CMORG
CROSS MARKET OPERATIONAL RESILIENCE GROUP

COLLABORATIVE SCENARIO TESTING OF CRITICAL THIRD PARTIES

Version 1 | July 2023

TLP CLEAR

Recipients may share **TLP CLEAR** information openly, with no limit on disclosure.

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.

Contents

1 Executive summary

This report summarises the work of the Operational Resilience Collaboration Group (ORCG) Collaborative Scenario Testing of Critical Third Parties (CTP)[1] working group. The group was tasked to develop a methodology and approach which can be applied to critical third parties supporting multiple financial institutions (FI), which can provide a partial or complete evidence base to draw on during scenario testing by individual FIs.

Over the period May 2022 to February 2023 the group developed a collaborative scenario testing methodology and undertook a pilot with two third party payment providers to assess the viability of that methodology. In addition, the group explored the utility of various assurance methodologies, and collected evidence from members over their views on the adequacy of assurance evidence currently available around the ability of CTPs to recover from severe but plausible disruption scenarios.

This industry-led paper has been sanitised to **TLP CLEAR** to encourage sharing and awareness among the financial sector and beyond, including other industries, third parties and jurisdictions. A full report exists at **TLP AMBER**, which includes the outcomes of a pilot tested on two third party payment providers. Due to sensitivities associated with the pilot's findings, it is only available on request to firms who are members of the ORCG.

The findings from this initiative include that:

- The requirement for each FI to engage separately with a given CTP to achieve the necessary level of assurance over their recoverability leads to duplication of activity and unreasonable expectations on CTPs to service the diverse needs of multiple FIs in providing assurance evidence.
- Existing CTP due diligence/assurance mechanisms focus on the existence of systems and controls (e.g. business continuity plans) rather than allowing estimation of recovery times associated with a given scenario.
- There are concerns over the adequacy of test evidence regarding the ability of CTPs to recover in the event of more complex scenarios, such as application corruption or cyber attack.
- There is a need to develop assurance models which allow a given CTP to provide evidence which the community of FIs can draw upon in reaching conclusions on their operational resilience.
- A range of potential assurance models exist, including: self-assessment, independent assurance and collaborative testing models.
- The collaborative test methodology set out in this report is feasible and has proved successful during the pilot with two third party payment providers, but that its utility may be limited to services which are provided community-wide and are broadly repeatable in nature.
- The self-assessment and independent assurance models set out in this report merit further investigation, with greater confidence attaching to the results of the independent assurance approach, albeit with the likelihood of increased cost.

[1] It should be noted that the use of the term 'critical third parties / CTP' in the context of this initiative is used to refer to third parties regarded as critical to the resilience of multiple FIs and/or which if disrupted could cause a systemic impact on the UK financial sector. However this methodology is expected to have wider applicability than those organisations formally designated as CTPs through the forthcoming policy. See also 2.3.

- The final community assurance approach is likely to involve a combination of self-assessment, independent assurance and collaborative testing, depending on the nature of the entity being tested and the nature of the service provided.
- All assurance models would be supported by further standardisation of scenarios, evidential requirements and reporting templates.
- There is considerable regulatory action to drive improvement of CTP resilience and security across all critical national infrastructure sectors in the UK and more widely in the EU, with expectations that such CTPs will embed an appropriate resilience testing regime.
- The work undertaken to date by ORCG can assist the Financial Conduct Authority (FCA) / Prudential Regulation Authority (PRA), and HM Treasury in framing regulatory expectations regarding scenario testing by CTPs under the proposed HM Treasury CTP regime.

2 Background

2.1 ORCG

The ORCG is a sub-group of the CMORG, acting as the strategic focal point for operational resilience collective action between the private sector and public authorities in the UK's financial sector. Established in 2019, the ORCG facilitates collaboration between FIs that have a common interest in operational resilience, and to focus on shared problems that firms may not be able to address alone.

2.2 Scenario Testing

The FCA and PRA have established regulations to improve the operational resilience of the financial sector in the UK. As part of these regulations, FIs are required to test their ability to remain within their impact tolerances for each of their important business services in the event of a severe but plausible disruption of its operations. This enables them to be assured of the resilience of their important business services and identify where they might need to act to increase their operational resilience.

2.3 Third Parties

In undertaking such scenario testing, FIs are also expected to assess their dependencies on third parties, and the extent to which the disruption of services provided by such third parties may in turn impact the operational resilience of the firm. FIs will therefore require evidence of the ability of the third parties on which they depend to recover from disruptive events (including associated recovery time estimates) and will base their judgements on their own recoverability on such evidence, along with additional substitutions or contingency plans they may have in place to deal with the disruption. The term CTP has been adopted in this report to refer to third parties which are regarded as critical to the resilience of multiple FIs and in particular those third parties whose disruption may cause a systemic impact on the UK financial sector. It is also noteworthy that working group members are also receiving such requests from upstream clients who regard them as being CTPs.

2.4 Challenge

Most CTPs, some of which may also be regulated financial market infrastructure (FMIs) in their own right, support a large number of FIs. This results in a one-to-many relationship which results in CTPs receiving multiple requests for evidence relating to various scenarios and their ability to recover from such scenarios. This can result in considerable (and sometimes conflicting) demands being placed on CTPs. There is also no agreed standard for the provision of such evidence to FIs, nor agreement on the types of scenarios for which CTPs may need to provide such evidence.

2.5 Scope

ORCG agreed to establish a working group to explore whether it was possible to develop a methodology and approach which can be applied to CTPs supporting multiple FIs, which can provide a partial or complete evidence base to draw on during scenario testing by individual financial institutions.

2.6 Approach

The working group sought to develop a scenario test approach which could be applied to CTPs; to pilot the application of this approach; and to document the test outcomes. Feedback would also be sought from participant institutions on the adequacy of the evidence base generated, and whether it would be

possible to modify the methodology and approach to create a future template for collaborative scenario testing of CTPs.

3 Methodology

3.1 Overview

The methodology selected was based a structured eight step assessment approach building on the experience of working group members in undertaking collaborative scenario testing between a single FI and an associated CTP. It involves an initial assessment of the relevant CTP services and products on which FIs depend, the development of a set of relevant scenarios around such products, the down-selection to the sub-set of scenarios to be tested, a structured review of the evidence available around the recoverability of CTP services and products in those scenarios, validation of those assumptions with the CTP (and further exploration of the scenario), and then a final reporting stage in which the scenario test report is agreed with the CTP and circulated to ORCG working group members to assess the utility of the report.

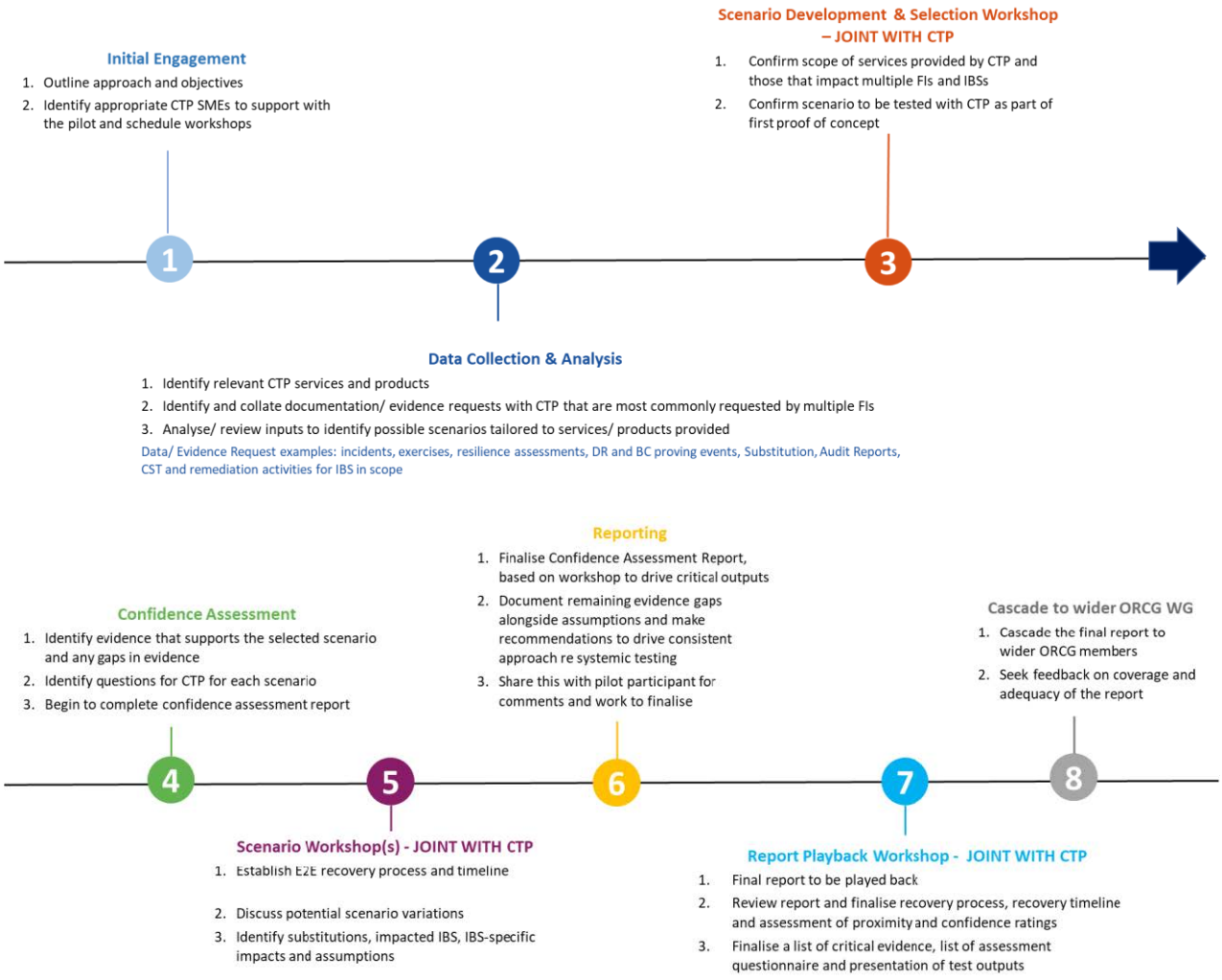

Figure 1: Proposed Test Methodology

4 Selection of Pilot

4.1 Initial Review

Working group members were invited to identify the types of CTP which might be selected for the initial pilot collaborative scenario test, in doing so they were invited to consider which CTPs they were most directly dependent on and which might directly impact their resilience. Their top three preferences were:

Figure 2: Initial Responses on CTP Dependency

In discussion the dependency on payment providers was regarded as key by most working group members, with cloud service providers and telecom service providers also being regarded as critical by working group members.

4.2 Community Survey

This initial "straw" poll was backed up a survey of working group members which asked them to confirm which third parties they regarded as critical to their firm. While not a comprehensive survey, this does provide a level of insight into the dependencies of concern.

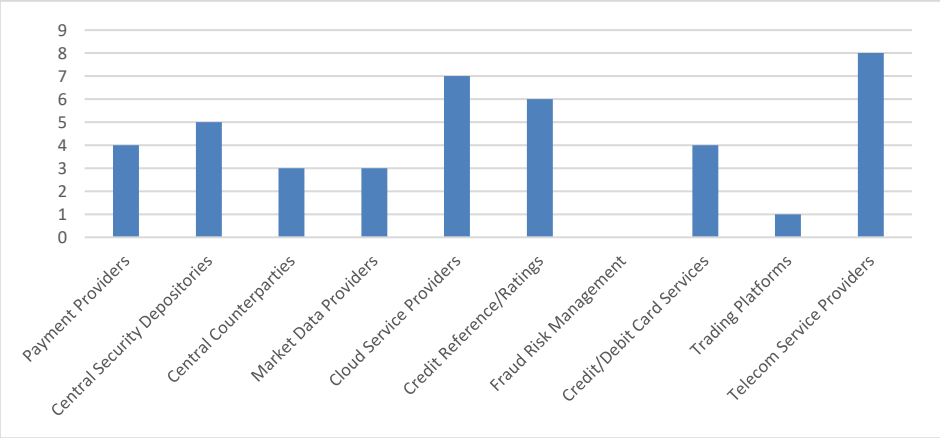

Figure 3: "Which third parties do you regard as critical" (select 3)

Once more cloud service providers and telecom service providers play a prominent role, alongside a wider range of CTPs depending on the nature of the FI. A second survey question probed working group members on which of the CTPs they regarded as being their top critical supplier in terms of dependency.

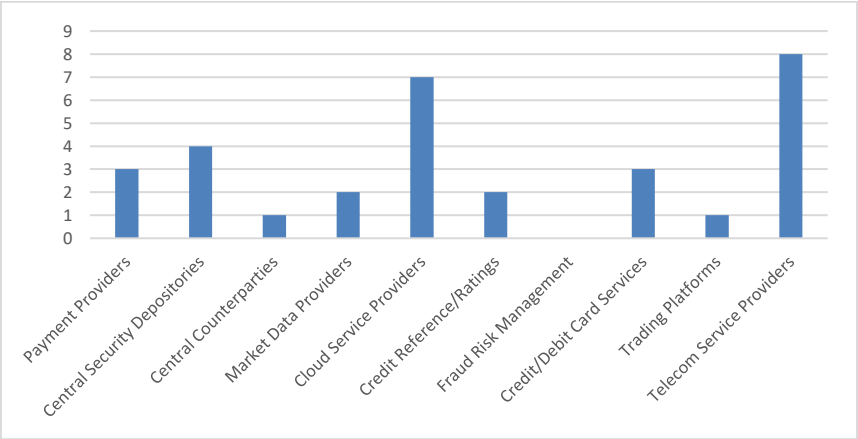

Figure 4: "Which third party do you regard as you top critical supplier"

This second survey question places greater emphasis on cloud service and telecom service providers.

4.3 Selection of Provider

Following working group discussion, it was agreed to select a payment provider as the initial pilot, with the option to approach a cloud service provider or telecom service provider as a second pilot, noting that there were ongoing discussions between UK Finance and cloud providers over assurance models. This also reflected negotiations with a variety of organisations on their willingness to participate in the pilot exercise, along with a recognition that FMI institutions were likely to have more mature approaches to embedding scenario testing within their own governance models given their regulation under similar Operational Resilience regulations to other FIs. It was, however, noted that cloud service providers were subject to regulation under the Network and Information Systems Regulation (as a digital services provider) and that discussions were ongoing with multiple FIs over the provision of enhanced assurance over resilience. The telecom regulatory regime was in the process of evolving as the Telecom (Security) Act 2021 entered into force.

Two third party payment providers indicated their willingness to participate in the pilot exercise and the working group wishes to record their thanks to both entities for their active support and the open and transparent approach they adopted throughout the pilot.

5 Scenario Selection

5.1 Regulatory Expectation

The operational resilience regulations require firms to assess a range of severe but plausible scenarios, providing guidance that such a range may include people, facilities, technology, information, and third-party scenarios. It is therefore reasonable to expect that CTPs may consider an equally broad range of scenarios in the assessment of their own resilience. ORCG has provided guidance in the form of a scenario library included within their interim guidance for firm operational resilience.

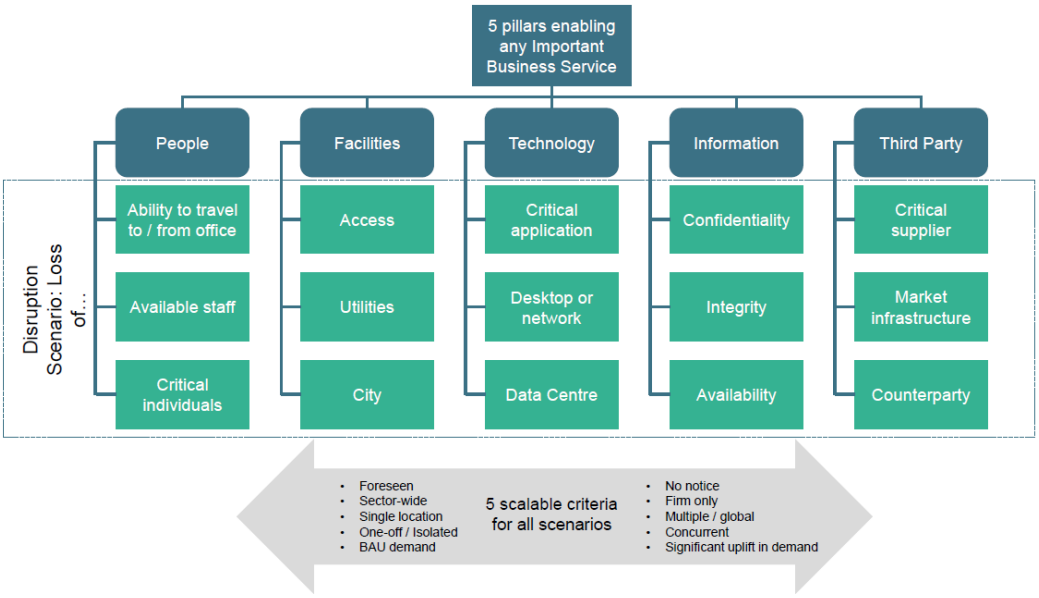

Figure 5: ORCG Interim Guidance – Scenario Themes

The working group therefore considered a broad range of scenarios for the pilot collaborative test.

SCENARIOS CONSIDERED	• People (unavailability of key staff - due to pandemic or adverse weather) • Property (unavailability of critical site/ data centre - due to fire, flood, power outage etc.) • Information (unavailability of critical data - due to malicious insider, human error or ransomware etc.) • Information (manipulation or corruption of critical data - due to malicious insider, human error or ransomware etc.) • Information (disclosure of sensitive data/ credentials/ critical assets - due to malware or insider) • **Technology (unavailability of network services - due to exploitation of vulnerabilities or DDoS attack)** • **Technology (unavailability of critical application - due to malware, ransomware, unauthorised access etc.)** • **Technology (unavailability of data centre - due to loss of network)** • **Cyber (major ransomware or other cyber compromise - ransomware, malware, encryption of critical applications)**

Figure 6: Initial Long List of Scenarios

5.2 Most Taxing Scenarios

A survey of the working group membership was undertaken to collect views on which of the scenarios might be regarded as most concerning in terms of plausibility and scale of impact should they occur.

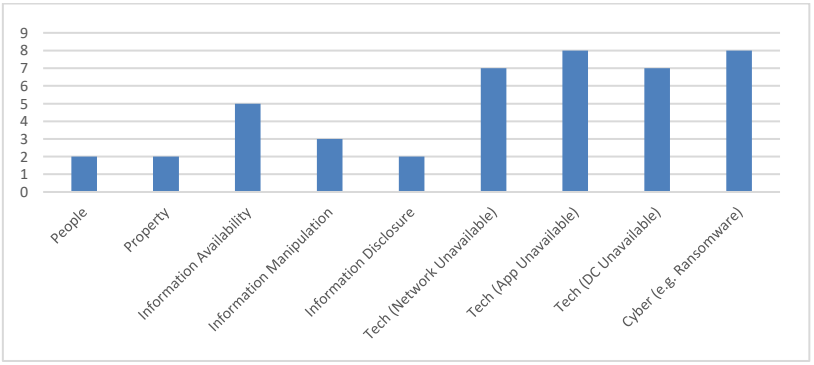

Figure 7: "Which 3rd party scenarios are most concerning in terms of plausibility and scale of impact"

A second survey question assessed which members found might represent the biggest risk to IBS provisioning should they occur, reflecting in part the confidence that each FI had in the ability of the CTP to recover.

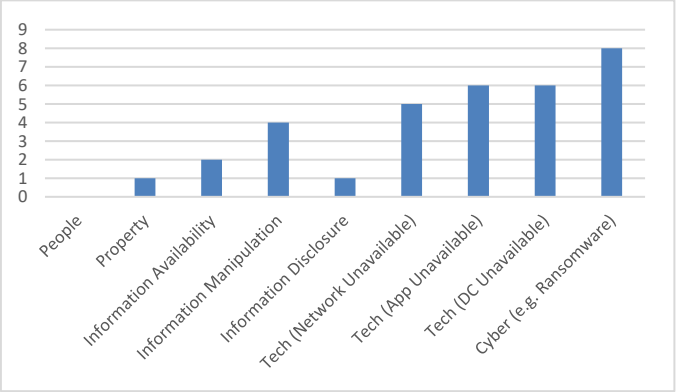

Figure 8: "Which scenario represents the biggest risk to your IBS provisioning"

These survey results reflected working group discussions in which most members had a greater degree of confidence in the ability of the CTPs they interacted with to deal with more straightforward scenarios such as a property event, whereas technology disruption, information manipulation and cyber (e.g. ransomware) scenarios were considered to be more taxing.

5.3 Recovery within ITOL

Further survey questions probed the expectations of working group members around the ability of their third parties to recover within the impact tolerance (ITOL) of the FI using such a CTP.

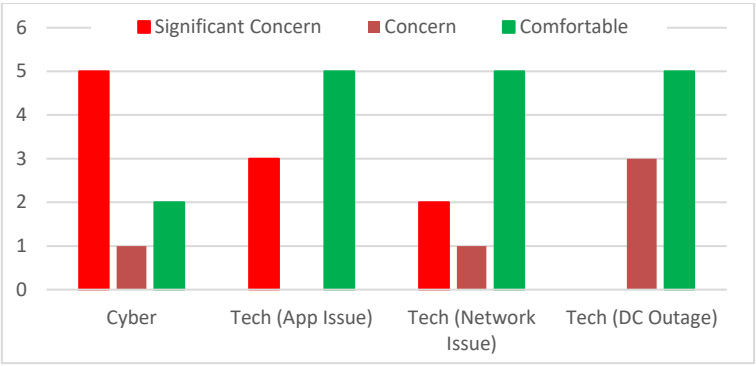

Figure 9: "Ability of CTP to recover within the ITOL of the FI"

There was significant concern that recovery of the CTP would not occur within ITOL in cyber scenarios such as ransomware, with a number of working group members also having significant concern that this might not be the case in the event of application corruption or integrity issues being encountered by a CTP. There was greatest confidence of the ability of CTPs to deal with data centre outage and network issues, reflecting in part the evidence provided by such CTPs over data centre fail over testing and other similar disaster recovery testing.

Finally, working group members were asked to rate the extent to which they have adequate visibility over the evidence available from CTPs to support their assertions regarding recoverability in these more complex scenarios.

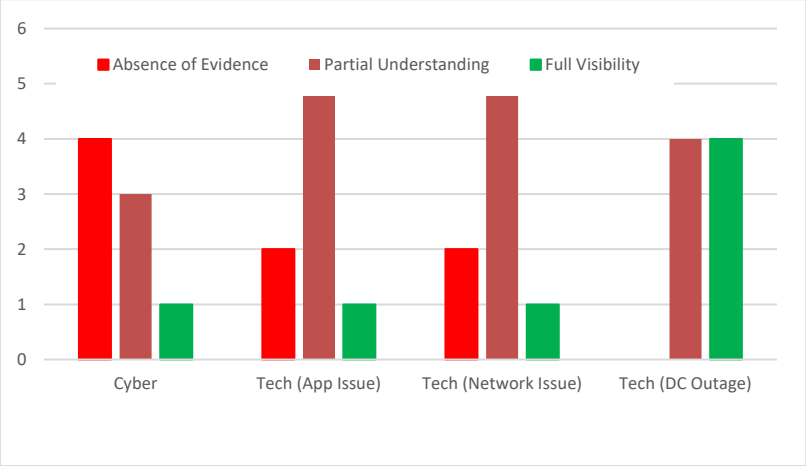

Figure 10: "Adequacy of evidence available to support 3rd party recovery assertion"

Concerns existed over the evidence base available to support assertions over recoverability in cyber scenarios in particular, with most regarding evidence as being absent or having only a partial understanding of the ability of the CTP to recover. There was greater confidence in their evidence base supporting assertions regarding recovery from application corruption/integrity scenarios and network issues; with the most visibility over data centre outage recoverability. This reflects, in part, the historic focus on availability issues such as data centre failure and disaster recovery planning, rather than more complex integrity and corruption scenarios.

5.4 Final Scenario

Initial review of the two critical third parties' testing results confirmed the expectations of the working group that more straightforward scenarios such as property outages, technology and data centre outage scenarios had been considered and that appropriate testing (business continuity, disaster recovery, validation or pan-industry exercising) had been undertaken to provide confidence in the ability to recover from such scenarios in a timely way. Based on this initial analysis, it was agreed to explore a range of cyber attack and complex technology disruption scenarios during the pilot scenario test.

6 Test Outcomes

6.1 Testing Undertaken

The scenario test was conducted as a desktop exercise in which all the key steps of recovery were discussed as part of working through one of the third parties' scenario run-book. Specific subject matter expert (SME) inputs were also provided from both third parties to assess the impact of the chosen scenario against one of the third parties' important business services (IBSs). The test itself took circa four months from initiation to completion.

The test was conducted in line with the draft methodology set out in section 3, which also included a review of the two third parties' relevant exercise and test materials. The results of the test remain TLP AMBER+STRICT given commercial confidentiality and risk of disclosing vulnerabilities.

7 Role of Collaborative Scenario Testing Going Forward

7.1 Utility Models

The working group considered whether collaborative scenario testing might form the basis for a utility model in which such tests could be undertaken by a single provider/institution in a way which would allow the results to be broadly adopted by FIs as part of their own evidence base for scenario testing.

7.2 Assurance Being Sought

In reaching this judgement the working group explored the types of assurance they might seek from a CTP over the robustness of their own scenario testing (or a comparable regime for assuring their disaster recovery and business continuity measures).

These judgements divided into assurance over the robustness of their scenario test processes (and whether they might align with regulatory expectations); whether the coverage of scenarios was sufficiently broad, whether the output met an accepted evidential standard; whether it provided confidence in their ability to meet ITOL (or provided confidence in a recovery times asserted by that CTP); and whether the CTP is taking action to improve their position in the event that they are considered to be beyond ITOL or a reasonable recovery time.

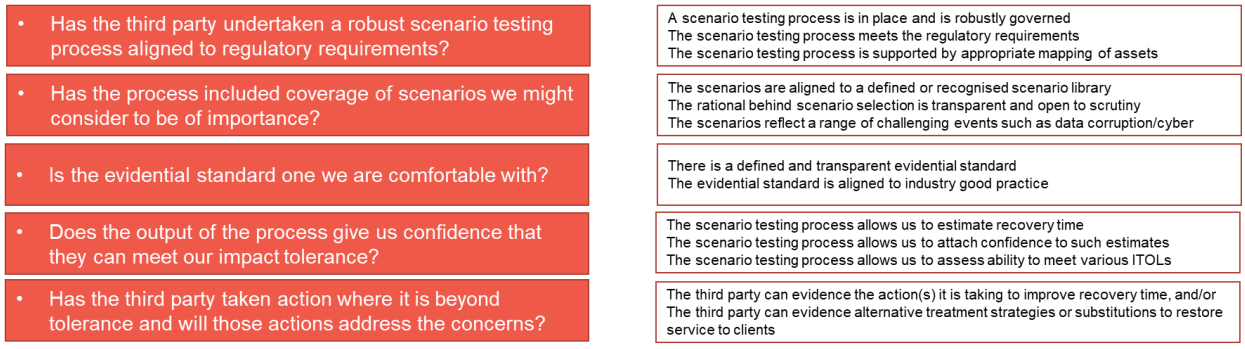

Figure 15: Aspects of assurance

The concept of ITOL is one which only realistically applies to CTPs regulated under the UK's operational resilience regulations, although CTPs regulated under other regimes (or indeed unregulated) might reasonably be expected to demonstrate their ability to meet a stated recovery timeline which could be shared with clients.

7.3 Assurance Models

The working group considered three different assurance models. The first is a self-assessment model in which the CTP undertakes its own scenario testing processes leading to a self-certification along with an evidential base which could be open to review by FIs. This allows the CTPs itself to select appropriate scenarios, and structure and organise its own test programme drawing on relevant business continuity and disaster recovery testing. The CTP would make its own judgements on the commercial sensitivity and releasability of internal information on system and controls, along with its resilience architecture. The risk is that such self-assessment may not provide sufficient challenge required for a given CTP, including comprehensiveness of scenario selection and appropriate evidential standards. The approach is, however, relatively straightforward to implement although it does require the relevant CTP to adopt a variant of scenario testing.

The second moves to an independent assurance model for CTPs. Such independent assurance would depend on a well-defined test and assurance methodology being available which any independent assurer could adopt. The focus of such assurance would be on the recoverability of the end-end services provided by the CTP, as well as the extent to which they have adopted a robust scenario testing methodology as part of exploring the adequacy of their resilience measures. Such assurances might cover the process of scenario testing, the comprehensiveness of scenario selection, the evidential base which supports judgements on recovery during that scenario, and the accuracy of any statements made over such recoverability. In designing such a model we can draw on previous experience in defining assurance approaches for security and business continuity controls and processes including assurance standards such as SOC 2 (an assurance standard for systems and controls).

These assurance reports would then be made available to FIs by CTPs. This would also require engagement with relevant assurance providers (such as professional services firms or to a pan-industry assurance organisation) to both establish such standards and the associated assurance regime and also train and skill the assessors.

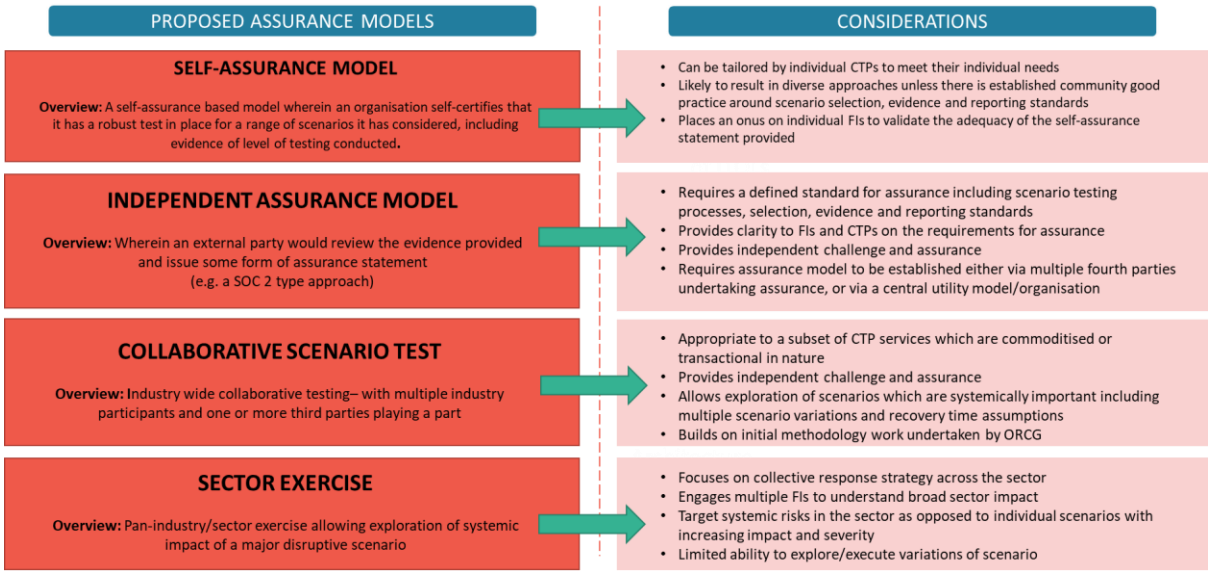

Figure 16: Assurance models

The third model, which was the focus of this working group, is the type of pan-industry collaborative scenario test undertaken in concert with the two third party payments providers during this study. In this case the independent body (for the purposes of this report, the lead FI) undertook the test on behalf of the community, including working with the CTP to define the scenarios, collect and structure the evidence base and report on behalf of the community. This form of testing could be undertaken by an independent test organisation who would also apply expert judgement to help frame the scenarios and probe underlying recovery time assumptions. This would require community agreement on methodologies and reporting standards, as well as an appropriate legal construct to protect that test organisation against any redress resulting from the judgements made in the test report.

Finally, it is worth noting that CTPs may also be involved in cross-sector exercising activities under the auspices of the CMORG Sector Exercising Group (SEG) including sector-level simulation exercises (SIMEX). Such sector level exercising allows multiple FIs to engage with a single scenario to understand the broad sector impact and explore collaborative responses. While exercises provide a rich environment to explore the dynamics of a given scenario, they do require significant planning effort which will limit the scalability of this model.

7.4 Applicability of Collaborative Testing

During the pilot it became clear that there were situations in which such testing may be effective and others where defining and agreeing the scope of the testing would be more problematic. In particular, collaborative testing would be most likely to be effective where the service(s) being provided were well defined and understood, and also likely to be consumed by FIs in a broadly consistent way. Payment services is one example. It would be less effective where the CTP offered highly tailored services to FIs, for example hybrid cloud services or managed service models. In such cases there would be greater benefit in joint testing between the CTP and the relevant FI consuming the service given the complex interaction between the two entities and the likely need for an integrated response to any issue.

Collaborative testing would also need to be of interest to sufficient FIs to justify the scale of effort involved and also ensure there was sufficient incentive on the CTP to participate in such activities.

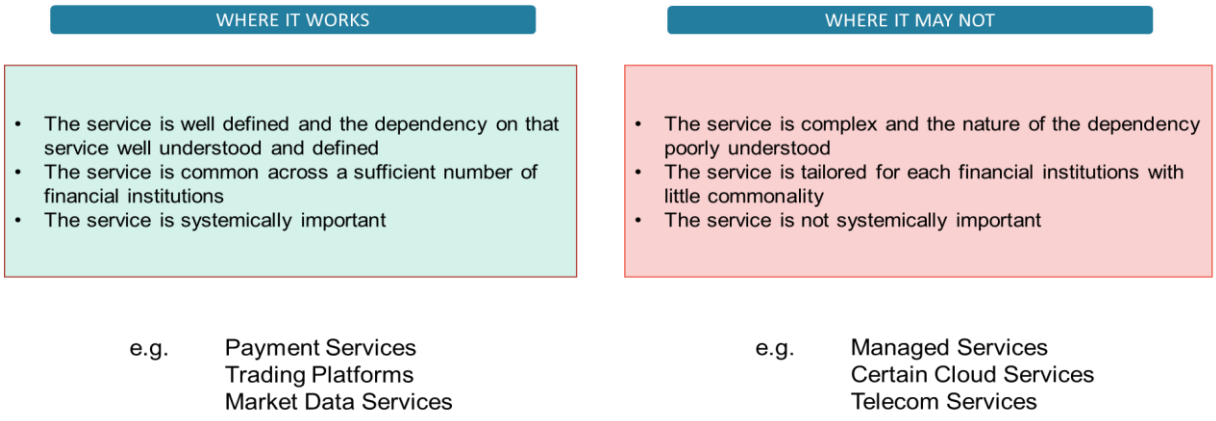

Figure 17: Applicability of Collaborative Testing Models

7.5 Areas for Potential Standardisation

Irrespective of the assurance model selected, there appear to areas in which the community would benefit from further standardisation activity. These include further development of the ORCG scenario library (and in some cases the adoption of community stressing scenarios); a standardised approach to structuring and assessing evidence; and the use of standardised reporting templates.

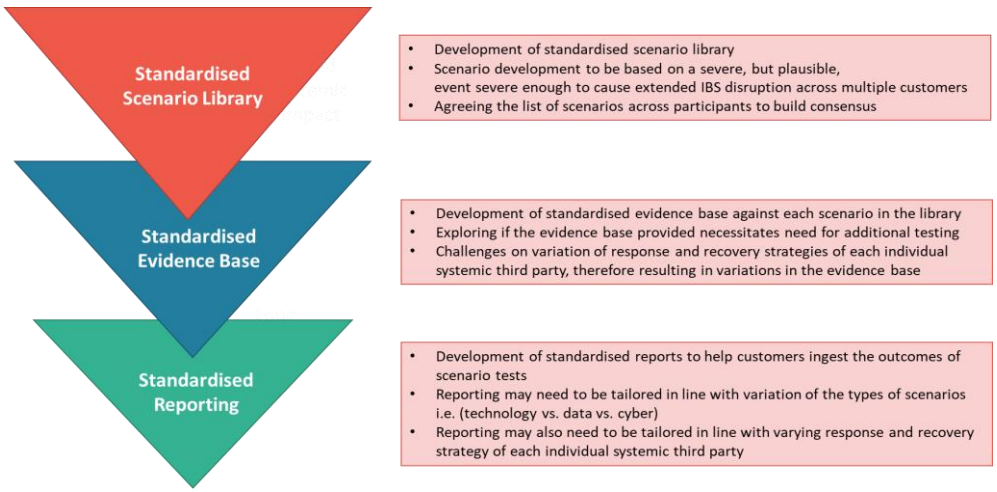

Figure 18: Areas for Standardisation

The benefits associated with such additional standardisation of scenario libraries, evidential and reporting standards are not limited to testing of CTPs, but would also apply to achievement of greater consistency in industry wide scenario testing by the FIs themselves.

Appendix A: Abbreviations

BACS	Bankers' Automated Clearing Services
CAF	Cyber Assessment Framework
CMORG	Cross Market Operational Resilience Group
CTP	Critical Third Party
DCMS	Department for Digital, Culture, Media and Sport (now reorganised)
DNS	Domain Name Service
DORA	Digital Operational Resilience Act
E2E	End to End
FCA	Financial Conduct Authority
FI	Financial Institution
FMI	Financial Market Infrastructure
FPC	Financial Policy Committee
IBS	Important Business Service
ICT	Information and Communications Technology
IP	Internet Protocol
ITOL	Impact Tolerance
NCSC	National Cyber Security Centre
NIS	Network and Information Systems Regulation 2018
ORCG	Operational Resilience Collaboration Group (a CMORG subgroup)
PRA	Prudential Regulation Authority
RDSP	Relevant Digital Service Provider
SaaS	Software As A Service
SME	Subject Matter Expert
SOC 2	A voluntary compliance standard for service organizations, developed by the American Institute of CPAs
TPRG	Third Party Resilience Group (a CMORG subgroup)