Operational Resilience Mapping Guide

v.1 January 2022

Introduction

This Best Practice Guidance documentation has been produced by the TISA Operational Resilience Mapping Working Group. The Group consists of representatives from a wide range of firm types. Each section was written by one or more members of the group and reviewed by all members of the group, to provide a balanced view of each key area of the requirements.

Please remember that the information contained within these statements is for information purposes only and is not intended as a substitute for the need of each firm to understand its own requirements and determine its own procedures that are relevant to its business. The information contained is for general guidance only, is not exhaustive and may change from time to time.

Oversight

Firms should consider effective oversight in two phases of their Operational Resilience journey – the implementation, and the BAU maintenance. Because this is not a one-off exercise, firms will be expected to review and maintain their Operational Resilience controls.

Implementation

In all areas of the Operational Resilience requirements, there are clear expectations that Boards and senior management functions will have oversight over the process and approve the output. The mapping exercise should be approached with this in mind. The regulators expect that someone on the Board or equivalent should approve the mapping exercise, and it would commonly fall to the SMF 24 (if they are in place) to take responsibility for the development of the mapping.

However, it is good practice to ensure that all members of the senior management team review the outputs, and collectively approve the results. Whilst SMCR has focused people on their individual responsibilities, it is important that the Board as a collective body fully understand the agreed scope of the mapping exercise, and the results obtained.

It is important for firms to be able to demonstrate that there has been informed debate, review and consideration, within the senior management team on the mapping process:

- The scope of the mapping and the proposed outputs
- Progress updates and challenges
- The final output, and its alignment with the proposals

The mapping activity is likely to be undertaken by subject matter experts in the 1st Line, as it is focused on the operational processes (technology, processes, facilities etc). But it is beneficial to include input from the control functions (Compliance, Risk etc), particularly in the initial scoping phase – to ensure that the approach to be taken aligns to the regulatory expectations.

Oversight

It would be expected that SMFs within Operations (e.g SMF 24) would be overseeing the progress of the mapping activity, ensuring that it is progressing against plan, and signing off the outputs as complete – prior to Board approval. In this, it is therefore important that senior management within Operations 'get it' – in the sense that they understand the rule requirements, and also the underlying principles. The underlying principles should be reflecting a customer-centric not firm-centric approach and that due consideration is taken for external stakeholders. If the1st line senior management (and also the Board) are not clear on the requirements, then the output will not be fit for purpose.

BAU maintenance

Going forwards, Boards will need to undertake at least an annual review and sign-off of the Operational Resilience controls, and the inevitable weaknesses and risks which have been identified during the implementation phase will need to be tracked to successful resolution.

It is therefore important that firms maintain the structures and expertise they have put in place for implementation, and also the formalised oversight and sign-off process. The 31st of March 2022 deadline is only the first milestone on the journey anyway. Firms should be looking at Operational Resilience work as an ongoing part of their operational control framework, in the same manner as Business Continuity.

It would be therefore expected that good practice and 'reasonable steps' would prompt firms to:

- Maintain dedicated expertise to manage Operational Resilience
- Have standing agenda items and updates at Board meetings
- Have dedicated sub-committees, or sufficient scope within existing sub-committees and forums to discuss and action issues
- Include Operational Resilience within the risk management framework (risk registers, KRIs, RCSAs, stress testing etc)
- Include Operational Resilience control within role profiles and performance management assessments

Elements of this can occur in line with Business Continuity work, but the distinct requirements of Operational resilience should be clearly defined.

Methodology

Once all Important Business Services (IBS) have been identified (see Identifying Important Business Services TISA Best Practice Guide), the end-to-end delivery of these services to clients or the market should be documented. To achieve a detailed and useful process mapping document, the following steps should be considered.

Split each IBS into critical processes

Each IBS can be divided into critical processes to provide a more detailed understanding of how a service is initiated, processed, delivered and reviewed. Examples of IBS critical processes might include: a client initiating a request; receipt of that request; delivering on that request; and a review to ensure that the client provision is complete and accurate. These critical processes should not be granular internal process steps but high-level requirements needed to provide a service.

The critical processes can be further broken down, depending on the complexity of the service and the complexity of the organisation providing that service (see section on critical sub-processes).

Identify the harm that can occur to clients/market/firm if each stage of the IBS were to fail

Once all critical processes of the IBS have been identified, the harm that could occur to clients, the market or the firm should be considered. It may be that the level of harm differs at different stages of the IBS. For example, a client may suffer less harm if they are unable to deposit funds into an IBS compared with being unable to withdraw funds. Documenting the degree of harm per IBS stage provides important context for the processes and resources currently in place.

Document the processes involved in delivering at each stage of the service

For each IBS stage, the processing requirements should be outlined. This should focus on the volume and value requirements of the items processed while determining any peaks throughout the day, week, month, quarter and year. The time to process an item through each stage should be understood.

TISA

Methodology

Map the technology, people, property, supply chains (3rd parties), and data which support the processes

Each IBS stage will be supported by a combination of technology, people, property, supply chains (3rd parties) and data. The amount and type of these resources that help deliver each IBS stage must be fully documented. The breadth and depth of these resources are key in determining whether an IBS is operationally resilient.

Capture the resiliency and fallback options in place for each stage of the service

Capturing the existing resiliency capabilities and fallback options for each IBS stage is useful for assisting with the scenario testing. These should be considered across technology, people, property, supply chains (3rd parties) and data. Examples might include: a back-up data centre; working from home capabilities; disaster recovery sites; additional connections to third parties; and multiple data feeds.

Create a flow diagram for each IBS, incorporating the key processes and resources

Once the process and resources for each IBS has been fully documented, a high-level diagram should be created. This helps those not familiar with the IBS to understand how it is delivered but is also key in assisting in the determination of the IBS' impact tolerance.

Outsourcing Tools and Resources

As firms are now being asked to scrutinise their Important Business Services (IBS) and set impact tolerances to mitigate potential disruptive events against the new Operational Resilience regulations, firms now need to assess the risks associated with outsourcing services and modelling tools to any third party.

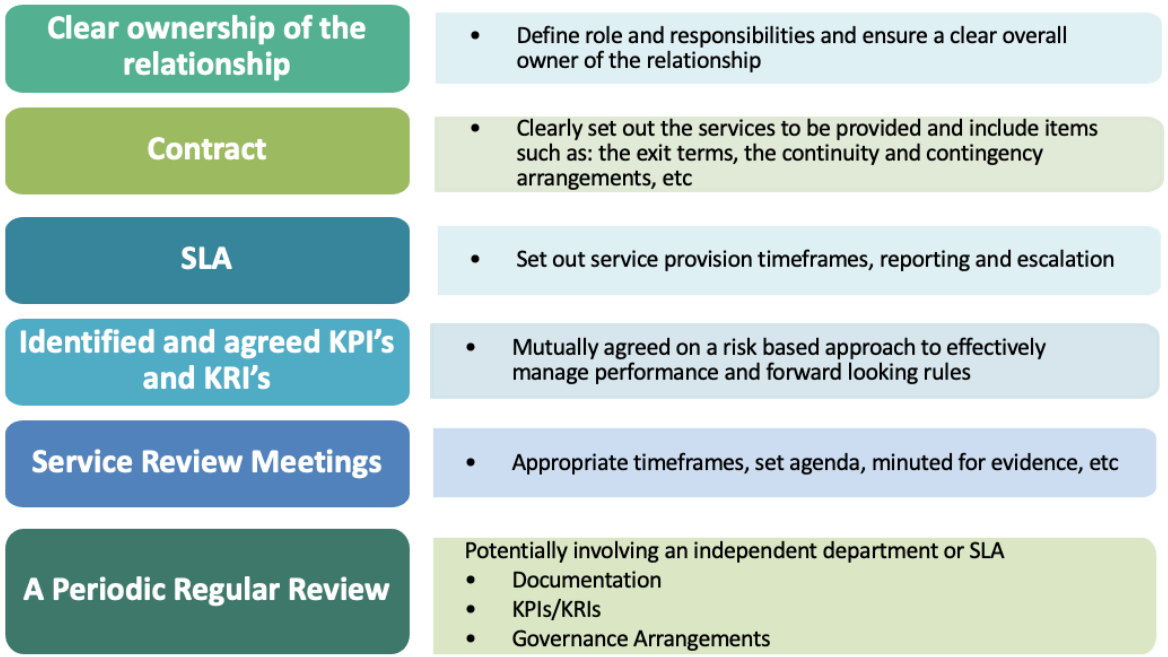
This may include outsourcing IBS themselves for example Client Relationship or Practice Management technology platforms, plus manage and monitor any systemic risks that this may bring. So, the outsourcing process will need to be FCA operation resilience rules across mapping of the people, processes, technology, facilities and information necessary to deliver each IBS.

In mapping Operational Resilience risk requirements within the business, firms should leverage existing outsourcing governance, risk and due diligence frameworks they may have introduced and comply with Principle 3 and SYSC 1.2.1G. Outsourcing reporting requirements should also be factored in as SYSC8.1.12G and SYSC 13.9.2G

Outsourcing Tools and Resources

Figure 1 below illustrates the key components to a sound outsourcing risk management process that can be applied to third party technologies and mapping tools.

Figure 1: Reasonable steps for managing outsourcing risk



Outsourcing Tools and Resources

Each component needs careful consideration when researching, on-boarding and managing outsourced tools:

Role ownership: Gatekeeper for the outsourced relationships who is accountable and responsible for on-going risk management as SYSC 3.1.1R and SYSC 4.1.1R

Contract: clear and understood by all stakeholders and reviewed at least annually

Service Level Agreement: Clear, understood and reviewed as the contract

Key Performance Indicators and Key Risk Indicators: Agreed and accountability across action planning for Performance and Risk management metrics such as data security where knowledge for FCA FG16/5: guidance for firms outsourcing to the 'cloud' and other third party IT services is of paramount importance

Service Review Meets: Clear responsibility for relationship management and accountabilities across KPI/KRIs to align with contract obligations above

Periodic Reviews: Evidenced based approach with all meetings minutes recorded centrally and aligned with contract and operational resilience annual review rule

The FCA SYSC15A.3R requires operational resilience strategies, processes and systems to be effective, comprehensive and proportionate to the nature, scale and complexity of the firm's activities. Examples of safeguards to managing the risks of outsourced tools include adequate termination rights, information reporting and notification obligations and step-in rights or remediation procedures. The needs of all stakeholders need to be incorporated with the organisation's clients and any vulnerable clients in particular front and centre of outsourced risk management.

Given operational resilience assumes failure not success, firms will need to ensure they have the right tools in place which can support their impact tolerances, mapping, scenario testing, governance and self-assessment and communications.

Outsourcing Tools and Resources

When it comes to managing risks associated with customer outcomes, conduct risk and market integrity, any outsourced strategy will need to ensure outcome-based objectives. This means strong systems and controls aligned with impact tolerance statements. This can be achieved with a level of service delivered within a designated timeframe, to agreed pre-set objectives and parameters for result expectations. For example, metric solutions would need to meet strong due diligence requirements linked to impact tolerances across consumer harm, conduct and market integrity risks.

Finally, but not least, third line of defence audits should also include outsourcing in the risk management procedures.

Case Study 1: Mapping of Assets to Critical Sub-Processes

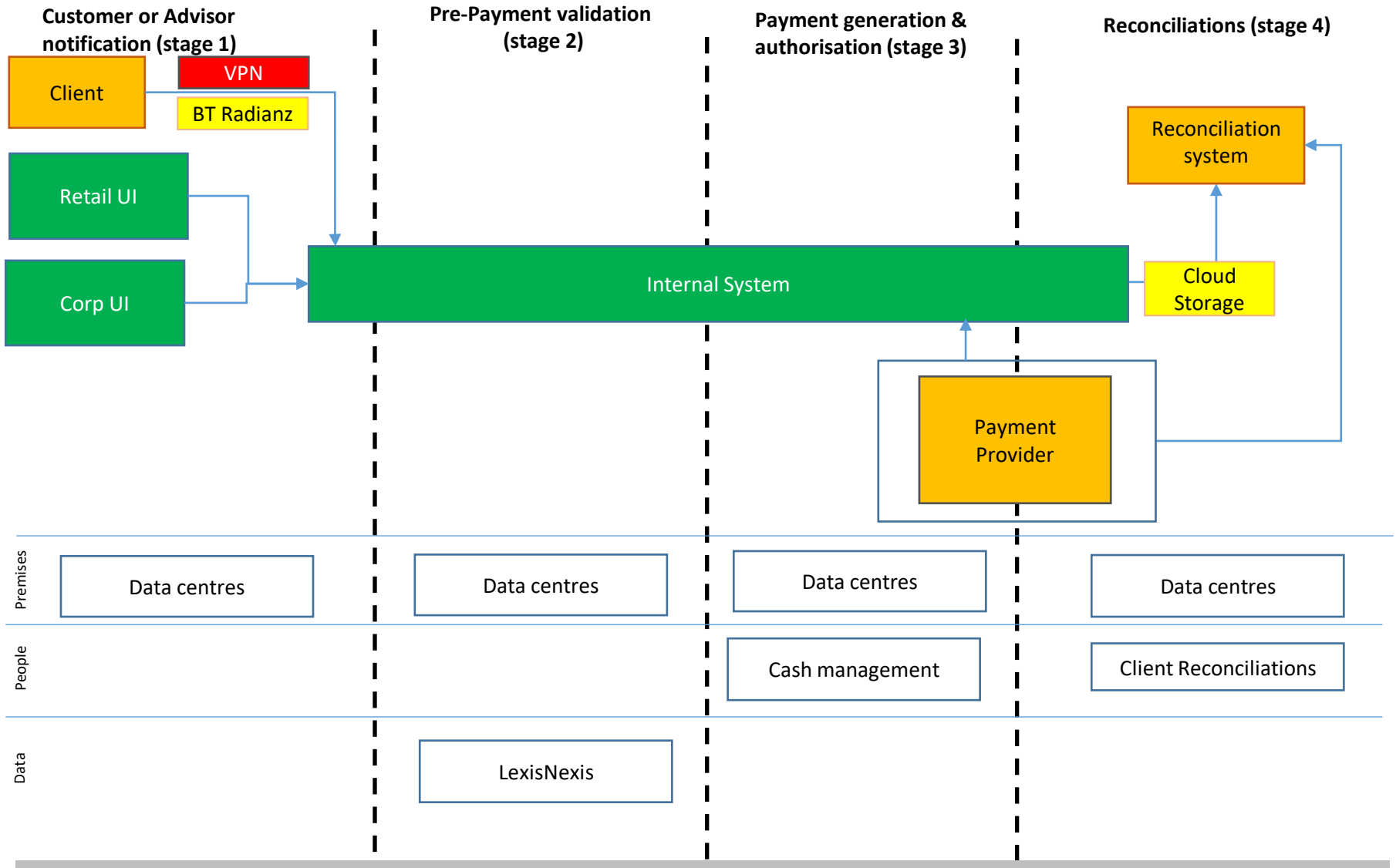
A firm has identified its Important Business Services (IBS) and the supporting critical processes. However, given the large size of the firm and the various nuances across business units, it finds that the mapping of assets to critical processes would not be sufficient for recognising critical dependencies and distinct sub-process ownership. Therefore, the firm decides to map the sub-processes that support the identified critical sub-processes. The regulation requires sufficient documentation and supporting rationale in mapping to (1) sufficiently allow the firm to identify vulnerabilities and (2) facilitate the testing of a firm's ability to deliver the IBS. Mapping to a level of granularity of sub-processes assists the firm in doing so.

Methodology

1. After the identification of a firms IBSs, the firm maps the processes used to support the delivery of the IBS.
2. The firm should then determine whether the underlying processes are critical or not critical. If a process is deemed 'not critical,' the firm should document supporting rationale as to why it is not included.
3. The firm should then further break out the processes into distinct sub-processes. If a process had been deemed not critical in the previous step, all the sub-processes below that process should also be deemed not critical. If a sub-process does appear to be critical, then the firm should re-evaluate whether the process should have been excluded in the first place.
4. The firm should then repeat the exercise of determining criticality for the sub-processes. If a sub-process is deemed not critical, the firm should document supporting rationale. **All sub-processes should have an owner who is ultimately responsible for completing the step - which could be the service owner.**
5. The firm then maps the assets (technology, data, people, facilities and third parties) to the identified critical sub-processes. The firm should document what workarounds are in place in case the assets were to fail. These will become very important when testing against the firm's impact tolerances.
6. If the data is available, the firm should supplement their critical sub-processes with periodic volumes (e.g., volume of trade volume of client activity) to identify where there are stress points located within the overall service.

The above-steps then helps the firm to identify precise assets which may lead to the failure of the overall Important Business Service and which critical sub-process would be impacted. This level of granularity will facilitate the development of scenario testing and the identification of vulnerabilities.

Example - Processing Mapping: Payments Out



Key: Green = Internal infrastructure; Amber = third parties providing/capturing data; Yellow = third parties transmitting data; Red = third parties transmitting data over the internet.