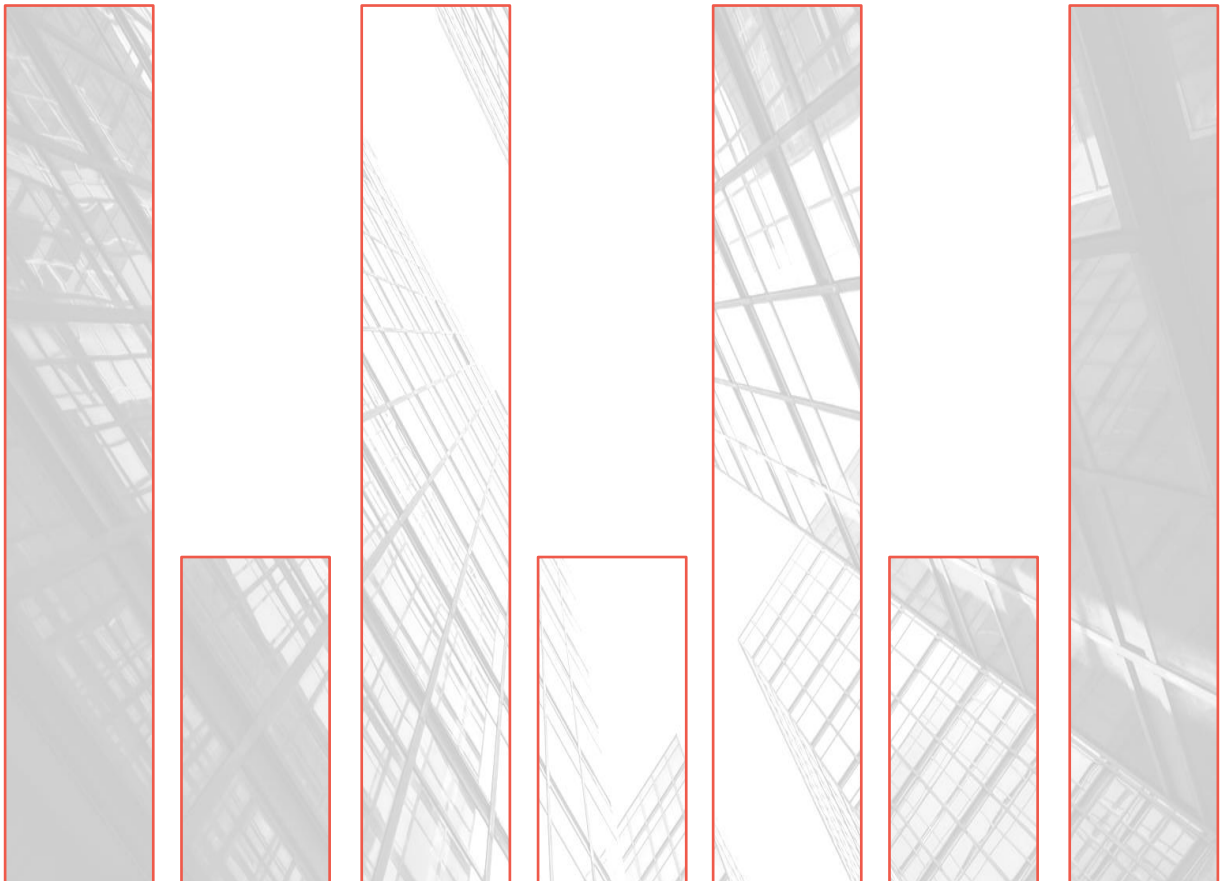
CMORG
CROSS MARKET OPERATIONAL RESILIENCE GROUP

Collaborative Scenario Testing of Third Parties

Effective Practices

VERSION 1.0 | SEPTEMBER 2024 | TLP CLEAR



Contents

CMORG-endorsed capabilities (including good practice guidance, response frameworks and contingency tools) have been developed collectively by industry to support the operational resilience of the UK financial sector. The financial authorities support the development of these capabilities and collective efforts to improve sector resilience. However, their use is voluntary, and they do not constitute regulatory rules or supervisory expectations; as such, they may not necessarily represent formal endorsement by the authorities.

1 Executive Summary

Following the promulgation of the Operational Resilience regulations by UK financial regulators, the industry has been evolving its understanding of good practice in relation to scenario testing. A key element of scenario testing is the analysis of the impact caused by possible disruption to third party services provided to financial institutions (FIs) and Financial Market Infrastructure providers (FMIs) – collectively referred to in this paper as "financial firms". This requires close co-operation with the third parties concerned to understand their resilience posture and would potentially benefit from direct involvement of those third parties in scenario testing.

The Cross Market Operational Resilience Group (CMORG) has identified that there is opportunity to enhance the quality and application of scenario testing with third parties. This document is not designed to be an exhaustive or prescriptive approach to scenario testing with third parties, but to reflect and reinforce the current principles-based regulatory landscape; financial firms (both regulated and unregulated) are encouraged to continue to strive for excellence in their management of third party risk including in a range of demanding scenarios, up to and including those which may drive a stressed exit from a given third party.

This document, therefore, is designed to provide a set of principles and broad expectations of the industry on how scenario testing with third parties should be conducted. The guidance here is intended to be used by financial firms of all maturities as either a guidance for building a framework for scenario testing with third parties, or to act as a check point for established programs. Additionally, third parties to the financial sector should also consider the expectations, standards, and reporting requirements herein. Third parties to the financial sector should note forthcoming regulation that may more directly oversee and expect Operational Resilience standards of Critical Third Parties[1]. This best practice guidance, which is a result of cross industry collaboration, seeks to set good practice on scenario testing with third parties. These include, but are not limited to:

- Selection of scenarios,
- Expectations around evidence of resilience during scenario testing,
- Typical coverage of any scenario test report,
- Incorporation of third party scenario test obligations into contracts.

Noting that the regulatory environment is expanding, and financial firms are individually seeking to deepen their testing approaches, this good practice guidance is intended to drive a consistent approach. Following orientation with UK regulatory bodies, this guidance is also aligned to forthcoming regulation. Adoption of the principles herein are intended to provide a runway for third parties and financial firms to deepen scenario testing capabilities.

[1] Bank of England "CP 26/23: Critical Third Parties to the UK Financial Sector" and the European Union's "Digital Operational Resilience Act"

2 Background

2.1 ORCG

The Operational Resilience Collaboration Group (ORCG) is a sub-group of the CMORG, the primary venue for collective action between the private sector and public authorities in the UK's financial sector.

Established in 2019, the ORCG facilitates collaboration between financial firms that have a common interest in operational resilience, and to focus on shared problems that financial firms may not be able to address alone.

2.2 Remit of the Working Group

The Collaborative Third Party Scenario Testing working group (phase 2) follows on from a previous ORCG working group report[2] which explored collaborative scenario testing methodologies. This report provides further guidance for the conduct of scenario testing by third parties including scenario selection, evidential requirements and reporting formats. The report also summarises regulatory expectations regarding such scenario testing, as well as considering the interaction with the proposed critical third party (CTP) regime under the Financial Services and Markets Act (FSMA)[3].

2.3 Scope of Regulatory Expectations

The Operational Resilience regulations within the UK, set out by the Financial Conduct Authority[4] (FCA) and Prudential Regulation Authority[5] (PRA), establish a framework for the regulation of resilience across financial firms. In particular, they introduce the concept of Important Business Services (IBS) which if disrupted would cause intolerable levels of harm to the financial firm's clients or pose a risk to the soundness, stability or resilience of the UK financial system or the orderly operation of the financial markets. They also require financial firms to establish impact tolerances (ITOLs) which is the point at which such intolerable harm or risks materialise.

Financial firms are required to undertake scenario testing under the FCA regulation SYSC 15A.5.3R and PRA PS 2/22 to assess their ability to remain within ITOLs for its IBSs in the event of a severe but plausible disruption of its operations. In carrying out scenario testing, financial firms are also advised to consider scenarios (SYSC 15.A.5.6G) relating to the unavailability of third party services which are critical to the delivery of its IBSs.

[2] Collaborative Scenario Testing, CMORG, July 2023
[3] Financial Services and Markets Act 2000 as amended by the Financial Services and Markets Act 2023
[4] Financial Conduct Authority Handbook, Systems and Controls (SYSC) chapter
[5] PS 2/22, Operational Resilience and Operational Continuity in Resolution: CRR firms, Solvency II firms, and Financial Holding Companies, March 2022

SYS 15A.5.5G sets out regulatory expectations that financial firms which rely on a third party for the delivery of its important business services, will work with the third party to ensure the validity of the financial firm's scenario testing under SYSC 15A.5.3R. To the extent that the financial firm relies on the third party to carry out testing of the services provided by the third party to or on behalf of the financial firm, the financial firm should ensure the suitability of the methodologies, scenarios and considerations adopted by the third party in carrying out testing. The regulations also make it clear that the financial firm is ultimately responsible for the quality and accuracy of any testing carried out, whether by the financial firm or by a third party on its behalf.

The Bank of England (BoE) has provided further clarification[6] regarding its expectations of third party testing, including the following principles:

- Material third party contractual arrangements to include necessary measures to enable financial firms to gain assurance of third party resilience, including access to premises, the third party's own testing outcomes and incident data (in line with the outsourcing and third party risk management policy - OTPRM[7]);
- Third parties directly participate in testing where practicable, sharing relevant data and demonstrating resilience capabilities with the financial firm;
- Assessing the resilience of third party arrangements in line with its own assets under the financial firm's own control (in line with OTPRM policy section on due diligence);
- The financial firm considers all elements of response and recovery from a scenario that are in its control, even where there is a primary reliance on the third party for full recovery, e.g. Firm responsible for data integrity and quality following cyber incident;
- Testing includes a financial firm's ability to resume delivery of IBS within Impact Tolerance (ITOL) when the material third party service becomes unavailable.

While this paper focusses on the UK regulatory regime, consideration has been given to alignment with the EU's Digital Operational Resilience Act (DORA)[8]. DORA places an obligation on financial firms to periodically test appropriate Information and Communication Technology (ICT) business continuity plans, notably with regard to critical or important functions outsourced or contracted through arrangements with ICT third-party service providers (Article 11 clause 4). It also requires financial firms to include the following contract provisions when contracting with ICT third parties who support critical or important functions:

- Requirements for ICT third party service providers to implement and test business continuity plans (Article 30 clause 3(c));

[6] Operational Resilience Implementation: Testing assurance and building resilience, Bank of England briefing to ORCG, March 2024
[7] PRA Outsourcing and Third Party Risk Management Supervisory Statement, SS2/21
[8] Regulation (EU) 2022/2554 of 14th December 2022

- Right to monitor the ICT third party service provider's performance, including unrestricted rights of access, inspection and audit by the financial firm (Article 30 clause 3(e)(i)) and an obligation on the ICT third party service provider to fully co-operate during onsite inspections.

2.4 Interaction with Critical Third Party regimes

The BoE and FCA have consulted on the establishment of the CTP regime envisaged under section 312L (3) of the FSMA. It is expected that a limited number of third parties would meet the test set out in FSMA, namely that the failure in, or disruption to, the provision of services by the third party could threaten the stability of, or confidence in, the UK financial system. As part of the consultation the BoE and FCA suggest that CTPs may be required to undertake regular scenario testing in their own right, and that those requirements would be adapted from the requirements and expectations in the operational resilience framework for financial firms.

DORA also envisages a similar regime under Article 31 which allows for the designation of ICT third party service providers who are systemically important as CTPs, with an appropriate oversight and enforcement regime (including penalties of up to 1% of average daily worldwide turnover).

While the list of CTPs designated under DORA or the UK CTP regime have yet to be confirmed, it is likely that this will be a small subset of those third parties which financial firms collectively may regard as impacting the delivery of one or more of their IBS should they fail. For the purposes of this paper, we have therefore divided third parties into:

- Those who are will be formally designated as critical third parties by HM Treasury (HMT) under the FSMA – they will be referred to as CTPs in this report;
- Those who are not so designated, but nevertheless are key to the delivery of the IBSs of one or more financial firms – they will be referred to as Significant Third Parties (STP) in this report;
- Those who do not support the delivery of IBSs – which are outside the scope of this work – but may wish on a voluntary basis to embed aspects of the practices outlined in this report.

The focus of this report will be on STPs, although the practices in this report may also inform the further development of regulatory practices (including supervisory statements) relating to the CTP regime in the UK.

The report does not set criteria for the identification of STPs, with financial firms left to determine which suppliers meet this threshold. Nevertheless, we expect such suppliers will be considered as the highest risk suppliers in the supplier risk management framework of the financial firms who depend on them. Various terms such as: Tier 1 supplier, critical supplier, high risk supplier, important or super severe supplier may be attached to those suppliers by the respective financial firms. These suppliers may include: communication services,

managed IT services, trading platforms, market data providers, card processing and payment services, rating services, fintech and a range of other support providers.

Figure 1 provides a graphical representation of the different categories of third parties, as well as the commonality of the services provided across the financial sector by the third party. There is value in collective action where third parties are key to IBSs (STPs) and where there is sufficient commonality in services to allow for collective action and alignment of the requirements for evidence across the financial sector.

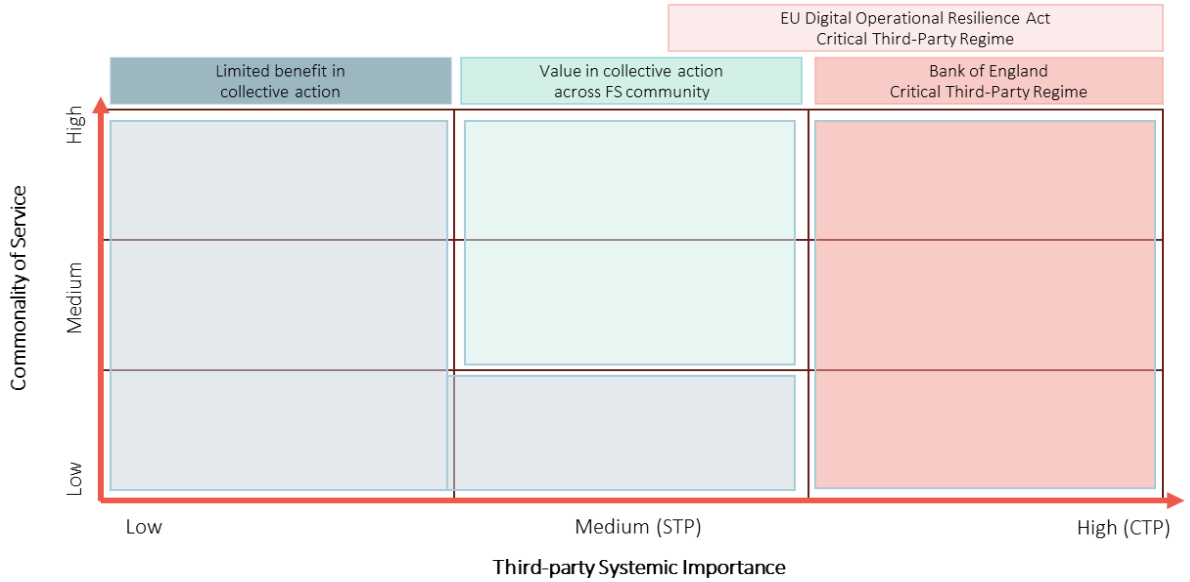


Figure 1: Different categories of third parties and degree of service commonality

2.5 Challenges of Implementation

In discussions with ORCG members, it has become clear that the evidential base provided by third parties to support scenario testing by FIs can be of varying quality and completeness. This is driven by a number of factors, including:

- Adoption of a conventional approach to business continuity and disaster recovery testing which does not fully consider the end-end service provision envisaged in the concept of an IBS within the operational resilience regulations;
- Failure to embed a scenario-based approach to testing, or consideration of a subset of the scenarios envisaged by the operational resilience regulations (e.g. focus on property, people and IT failure events rather than more complex cyber and data corruption scenarios);
- Third parties in the financial services sector are more conversant with the concept of scenario testing, while this approach may not be widely recognised in other sectors;
- Establishment of a different threshold for the definition of “severe but plausible” when defining scenarios leading to limitations or variations in the scope of testing;
- An assumption that protective controls are sufficient leading to exclusion of testing of certain events and the associated response and recovery processes;

- Commercial sensitivities regarding the disclosure of information regarding the resilience of services, including the results of testing and/or post incident reporting.

For their part, many third parties have noted the diverse approaches adopted by financial firms in requesting information on their resilience posture, resulting in additional workload in responding to multiple requests in varying formats. This issue was explored in the first phase of this work and remains relevant.

Together these challenges have resulted in significant gaps in the evidence base available to financial firms to underpin their own scenario testing, reducing the confidence in such testing and the ability of financial firms to deal with a major disruptive third party scenario. These gaps are particularly acute in sub-sectors such as market data provision, where commercial considerations have limited engagement by third parties.

As an illustration of the challenges encountered, the boxed entry overleaf provides a perspective from an ORCG member on their engagement with cloud services providers. Despite this perspective, the engagement with cloud service providers has been constructive and they have demonstrated a willingness to engage and understand the firms' perspectives and requirements. In other areas such as market data provision, there has been less constructive engagement to date raising questions over whether co-ordinated action by the financial sector may be required to gain the necessary levels of assurance over the resilience of services.

Reflections from engagement with Cloud Service Providers (CSPs)

"The information is there for you to see on our customer portal".

This has been a common response to requests for resilience related information when posed to CSPs. On the surface this is not an incorrect statement, there is an abundance of documentation available from the CSPs with regard to compliance. Compliance in this context refers on the most part to both industry standards and international regulatory requirements. The onus however is on the recipient to read through the volumes of information to find the data required that specifically relates to the resilience assurance requirements. But in the context of resilience across Financial Services, are we truly clear on what we are looking for and really need to evidence. And given the volume of data this could involve, what do we regard as the most effective/efficient method by which to format/receive this information.

Currently, there is an element of classic compliance from CSPs: ISO certifications, periodic evaluation reports listing 'passed' tests to complex methodologies providing phased approaches to resilience and incident management. But this provides only a starting point from which to start our own due diligence. The situation is improving, slowly. CSPs are looking at what CTP regulation may require and are looking to financial firms for support. Through continued dialogue with CSPs, collective understanding of 'the ask' is becoming clearer, but more work is required; the need for identify data to support concentration risk

analysis, understand critical cloud infrastructure and more detailed incident data to enable more informed scenario definition is beginning to emerge. What requires focus is the accuracy and timeliness of this data. From a CSPs perspective, the main concern remains provisioning such data requests in a consistent format since with growing focus on CSP resilience, the ability to satisfy/service all resilience enquiries from multiple clients will become onerous. Therefore, collaboration is key and by recent experience is proving effective in 'unlocking' previous perceptions of a lack of transparency.

2.6 Approach

This report sets out good practice related to STPs, including:

- The conduct of the scenario testing process itself, including commonly adopted methodologies, approaches and governance;
- Selection of appropriate scenarios to ensure adequate coverage, while also ensuring they are judged to be severe but plausible in nature;
- Expectations around evidence of recoverability during scenario testing, including the typical sources and types of evidence which may support assertions concerning resilience;
- Typical coverage of any scenario test report in terms of key elements, layout and analysis of findings;
- Incorporation of third party scenario test obligations into contracts;
- Next steps on further development of collaborative testing models.

Where appropriate, this advice builds on the practices set out in the CMORG Guidance for Firm Operational Resilience (GFOR)[9].

[9] Guidance for firm operational resilience, CMORG, Version 2, November 2023

3 Scenario Selection

3.1 Overview

This chapter of the report provides guidance on the selection and calibration of appropriate scenarios for a STPs to consider as part of its scenario testing process. Scenario selection seeks to identify a set of relevant severe but plausible scenarios (or extreme but plausible in the case of FMIs) which may impact the resilience of the key services which a STP provides to financial firms which in turn are critical to the delivery of one or more IBSs by those financial firms.

Financial firms are encouraged to communicate to STPs which of their services are key to the resilience of their IBSs, and where possible to give an indication of the recovery times they would expect for those key services. It should be noted that these recovery times may be shorter than the impact tolerances financial firms set for their IBS to allow for additional recovery times required by the financial firms post key service restoration.

Scenario selection and the calibration process should be informed by consideration of external threats, patterns of incidents, and known vulnerabilities with a focus on the resilience of those key services. Scenario selection should take into account an understanding of how key services are delivered, informed by an end-end mapping of those key services and the critical components which support their provision including any 4th party dependencies. For example, the potential single point failures associated with those components.

These factors will aid STPs in considering the most stressing scenarios for testing to provide confidence in their ability to continue providing key services in the event of their failure or severe but plausible disruption. Further guidance on the calibration of scenario severity and plausibility is provided in the GFOR in section 5.2.

3.2 Scenario Selection & Sources

STPs are expected to consider that disruption would occur, rather than basing their resilience assessment on the relative probability or likelihood of the incidents occurring. Therefore, the scenario selection process should include identification of severe but plausible scenarios to use in their scenario testing exercise of key services.

A scenario library acts a repository for generic real-life severe but plausible scenarios that can be used to design service-specific scenario tests. These scenarios may be extended through the addition of relevant complicating factors, including additional issues which may make a scenario more demanding in terms of recovery. Typical examples include: events occurring during peak processing and/or loading periods; events occurring during out of hours and/or holiday periods; events occurring during system migration or upgrade; events complicated by other factors such as extreme weather; events complicated by customer, peer or third party actions.

In order, to form an initial scenario library framework, STPs can use the five key scenarios categories outlined in the Operational Resilience regulations to form an initial scenario library framework. These relate to:

- Loss or reduced provision of technology underpinning the delivery of key services;
- Corruption, deletion, manipulation or compromise of data critical to the delivery of key services;
- Unavailability of facilities impacting delivery of key services;
- Unavailability of key individuals and/or groups of people impacting delivery of key services;
- Unavailability of fourth party services which are critical to the delivery of key services (e.g. the extent to which the STP itself depends on contractors or suppliers)

It is expected that STPs will build the maturity and the sophistication of their scenario testing over time. Hence in addition to the five scenarios outlined above, they can also leverage a range of existing sources to inform the creation of a comprehensive scenario library. These would include:

- Scenarios derived from the government's National Risk Register[10];
- Threat intelligence based on the National Cyber Security Centre (NCSC)'s sector threat assessments;
- CMORG Guidance for Firm Operational Resilience, and in particular section 5 dealing with scenario testing;
- CMORG Strategic Review into Sectoral Risks to Operational Resilience;
- Annual Horizon Scan conducted by the Business Continuity Institute;
- Actual incidents and near-misses for the STP, its peers and the industry;
- Internal, business specific risk registers;
- And any other source that the STP believes to be relevant in the design of the scenarios.

The scenario library should be regularly reviewed and updated to reflect the latest threats and vulnerabilities identified from the STPs broader horizon scanning and intelligence gathering exercise. A formal review of the scenario library should be undertaken on at least annual basis.

3.3 Scenario Design

The scenarios are broadly based on two main categories - the unavailability of individual resources or combination of resources (such as people, premises, technology, suppliers) and

[10] National Risk Register, 2023 Edition, HM Government, August 2023

specific events or trigger-based scenarios resulting in the disruption of the resources (such as cyber-attack, insider threat, data corruption or environmental factors such as a severe weather event).

Following the initial stage of selecting a scenario, the third parties can also benefit from adopting a detailed scenario design and development process which informs the focus and the scope of testing, and also considers additional factors that test the STP's ability to deliver their key services. Some of the additional aspects for consideration would include:

- Scenario analysis that details the understanding of the impact of the scenario on its operations, data or clients along with identification of key dependencies and critical processes that would be impacted as result of an event materialising;
- Assessing control frameworks, security measures and procedures to identify any existing vulnerabilities and weaknesses that could be exploited as a result of a chosen scenario. This ensures the use of empirical evidence that STPs will have through the knowledge of existing vulnerabilities, therefore proving or disapproving such gaps through the mechanics of scenario testing;
- Developing an understanding of the root cause that highlight the contributing factors leading up to the failure or breach. These could include technical vulnerabilities, external threats, inadequate controls or human error.

3.4 Severe But Plausible Scenarios

Operational resilience is based on withstanding and recovering from severe shock to the key services and operations of a business. The focus on 'severe but plausible' scenarios require STPs to consider scenarios that would truly push their ability to deliver key services (see Figure 2). When considering 'plausibility', STPs should consider whether the event is conceptually consistent with what is known to have occurred in the past i.e., it has some basis in prior knowledge. It is also reasonable to extrapolate such events to reflect known trends in threat landscape or other external factors.

Whilst the scenario should not be so remote that it becomes meaningless or impractical to respond to, the focus is on the 'severity' and the significance of the 'impact' resulting from severe scenarios. Operational resilience scenarios should be demanding in testing the resilience of the organisation and should also help STPs test the boundary of their ability to recover key services in a timely manner. In extremis, operational resilience scenarios may call into question the viability of the STP. The range of scenarios tested should also seek to explore differing aspects of the resilience of the STP, as well as the associated recovery processes.

Operational Resilience scenario testing complements (and draws on) other testing undertaken by the STP including business continuity and disaster recovery testing (focussing typically on higher likelihood events), and links to reverse stress testing and other forms of testing which explore the ability of the STP to deal with catastrophic failure.

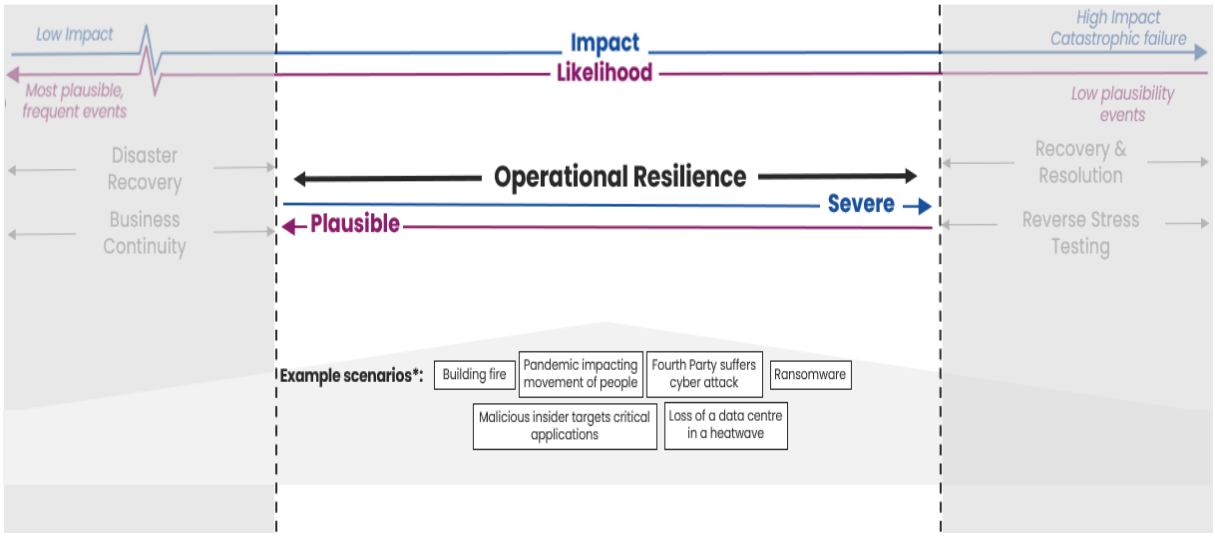


Figure 2: Operational Resilience relative to the severity and plausibility spectrums

It is expected that STPs which are early in their operational resilience journey or fall in the bracket of non-regulated entities will have existing business continuity and incident management frameworks to ensure ongoing provision of their key services.

Figure 3 elucidates how impact and severity of scenarios aligns to conventional business continuity and incident management approaches whilst also linking with Operational Resilience.

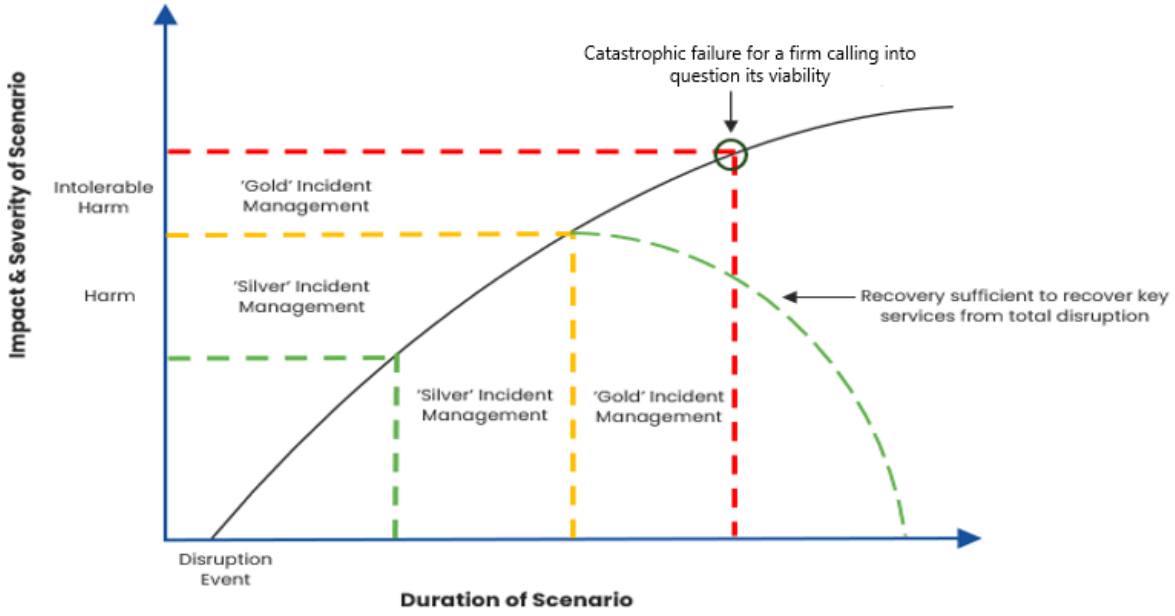


Figure 3: Scenario Impact and Severity relative to BC/Incident Management approaches

STPs are also encouraged to build a view of the key scenarios, the types of impact and the likelihood ratings based on criteria of key threats and vulnerabilities that a business faces. The scenario selection logic helps demonstrate to clients and customers that a robust and defensible process has been adopted to select appropriate scenarios for test.

Below is an illustration of how scenarios can be graded based on their likelihood:

Impact Scenarios	Impact *(Confidentiality, Integrity, or Availability)*	Examples of how impact might be realised	Likelihood Rating *(based on key threats and vulnerabilities)*	Impact Considerations
Takeover of external DNS records and domains	• Confidentiality • Integrity • Availability	Exploitation of vulnerabilities either manufacturer defects or weak configuration on DNS systems	High / Medium / Low	• Impacted volumes of IBS consumers • Impact total volumes of transactions • Reputational damage • Financial safety and soundness • Impact on UK market stability
Disruption of critical supplier due to cyber event	• Confidentiality • Integrity • Availability	All cyber-related scenarios	High / Medium / Low	
Unavailability of critical supplier (non-cyber)	• Availability	All non-cyber scenarios including fire, flood, terrorism, loss of network, failed change, infrastructure failure	High / Medium / Low	
Disruption of critical industry-wide services	• Availability	Malware / Ransomware attack	High / Medium / Low	
Disruption at another firm in sector	• Availability	Various scenarios	High / Medium / Low	

4 Evidential Requirement

4.1 Overview

Clients seek to assure themselves of the operational resilience of an STP including its ability to remain resilient in the face of severe but plausible scenarios. Existing third party risk management (TPRM) regimes typically seek assurances from third parties over the existence of various control measures. For example, confirming the existence of a disaster recovery policy and seeking evidence of the regular testing of such a policy, but do not seek evidence on the ability of the STP to respond to a specific disruptive scenario or class of scenarios.

To illustrate this point, TPRM may confirm the existence of backup and restore processes for critical data, but do not require the STP to provide evidence that such processes can be invoked in a timely way to restore the key service and to demonstrate through testing that such timescales can be met. Equally, TPRM will focus on confirming the existence of various cyber security controls but will not provide a holistic view of the ability of a STP to recover from a given ransomware scenario including data recovery and subsequent business process recovery.

This chapter outlines evidence requirements linked to the scenario testing process which allow a financial firm to gain a deeper understanding of the resilience posture of the STP, as well as setting out how STPs can build confidence in the minds of their clients over their resilience posture.

The evidence sought by financial firms is likely to include detail of:

- Organizational and process controls
- Technical controls
- Contractual controls in place with 4th parties
- Testing including exercising of controls (this could be a mix of activities including scenario testing, business continuity testing, disaster recovery testing, and red team testing)
- Relevant incidents (normally summarised in post incident reports), or in some cases “near misses”

4.2 Resilience Assurance Statements

The first approach considered is based on the development of a standard resilience assurance statement by the STP which can be readily consumed by financial firms who are their clients. This provides a minimum level of assurance in a consistent way to meet the bulk of the needs of those clients, while recognising that individual clients may seek additional detail to meet their specific requirements.

The standard assurance statement would provide evidence that the STP:

- Has clearly defined key services (also defined as important business services as per the UK Financial Regulations defined by PRA, FCA and BoE; and defined as critical or important functions under the EU regulations under DORA);
- Has a well-developed view of end-to-end mapping of key services, and the means to maintain the currency of such mappings;
- Has a well-developed library of severe but plausible scenarios (aligning to the ORCG scenario library) and the means to maintain such a library;
- Has conducted scenario testing on their critical supporting services on a regular basis against a broad range of such scenarios;
- Has a demonstrable and appropriate governance for the management of operational resilience of the STP, with evidence of senior executive engagement;
- Has a structured approach and mechanism relating to the management and remediation of operational resilience vulnerabilities, including those derived from scenario testing.

This would complement evidence of the existence of control measures such as security, disaster recovery and business continuity processes, which support aspects of the recovery of the financial firm in various scenarios.

4.3 Scenario Testing Scope and Plan

The second, and complementary, approach is the sharing of the STP's scenario testing scope and plan, or a summary version of such.

Developing a scenario testing scope and plan along with a structured approach to understanding how points of failure have been considered and assessed to ensure the real impact to the business is understood, is considered crucial to evidencing the STP's approach to scenario testing activity. The testing plan is also expected to be aligned to their wider strategic resilience objectives and can include how STPs intend to build the sophistication of their scenario testing activities/ plans over time. It is expected that as STPs grow in their resilience maturity, that their scenario testing plan will be developed and enhanced accordingly.

The sharing of evidence relating to the process of scenario selection and testing aids financial firms in understanding of how the STP's test scope and plan has been formulated and graded for priority testing. Below is a list of suggested evidence base of what a good test scope and plan should include:

- What has been the process of identifying scenarios related to a STP's key services and their mapped dependencies on people, process, technology, suppliers etc;
- How past failures, both within and outside of a STP, have informed the operational resilience scenario testing scope;

- What has informed the scenario selection and deselection criteria to evidence the rationale for progressing and/or not progressing across a range of scenarios (including which scenarios have been excluded as being implausible or of such severity that they will not be considered further);
- How scenario construction has brought together the distinct parts within a STP's existing processes such as business continuity management, disaster recovery plan, past incident logs and operational risk management etc;
- How the STP's risk appetite has helped create a prioritised action plan to mitigate vulnerabilities established through scenario testing;
- How any know vulnerabilities associated with scenarios are assessed against the resilience strategy and objectives of the STP.

Please note that the above is not an exhaustive list and has been developed whilst drawing appreciation to the interconnectedness of disparate processes that inform the overall resilience assurance and scenario testing processes.

4.4 SOC 2 Style Control Assurance Statements

The sharing of a resilience assurance statement and summary version of scenario testing plan provide good insights into the STP's implementation of an operational resilience regime comparable in approach to that mandated on financial firms under the UK Operational Resilience regulations.

This can be complemented by the sharing of an assurance statement giving confidence in the control environment within the STP, whether in response to a third party due diligence process (including that delivered via industry wide utility models such as the Financial Services Qualification System (FSQS)) or through independent assurance against a recognised assurance standard.

System and Organization Control (SOC) reports are internal control reports created by the American Institute of Certified Public Accountants (AICPA) to provide confidence in the services provided by a service organisation so that end users can assess and address the risks associated with outsourced services. These are assessment reports undertaken by an independent entity. The SOC 2 report which typically reports on controls at a service organisation relevant to security, availability, processing integrity, confidentiality or privacy is gaining broad adoption and can provide confidence in aspects of resilience. SOC 2 reports have been standardised internally under the International Standard on Assurance Engagements (ISAE 3402)[11].

While we do not set out a prescriptive requirements for STPs to provide a SOC 2/ISAE 3402 assurance statement validated by an independent entity, we do encourage STPs to share a

[11] International Standard on Assurance Engagements 3402 – Assurance reports on controls at a service organization

set of self-assessed SOC 2 style assurance statements with financial firms which provide detail on a STP's security and resilience posture.

These assurance statements should cover the below aspects of a STPs internal security controls:

- Confidentiality: data classification and life cycle management, access control and management;
- Integrity: integrity checking and maintenance, data backup and restoration in the event of corruption;
- Availability: high availability design, fault tolerance, disaster recovery and business continuity controls;
- Asset Management: asset identification and life cycle management, including currency of those assets;
- Vulnerability Management: configuration management, patch and vulnerability management;
- Performance Management: performance monitoring, service management and capacity management;
- Resilience by Design: development lifecycle controls and architectural approach to resilience;
- Incident Management: event, incident and crisis management;
- Supply Chain Management: supply chain risk management.

5 Reporting Formats

5.1 Key building blocks of a Scenario Test Report

A number of different strategies can be utilised by the STPs to collate and present the outputs of their scenario tests, ranging from spreadsheet to presentation reports. Formulating a comprehensive scenario test report that addresses the purpose and outcome of the test conducted is crucial in ensuring that the key learning and remediation work are prioritised and taken forward in addition to it forming part of the governance process of the STP.

Adopting a standardised reporting template which can be shared with one or more clients ensures there is consistency in the information sharing across the financial firms who may be reliant on the STP.

Below is a representation of key building blocks of scenario test report encapsulating four main segments i.e., Executive Summary, Scenario Exercise Overview, Scenario Exercise Outcome and any other pertinent factors that form part of the exercise process:

Key Segments of Reports	Detailed Content	Summary
Executive Summary	Introduction	Rationale behind conducting the test and key objectives
	Approach & Background	Covering the test approach and background on the tested capability
	Outcome & Next Steps	Key vulnerabilities / observations as an outcome of the test and focus on next steps
	Key Services Recovery Threshold Overview & Assessment Outcome	A view of recovery thresholds of key services against the selected scenario. Assessment outcome can be based on proximity of recovery against the set thresholds and the confidence in the identified proximity grading
Scenario Exercise Overview	Scenario Description	Detailed overview of scenario tested and rationale of why the scenario was deemed to be 'severe but plausible'
	Scenario Variations	Any scenario variations or 'complicating factors' that were deemed to be in or out of scope of the main scenario
	Response and Recovery Timelines	Triage process and assessment of detection and containment controls E2E Technical Recovery Timeline Workarounds and Substitution Customer Treatment Strategies Market Treatment Strategies
Scenario Exercise Outcome	Vulnerabilities and Mitigation	Key vulnerabilities with ownership defined to track mitigation of the identified gaps
	Observations and Recommendations	Key observations and recommendations including any areas of good practices identified through the course of conducting scenario testing
	Assumptions	Key assumptions that were considered as part of the test which may impact the overall service recovery thresholds
Appendix	Key Participants	Details around scenario participants for e.g., an internal test vs. join activity
	Test Methodology	Scenario Testing Methodology and alignment to regulatory policy statement

Where appropriate, the scenario description should also consider how judgements on the severity and plausibility of the scenario were reached drawing on scenario calibration guidance in the GFOR.

5.2 Drawing alignment between scenario test report & self-assessment requirements

Under the UK operational resilience regulations, financial firms are required to prepare a self-assessment report which provides an assessment of its compliance with the UK operational resilience regulations. This will include, along with an assessment of internal systems and controls, conclusions based on relevant third party scenario testing and assurance activities. This report must be approved by its board and may be requested by the PRA or FCA as part of its supervision of such financial firms.

The content of this report is set out in the regulations, including: identification of IBSs and ITOLs, approach to mapping of IBSs, testing strategy, risks to resilience, and approach to addressing any vulnerabilities identified during testing.

Depending on the nature of STPs i.e., if they are regulated or unregulated entities, they may or may not be required to complete such a self-assessment report. However, drawing on the concepts of the self-assessment process would enable STPs to consistently demonstrate that:

- they have implemented the principles of operational resilience and have a robust framework in place to evidence improvement in their resilience posture;
- they have a documented and an evidentiary based approach in developing operational resilience methodologies including those relating to scenario testing;
- they are able to reflect on the lessons learned from their approach to implementing operational resilience and outcomes of scenario tests including accounting for any changes, vulnerabilities or emerging gaps.

On a high-level STPs can adopt an approach of the regulatory self-assessment requirements and keep an up-to-date record of its resilience assessment which aligns to the operational resilience principles. Whilst it is understood that every business will have its own specific approach to operational resilience therefore driving a business specific view of such a compliance report, there is a list of some essential ‘good to have’ sections that could be considered as guidance for STPs.

The representation overleaf should not be considered to be an exhaustive list of items for this report and STPs are encouraged to include any relevant information as they see fit (such as post-incident reviews, pertinent extracts/ parts from internal or external audit reports, references to any additional test exercises outside the scope of operational resilience etc.).

Strategic Requirements	
Identifying Key Services	Detailing the justification and approach of how the key services were identified, their impact assessed from the perspective of their criticality to any upstream or downstream clients of STPs
Defining Service Recovery Thresholds	Covering how key services have been assessed by the STPs for their recovery thresholds with a view of reducing or mitigating any impact to the IBSs of their clients
Evidencing the ability to remain within Service Recovery Thresholds	Documenting and evidencing the ability to remain within the defined recovery thresholds; process of scenario selection and reviewing the outcomes of stress testing such key services; understanding of vulnerabilities and gaps along with mitigating actions; and lessons learned through embedding the end-to-end operational resilience principles
Supporting Requirements	
Governance	• Governance models including formal committees, relevant owners and people fulfilling key roles • Risks, Issues and Actions, including any key metrics as per the relevant procedures
Mapping of Key Services	• Resource identification across people, process, premises, technology that enable the delivery of key services • End-to-end mapping of all internal and external dependencies to ensure a comprehensive view of supply chain dependencies • Mapping that supports the identification of vulnerabilities and gaps to be tested via scenario testing exercises
Scenario Testing	• Strategy, scope and detailed test plans including any assumptions or exclusions around the scenarios considered but not tested • Type of testing activity conducted i.e., desktop exercises, technical testing, joint testing with the end clients, etc… • Description of scenarios tested with the rationale behind testing these • Description of scenarios tested where the STP could not remain within their set service recovery thresholds
Vulnerabilities	• Description of the vulnerabilities identified through scenario testing • Actions plans to mitigate such vulnerabilities along with completion timeframes
Lessons Learned	• Detail approach on the post-incident review process • Documenting lessons learned, action plan taken and justification of timeframes to enhance overall resilience posture
Communication Strategies	• Internal and external communication strategies with specific focus on liaising with any upstream or downstream clients who have identified the said supplier as ‘significant’ in ensuring the provisioning of their IBSs • Escalation paths and mitigating actions during a live incident

6 Contract Obligations

While DORA does require a financial firm to embed certain mandatory contract requirements relating to audit and inspection into contracts with third parties, there is no comparable obligation in the UK operational resilience regulations which might require the sharing of scenario testing results undertaken by a third party or require the co-operation of third parties in the conduct of a financial firm's scenario testing.

CP 23/30[12] (6.23 and 6.24) does suggest that CTPs would be required to share: the results of scenario testing and financial sector incident management playbook testing with the regulators' requirements, including any recommended remediation (where that information relates to a financial firm to which it provides services); and a summary of the information contained in the CTP's annual self-assessment submitted to the regulators. The CTP would be responsible for developing an appropriate method for sharing these summaries and other information with its financial firm customers. This method should include controls to ensure that confidential or sensitive information is appropriately protected.

While STPs do not fall within the scope of the CTP regime, there is an opportunity to develop model contract clauses to be adopted by financial firms as a basis for contract negotiations in respect of operational resilience regulations, noting that consistency of adoption would send a strong signal to STPs over the importance of embedding scenario testing and in providing financial firms with a relevant summary of such testing. As a minimum we would recommend that STPs be required to share a resilience assurance statement of the form set out in section 4.2 with clients. This should be a descriptive report which provides sufficient detail for financial firms to draw confidence and assurance over the STP's resilience. We would further encourage the sharing of a summary scenario test scope and plan as set out in section 4.3.

While we recognise the sensitivity of detailed test results (disclosing as it may detailed vulnerabilities), we believe that this minimal level of disclosure is appropriate and necessary to allow financial firms to meet their regulatory obligations and exercise appropriate due diligence regarding the resilience of their third parties. Appropriate protocols may need to be adopted for the sharing of sensitive information, including relevant non-disclosure agreements and need to know mechanisms. In the absence of such detail financial firms may be forced to adopt a precautionary approach in which they judge that the STP is not able to demonstrate recovery within ITOL.

Lastly, we consider that STPs should be obligated to support financial firms in undertaking scenario testing where the scenarios being considered relate to the key services they provide to support the IBSs of those financial firms. Such an obligation may also need to extend to sub-contractors who are critical to that service.

[12] Consultation Paper: Critical third parties to the UK Financial Sector

7 Scope for Community Wide Testing

In requiring a STP to support scenario testing by individual financial firms, there is a risk of duplicative testing and significant additional overheads and burdens for the STP. While this may be unavoidable for STPs who provide tailored services to each financial firm, there may be scope for community testing where the services provided by the STP are of a commoditised or standardised nature and therefore consumed consistently across the community.

The pilot collaborative scenario test undertaken during the first phase of this work[13] was an example of such a test and validated the utility of such testing. The implementation of such a test scheme would require collaboration between financial firms to sponsor (and potentially fund) the execution of the test scheme. There would also need to be an acceptance by the financial firms themselves (and implicitly by regulators) that the results of such testing would provide a robust basis for evidencing resilience.

At this time current utility models for due diligence around third party resilience (such as the Financial Services Supplier Qualification System – FSQS) focus on the existence and coverage of third party business continuity and disaster recovery plans, along with standards compliance (such as ISO 22301[14]) rather than exploring the existence or adequacy of scenario testing processes or the results of such testing.

In the case of CTPs who are directly regulated there is also likely to be an assumption that financial firms can place a degree of reliance on the testing being undertaken by that regulated entity, although the responsibility for remaining resilient in the face of disruption would ultimately remain with the financial firm itself. The proposed CTP regime includes the concept of CTP fundamental rules. The draft CTP 6 imposes an obligation on CTPs to:

> *"deal with the regulators in an open and co-operative way, and disclose to the regulators appropriately anything relating to the CTP of which they would reasonably expect notice."*

It is arguable that a similar fundamental rule should be crafted to require CTPs to engage with financial firms (their clients) in an open and co-operative way given the need for those financial firms to meet their regulatory obligations under the operational resilience regulations.

[13] CMORG Collaborative Scenario Testing of Critical Third Parties, 23rd May 2023
[14] ISO 22301:2019 Security and resilience – Business Continuity Management Systems - Requirements

8 An Integrated Approach

Figure 4 illustrates a possible overall strategy for embedding scenario testing where the choice of approach is driven by the systemic importance of the third party (CTP, STP or other) along with the nature of the services being provided. The CTP regime will provide the regulatory basis for embedding scenario testing for third parties of high systemic importance. This is likely to include mandated use of scenario testing and associated self-attestation of results in the interim, with a possible move to independent audit over time including the use of ISAE 3402 style attestations. There may also be scope in the longer term for BoE commissioned scenario testing of CTPs, particularly those which offer commoditised services to the sector. Such CTPs are also likely to be involved in SIMEX style community resilience testing.

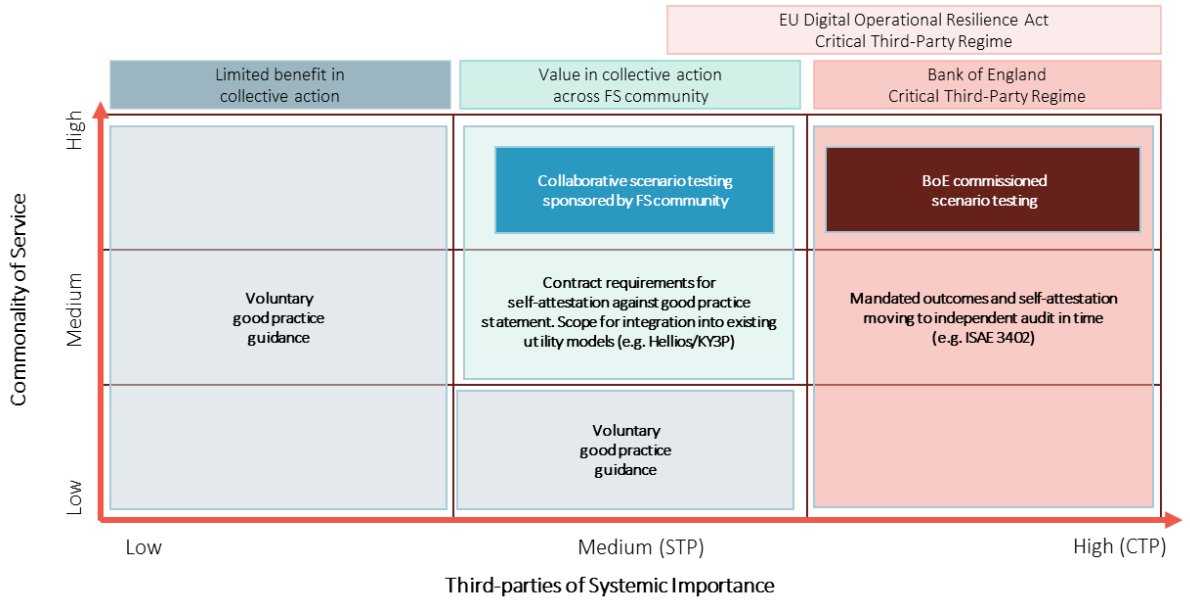


Figure 4: Possible strategy for embedding scenario testing

For STPs there is scope to embed requirements in contracts using model clauses as a vehicle for achieving a degree of consistency in approach across the community. Existing utility models may also offer a means for embedding aspects of scenario testing good practice through extension of existing operational resilience question sets. There is also potential benefit in collaborative scenario testing of those STPs who offer commoditised/transactional services to the community.

For other third parties, it is likely to be disproportionate to seek to embed additional requirements in contracts, and the optimal approach is likely to be the promotion of the adoption of good practice guidance on a voluntary basis.

9 Conclusions and Recommendations

9.1 Conclusions

The approach to scenario testing with STPs is an important and regulatory driven expectation. The production of this guidance supports the evolution that financial firms and regulators are seeking to drive as the industry continues to strengthen the resilience of the ecosystem.

This guidance is designed to be relevant and usable for the wide variety of financial firms that deliver an Operational Resilience program, as well as providing guidance to third parties around expectations, principles, and expectations for scenario testing.

Scenarios that third parties chose to exercise can be tailored but should be aligned with the principles of severe but plausible events. Scenario selection should also be considered from the ORCG Scenario Library, the CMORG Strategic Risk Register, and what can be demonstrated at the time of publication in the current release of the DORA primary legislation.

It is acknowledged that information that would form part of the evidence of scenario testing will already exist at most STPs. However, scenario testing moves beyond the sharing of IT disaster recovery tests, SOC 2 reports, etc. Third parties will be required to provide additional evidence of the rationale for scenario selection, how the scenario test was run, and (where applicable) how identified vulnerabilities are being mitigated.

It is critical to ensure that the interconnectivity of service components are tested through the scenario, which often produces deeper insight into the resilience of the service, rather than a one-dimensional view of those components in isolation.

Whilst this guidance and these recommendations are predominately focussed on STPs, CTPs that may fall within the scope of CP23/30 and DORA should consider how these recommendations align to their plans for compliance with these forthcoming regulatory regimes. Equally, third parties that might not reach the threshold to be considered a STP or CTP, should consider these recommendations as best practice.

9.2 Recommendations

Third parties that fall within the principles of definition of a STP should consider their approach to scenario testing and, where relevant, align to industry expectations. These expectations ensure that financial firms can deliver against their regulatory obligations under Operational Resilience.

STPs are recommended to conduct scenario testing such that the end-to-end service is tested, including the interconnectivity of components that support their material service delivery to clients.

Financial firms and third parties should consider deepening contractual provisions such that third parties can commit to supporting financial firms deliver their regulatory obligations, as well as the good practice of operationally resilient delivery to clients and the industry. The development of model contract clauses may assist this process.

A recommended reporting format is provided. This minimum baseline supports a consistent insight into the scenario testing at third parties across the industry. This is not a formal requirement, and financial firms / third parties are encouraged to develop this as required in support of the maturing evolution of transparency across the industry.

Where STPs in particular provide an operational service to a wide number of clients, it is recommended that "community testing" be considered, and if appropriate, adopted by the regulators in the Fundamental Rules. This would empower transparency and efficiency, as well as underpinning the evolution of resilience regulation.

Lastly, CMORG should consider opportunities to provide community wide education across STPs to assist in an improved understanding of the requirements and obligations of financial firms in relation to operational resilience.

Annex A. CP26/23 Extract – Operational resilience: Critical third parties to the UK financial sector

Testing Requirements

Scenario Testing

6.9 Under the regulators' proposals, a CTP would be required to:

- carry out regular scenario testing of its ability to continue providing each material service within its maximum tolerable level of disruption in the event of a severe but plausible disruption.
- identify an appropriate range of adverse circumstances of varying nature, severity, and duration relevant to its business, risk profile, and supply chain and consider the risks to the delivery of the material service in those circumstances.

6.10 The proposed scenario testing requirements and expectations for CTPs are adapted from the requirements and expectations in the operational resilience framework for firms and FMIs. CTPs would be expected to assume that disruption is inevitable when designing their scenarios for testing.

6.11 The regulators would expect the sophistication of a CTP's scenario testing to be consistent with its systemic significance while balancing minimising the risk of disruption to its operations or customers.

Testing financial sector incident management playbooks

6.12 The regulators propose to require a CTP to test its financial sector incident management playbook annually. If justified, the regulators could also direct a CTP to re-test its playbook at a different time or more frequently than once a year. For instance, following significant disruption. The regulators would expect the testing to:

- be organised and coordinated centrally by the CTP;
- include an appropriate representative sample of the CTP's firm and FMI customers to which it provides material services; and
- be reviewed and approved at an appropriate level in the CTP.

6.13 The regulators also propose to require each CTP to produce a report following each test of its financial sector incident management playbook and share it with the regulators. The report should be completed as soon as reasonably practicable and sent to the regulators immediately after the report is completed. The report would be expected to set out:

- the key findings from the test;
- proposed revisions to the CTP's Financial Sector Incident Management Playbook or the CTP's incident management more broadly; and
- general non-attributable feedback to the CTP's firm and FMI customers based on the test e.g. on best practices identified.

Annex B. Abbreviations

AICPA	American Institute of Certified Public Accountants
BoE	Bank of England
CMORG	Cross-Markets Operational Resilience Group
CRR	Capital Requirements Regulation Firms
CSP	Cloud Service Provider
CTP	Critical Third Party
DNS	Domain Name Service
DORA	Digital Operational Resilience Act
DR	Disaster Recovery
E2E	End to End
FCA	Financial Conduct Authority
FI	Financial Institution
FSMA	Financial Services and Markets Act
FSQS	Financial Services Qualification System
FMI	Financial Market Infrastructure
GFOR	Guidance for Firm Operational Resilience
HMT	HM Treasury
IBS	Important Business Service
ICT	Information and Communications Technology
ISAE 3402	International Standard on Assurance Engagements 3402 engagements provides independent assurance on controls over processes related to financial reporting that have been outsourced to a third party
ITOL	Impact Tolerance
NCSC	National Cyber Security Centre
ORCG	Operational Resilience Collaboration Group
OTPRM	Outsourcing and Third Party Risk Management
PRA	Prudential Regulation Authority
SIMEX	Community Wide Simulation Exercise
SOC 2	A voluntary compliance standard for service organizations, developed by the American Institute of Certified Public Accountants
STP	Significant Third Party
TPRM	Third Party Risk Management

Annex C. Glossary

Terms	Definition
Critical Third Party	As per HM Treasury's proposed regime for critical third parties, a third party will only be designated as a CTP if it considers that a failure or disruption to the services it provides to firms "could threaten the stability of, or confidence in, the UK financial system". In considering whether to designate a third party, HMT is required to have regard to the materiality of the services the third party provides to the financial sector, and the number and type of firms that rely on those services
Critically Important Functions	A "Critical or Important Function" is defined under DORA as a function, the disruption of which would materially impair the financial performance of a financial entity, or the soundness or continuity of its services and activities. Or the discontinued, defective or failed performance of which would materially impair the continuing compliance of a financial entity with the conditions and obligations of its authorisation, or with its other obligations under applicable financial services law.
Digital Operational Resilience Act (DORA)	The aim of DORA is to strengthen the EU financial sector's resilience to ICT-related incidents and introduces very specific and prescriptive requirements that are homogenous across member states. Critical ICT third parties which provide ICT-related services to financial institutions, such as cloud platforms, data analytics and audit services, are also subject to this new regulation. Organisations are required to be able to withstand, respond and recover from the impact of ICT incidents, thereby continuing to deliver critical and important functions and minimising disruption for customers and for the financial system.
Financial Firm	For the purposes of this document, a financial entity including financial market infrastructure (FMI) falling within the scope of the UK operational resilience regulations.
Important Business Service (IBS)	IBS means a service provided by a firm, or by another person on behalf of the firm, to one or more clients of the firm which, if disrupted, could: (1) cause intolerable levels of harm to any one or more of the firm's clients; or (2) pose a risk to the soundness, stability or resilience of the UK financial system or the orderly operation of the financial markets.
Impact Tolerance (ITOL)	ITOL means the maximum tolerable level of disruption to an important business service, as measured by a length of time in addition to any other relevant metrics, reflecting the point at which any further disruption to the important business service could cause intolerable harm to any one or more of the firm's clients or pose a risk to the soundness, stability or resilience of the UK financial system or the orderly operation of the financial markets.
Operational Resilience	Operational resilience is the ability of firms, financial market infrastructures and the financial sector as a whole to prevent, adapt and respond to, recover and learn from operational disruption.
Severe But Plausible Scenarios	Severe but plausible scenarios consider events that cause disruption to the provisioning of IBSs and is built across an appropriate range of adverse circumstances, varying in nature, severity, and duration, aligned to the risks and vulnerabilities of a firm.
Scenario Testing	Firms are required to carry out scenario testing, to assess its ability to remain within its impact tolerance for each of its important business services in the event of a severe but plausible disruption of its operations.
Significant Third Party	Third parties who are not so designated (by HMT under FSMA) as CTP but are key to the delivery of the IBSs for one or more financial firms.