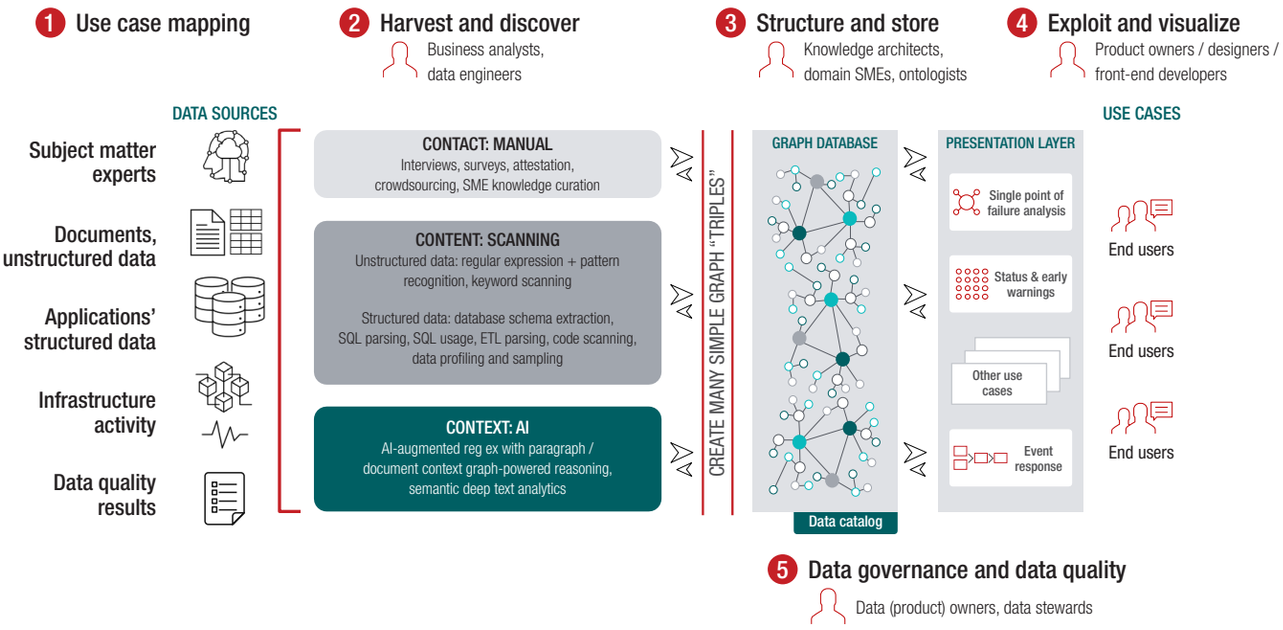
- Paper-based scenario testing
- Simulation
- End-to-end testing.

Paper-based scenario testing. Firms typically use offline, paper-based scenario tests with more advanced tests that look at how they can improve the effectiveness of the testing while also reduce the resources required to carry out the tests. This is leading firms to look at simulation-based approaches that run the tests automatically online with limited manual intervention. We will explore one of the options:

Simulation: the digital twin. Imagine an online, living simulation of the delivery processes for your IBSs that captures the true complexity of your operating environments and that can be reconfigured as required to understand the impact of disruption. Imagine being able to run multiple scenarios automatically without a room full of SMEs. Imagine being able to evaluate actions to address a crisis in real time to understand the downstream effects. This is what a digital twin based on graph technology can deliver.

Graph databases feature nodes (e.g., process steps) and edges (how those steps are linked together) as a way to capture and represent myriad interdependencies. The same technology underpins satellite navigation systems, providing both the flexibility to adapt to changes and capturing the complexity of the real world. The technology is largely self-learning, with limited manual curating required, and it can interrogate documents, tabular/structured data and even the firm's activity (e.g., log files).

In mapping the interconnectivity and complexity within delivery processes this way, a richer representation of the process can be created in a more efficient fashion than traditional, largely manual methods. This high-fidelity map is also easier to modify to understand the impact of disruptive events, both when testing against scenarios and when testing solutions to crises. More broadly, the digital twin has a part to play in process design and optimisation well beyond operational resilience.



End-to-end testing

The third type of testing that the regulators refer to is live, end-to-end testing. While this is certainly possible, we would argue that this is not the most cost-effective method of ensuring that delivery processes are resilient due to the sheer amount of time required to formulate and execute this sort of testing, which inevitably leads to testing only a very limited number of scenarios. Our preferred alternative is to rehearse the decision-making apparatus, and the individuals who are responsible for executing the recovery actions, separately to scenario testing. This gives a better outcome by ensuring team members are exposed to a broad range of scenarios. We will cover this in the next section.

VALIDATING THE RECOVERY INFORMATION IN PROCESS MAPS

Scenario testing is dependent on the recovery information contained within the maps of those processes delivering IBSs. To be confident that these are accurate, the recovery point and time objectives (RPOs and RTOs) for each process element need to be tested against the full range of potential events contained within the material risk inventory maintained by the firm. This should include cyberattacks that breach the firm's defences and should also take into account the time needed to identify the problem and decide on the appropriate course of action, as well as the time to remediate.

Process elements should be prioritised for testing in terms of the impact on the end-to-end process of their failure. We recommend that validation testing is carried out at least annually for the high-priority elements. This testing will not only give the firm confidence that they are indeed as resilient as they believe they are, but will also train the individuals tasked with investigations and carrying out recovery actions. By default it also identifies any issues with the actions in incident recovery playbooks.

Delivery process testing. Based on our experience, testing single applications, processes, units or connections fails to provide a realistic depiction of what would happen in a live production environment. This means, without end-to-end testing of delivery processes, the first time a firm will experience the true impact of load and capacity challenges will be in real life. While these exercises take time to set up, they do give a much more realistic view of the time needed to recover.

Third parties. Many firms make extensive use of third parties to deliver their IBSs. In our paper 'Getting the Mix Right – a Look at the Issues Around Third Party Outsourcing[6]' we highlighted that third parties that perform material outsourced functions should be treated in fundamentally the same way as if those processes were being carried out in-house. This includes testing, so we would recommend that firms:

A. Include in detail within their process maps the recovery information of third parties carrying out material outsourcing and factor this into their scenario tests

B. Review the third parties' recovery actions and the evidence that these have been tested

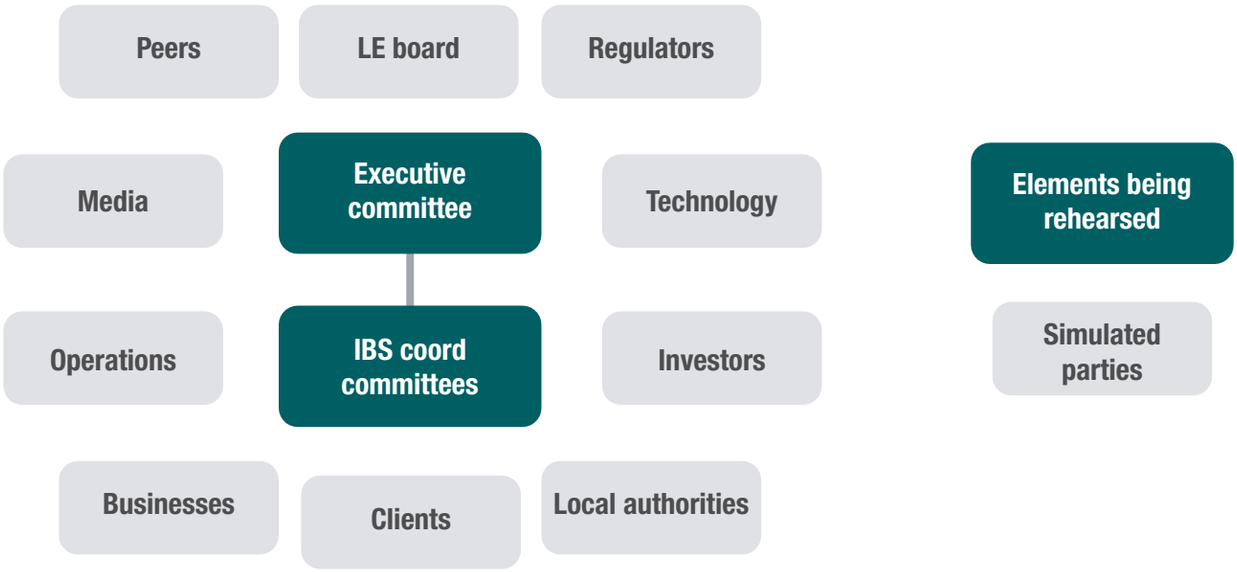
C. Include the most critical third parties in the rehearsal of the incident response apparatus review.

TESTING EFFECTIVENESS – REHEARSING THE RESPONSE

Testing the decision makers

Most firms have a well-established incident response apparatus to make and challenge decisions – particularly in light of COVID-19. Our paper 'Excelling in a Crisis'7 set out how these could be optimised. Part of the approach includes rigorous rehearsal once executives have been trained in the basics of crisis management and their role during an incident.

Initially, testing should be run in slow time, with frequent pauses to reinforce lessons; once executives are more experienced, to maximise realism, this can progress to no-notice tests with 'knowledgeable actors' role-playing external parties outside the groups being exercised. The illustration below is a representation of how it could be organised:



Exercises such as these need careful preparation to get the most out of them. Scenarios should be meticulously developed, incorporating realistic signals and incoming information, with careful observation from the exercise coordinators to capture what went well and areas for improvement. There should be a 'main events' list that outlines the progression of the exercise inputs with timings. Once the exercise is over, the actions taken should be reviewed thoroughly with participants to ensure that lessons are learned and applied. While some firms may feel that the fact they are dealing with situations on a regular basis obviates the need to rehearse, in reality it is unlikely that they will encounter the full spectrum of potential events if they were to rely on this approach in the long term.

We include those in technology who are responsible for identifying and investigating disruption as well as providing solutions in our definition of decision makers. These individuals should be tested using simulations of scenarios that they would face in a live event, with the exercise treated in exactly the same way as the executive response.

CONCLUSION

“Train hard, fight easy.”

Alexander Suvorov,
celebrated 19th century
Russian military commander

The current operating environment for firms encompasses a wide range of potential threats that could disrupt the services that they offer, with implications for their clients, their revenues and their reputations. In purely practical terms, it is impossible for firms to prepare for every single one of these eventualities, but firms can gain both valuable hands-on experience and confidence around their level of resilience via rigorous testing across a broad range of threats.

We have shown how firms can practically carry out testing in both an effective and efficient manner by breaking the testing down into elements followed up by a comprehensive ‘lessons learned’ review. If carried out rigorously and led from the top. firms can gain assurances of and improve their operational resilience.

At the end of the day, there are no shortcuts to resilience.

REFERENCES

1. PRA PS6/21 Operational Resilience: Impact tolerances for important business services. https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/policy-statement/2021/march/ps621.pdf?la=en&hash=A15AE3F7E18CA731ACD30B34DF3A5EA487A9FC11

2. FCA PS21/3 Building operational resilience: Feedback to CP 19/32 and final rules. https://www.fca.org.uk/publication/policy/ps21-3-operational-resilience.pdf

3. FRBNY et al. Sound Practices to Strengthen Operational Resilience. https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20201030a1.pdf

4. HKMA SPM OR-2 Operational Resilience. https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/OR-2-20211222.pdf

5. FCA Handbook SYSC 15a.5 Scenario Testing. https://www.handbook.fca.org.uk/handbook/SYSC/15A/5.html?date=2022-03-31

6. Capco 'Getting the Mix Right – a Look at the Issues Around Third Party Outsourcing and Operational Resilience'. https://www.capco.com/Intelligence/Capco-Intelligence/A-Look-At-The-Issues-Around-Outsourcing-And-Operational-Resilience

7. Capco 'Excelling in a Crisis – Lessons for Financial Services from the Military Approach to Crisis Management. https://www.capco.com/intelligence/capco-intelligence/operational-resilience-excelling-in-a-crisis

AUTHOR

Will Packard,
Operational Resilience Practice Lead, will.packard@capco.com

CONTACTS

Will Packard,
will.packard@capco.com

Lucinda Szebrat,
lucinda.szebrat@capco.com

ABOUT CAPCO

Capco, a Wipro company, is a global technology and management consultancy specializing in driving digital transformation in the financial services industry. With a growing client portfolio comprising of over 100 global organizations, Capco operates at the intersection of business and technology by combining innovative thinking with unrivalled industry knowledge to deliver end-to-end data-driven solutions and fast-track digital initiatives for banking and payments, capital markets, wealth and asset management, insurance, and the energy sector. Capco's cutting-edge ingenuity is brought to life through its Innovation Labs and award-winning Be Yourself At Work culture and diverse talent.

To learn more, visit www.capco.com or follow us on Twitter, Facebook, YouTube, LinkedIn Instagram, and Xing.

WORLDWIDE OFFICES

APAC
Bangalore
Bangkok
Gurgaon
Hong Kong
Kuala Lumpur
Mumbai
Pune
Singapore

EUROPE
Berlin
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
London
Munich
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA
Charlotte
Chicago
Dallas
Hartford
Houston
New York
Orlando
Toronto
Tysons Corner
Washington, DC

SOUTH AMERICA
São Paulo

WWW.CAPCO.COM

CAPCO
a wipro company

JN_3828