Operational Resilience in Supply Chains

December 2020

Contents:
1. Introduction
2. Regulatory Landscape
3. Overview of Tolerance Thresholds
4. Managing Resilience in Supply Chains
5. Targeted Framework Enhancements
6. Identifying Critical Suppliers
7. Risk Mapping
8. Suggested Approaches
9. Supplier Monitoring
10. Suggested Enhancements
11. Remediating Risk of Disruption
12. Summary

Helping organisations to identify, assess, monitor and remediate risk in the supply chain.
1. Managing Operational Resilience in the Supply Chain: Introduction

Operational Resilience is a specific regulatory requirement in Financial Services with defined activities and outcomes.

Whilst effective supply chain management is a key component of operational resilience, organisations are facing a number of consistent challenges:

1. Identifying critical suppliers, including 4th parties
2. Clearly defining resilience requirements in contracts
3. Defining and testing robust plans to ensure service resilience
4. Operating effective monitoring controls and oversight over critical suppliers

### Business Context

Operational Resilience demands detailed assessment and continuous monitoring of suppliers supporting the delivery of critical and important business processes.

### Resilience Requirements

- Define organisational impact tolerance thresholds
- Ensure the initial assessment of third party risk identifies truly critical relationships
- Oversight and monitoring activities must be enhanced for the most critical supplier relationships
- Develop clear contingency protocols to be implemented when tolerance thresholds are breached

### Supply Chain Impacts

- Ensure the organisation has clearly defined tolerance thresholds for disruption aligned to their Risk Management framework
- Risk assessments should be completed at both a service and a supplier level for suppliers and subcontractors
- Invest in more robust oversight and monitoring activities: data-led, based on leading indicators, informed by continuous monitoring

- Protocols should be: differentiated; proportionate; practical; and validated
- Roles and responsibilities should be clearly understood by all
2. Regulatory Landscape

Next Steps:

• The PRA has indicated that it plans further work to consider what regulatory reporting should be required for operational resiliency purposes. In the context of outsourcing the PRA has also indicated there may be further consultations, including on the treatment of third party providers.

Third Party Impact

A. Identify important business services and map any third party dependencies

B. The consultation paper suggests no more than 3 years after the rules come into effect for organisations to remain within their tolerance threshold\(^1\), which indicatively means compliance by 2024. Organisations should focus immediately on:

1. Setting operational impact tolerances
2. Designing scenarios against which to test their third parties resilience as it impacts upon operational tolerance\(^2\).

C. Ensure MI is available to evidence resilience and the basis of strategic decision-making

---

\(^1\) FCA paper CP19/32, section 5.23
\(^2\) Building operational resilience: impact tolerances for important business services (‘Joint CP cover paper), section 3.5
Organisations should set their impact tolerances at the first point at which a disruption to an important business service would cause intolerable levels of harm to consumers or market integrity. Suppliers’ impact on these tolerance measures should be identified and monitored, there may be a single or multiple indicators.

**Impact tolerance:** The maximum tolerable level of disruption to an important business service, including the maximum tolerable duration of a disruption.

Tolerance thresholds should be expressed by reference to specific outcomes (e.g. maximum value of disruption, the number of transactions or number of clients affected).

Organisations must set tolerance for disruption at business service level, this may be impacted by multiple suppliers. The FCA propose consideration of the following factors:

- Number and type (such as vulnerability) of consumers adversely affected, and nature of impact
- Financial loss to consumers
- Financial loss to the organisation
- Reputational damage
- Impacts to market or consumer confidence
- The spread of risks to their other business services
- Loss of functionality or access for consumers
- Any loss of confidentiality, integrity or availability of data

---

**Recommended Third Party Focus**

A. Identify third parties on which your critical or important businesses are dependent

B. Assess how a disruption with the third party will impact your ability to operate within your tolerance thresholds

C. Define third party controls and metrics to mitigate risks of disruption

D. Establish effective oversight regime to monitor effectiveness of controls and identify potential disruption events

---

1. Building operational resilience: impact tolerances for important business services (‘Joint CP cover paper), section 3.5
Organisations should deploy a risk-based approach to managing supply chain resilience, in line with their own internal tolerance for disruption.

Organisations developing their resiliency strategies should be seeking to manage risk rather than simply comply with process.

Organisations should be able to:

1. State with confidence which suppliers it needs to be most concerned about.
2. Monitor the resilience of its supply chain against defined tolerance thresholds.
3. Take decisive action to mitigate the risk of operational disruption when this tolerance is breached.

1. Define organisational tolerance for disruption
   - Identify the point at which a disruption would cause intolerable levels of harm to clients or business integrity (see slide 3).

2. Identify critical third parties
   - Enhance initial risk assessment methodology to ensure criticality of suppliers are fully understood (see slides 6 - 8).

3. Monitor third party performance against tolerance threshold
   - Implement enhanced oversight routines for assessment and monitoring of critical suppliers (see slides 9 – 10).

4. Remediate risk of operational disruption
   - Define effective routines that can be executed to remediate potential risk events (see slide 11).
The image below represents our suggested approach and model which, if followed, will give organisations an effective framework for managing third party risk and operational resilience in their supply chains. Further detail on how key components highlighted in green should be adapted to effectively manage operational resilience are covered in subsequent slides.

5. Targeted Framework Enhancements

- Ensure that all suppliers are risk assessed and that assessments take into consideration all factors contributing to supplier criticality.
- Conduct regular checks of your most critical suppliers to monitor indicators of disruption and performance against your own tolerance thresholds.
- Ensure that your supplier assessment programme is measuring the right things. Focus on operation of controls, as well as design.
- Implement ongoing monitoring of supplier performance. Are there leading indicators that could show a supplier is in difficulty?
- Leverage available technology solutions, such as security ratings tools, to enhance supplier oversight.
- Develop clear contingency protocols to be implemented when tolerance thresholds are breached.
6. Identifying Critical Third Parties: Overview

Early identification of critical suppliers is key in determining where resource should be deployed to monitor and manage resiliency risks effectively. Identification should take into account 3 broad components: (1) the likelihood of failure, based on characteristics of the supplier organisation; (2) the impact of failure, based on the services that the supplier is providing / processes being supported; and, (3) aggregation based on all supplier / subcontractor interactions at an organisation level.

1. Likelihood of failure
- Financial stability
- Service expertise
- Location(s) of operation
- Market sector

2. Impact of failure
- Critical processes supported
- Concentration of supplier / availability of alternate supply
- Ease of service transition

3. Service aggregation
Aggregate view of likelihood and impact across all services being provided

Supplier Criticality
- Tier 1
- Tier 2
- Tier 3
- Tier 4

Recommended Approach
- Assessment of criticality should combine intelligence captured during onboarding through the service risk assessment process (SRA) and input from specialist functions (e.g. business continuity) – see appendix 1
- Assessments should be completed at both a service and a supplier level (i.e. aggregate impacts across entire relationship, this may cover multiple services)
- Periodic re-assessment must be undertaken throughout the supplier lifecycle
- Suppliers and subcontractors must be covered by these assessments
Organisations will have numerous key or high risk suppliers that require oversight, however there will typically be a much smaller sub-set of these suppliers with whom disruption or business failure could represent a significant impact.

**Increased impact characteristics**
- A supplier / subcontractor providing a service that is fundamental to the successful operation of business critical processes and that cannot be supported or easily transitioned in-house / to an alternative provider.
  - Heavily specialised service
  - Reliance on supplier’s IP, such as customised technologies
  - Legal / regulatory permissions and licenses
- A supplier / subcontractor that is fundamental to the successful operation of multiple business processes

**Increased likelihood characteristics**
- A supplier / subcontractor
  - Suffering financial, operational or regulatory difficulty
  - Operating in an industry under significant market stress
  - Operating jurisdiction(s) prone to significant natural or geopolitical disruption
# 8. Identifying Critical Third Parties: Suggested Approach

Accurate assessment of a supplier’s criticality to your organisation will require a coordinated approach across Procurement and Resilience / Op Risk functions.

## 1. Likelihood of Failure

<table>
<thead>
<tr>
<th>Measure</th>
<th>When to Capture</th>
<th>Suggested Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial Stability</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Expertise</td>
<td>Service Risk Assessment</td>
<td>Procurement</td>
</tr>
<tr>
<td>Location of operation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Market Sector</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## 2. Impact of Failure

<table>
<thead>
<tr>
<th>Measure</th>
<th>When to Capture</th>
<th>Suggested Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criticality of processes supported</td>
<td>Pre-contract</td>
<td>Resilience/Op Risk</td>
</tr>
<tr>
<td>Concentration of supplier</td>
<td></td>
<td>Procurement</td>
</tr>
<tr>
<td>Availability of alternative supply</td>
<td>Market Research</td>
<td>Procurement</td>
</tr>
<tr>
<td>Ease of service transition</td>
<td>Pre-contract</td>
<td>Procurement/ Business</td>
</tr>
</tbody>
</table>

## 3. Service Aggregation

<table>
<thead>
<tr>
<th>Measure</th>
<th>When to Capture</th>
<th>Suggested Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>Likelihood/Impact aggregation</td>
<td>Pre-contract</td>
<td>Procurement</td>
</tr>
</tbody>
</table>

## Recommended Approach

- **A** Review your supplier assessment processes and ensure they are accounting for likelihood, impact and aggregated factors.

- **B** Consider how **aggravating and mitigating factors** are considered e.g. the risks associated with a supplier supporting critical processes may be mitigated if you’re able to easily able to transition to a suitably qualified alternative.

- **C** Ensure all informed parties are able to contribute to the process. **Resilience, Op Risk and Procurement should all contribute to form an overall view of criticality.**
9. Supplier Monitoring

Organisations must monitor the resilience of its supply chain against its defined tolerance thresholds. For tier 1 critical suppliers it is appropriate to invest more effort into a mix of activities to give enhanced oversight capabilities, above and beyond those that may have been operated traditionally.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Definition and documentation of the activities and processes to be followed in the event of possible disruption scenarios. Emphasis should be on ensuring that roles and responsibilities are understood by all parties.</td>
<td>Data-led approach to monitoring performance indicators across multiple sources to identify signs that suppliers may be experiencing difficulties or represent a greater risk of disruption / operational failure</td>
<td>A schedule of testing activities to ensure that suppliers are operating control environments appropriately to effectively manage business continuity</td>
</tr>
</tbody>
</table>

**Minimum:**
- Supplier documented BCPs (including supplier roles and responsibilities)
- Defined exit plan and exit strategy

**Recommended:**
- Develop effective and practical contingency plans
- Reference obligations contractually

**Minimum:**
- Performance management and regular SLA review
- Periodic financial stability monitoring

**Recommended:**
- Review enhanced datasets: draw insight from multiple sources
- Leverage leading indicators: enable a shift from reactive event response
- Continuous monitoring: augment existing time-bound practices with continuous monitoring tools

**Minimum:**
- Periodic BCP testing
- Enhanced due diligence and subsequent risk assessment activities through term of contract

**Recommended:**
- Frequent, scenario-based testing of BCPs to validate efficacy
- Periodic validation of contingency plans
Organisations must establish effective monitoring and oversight activities of their most critical suppliers, proportionate to the associated risks. Many recommended activities may already occur but not are not considered from an Operational Resilience perspective (see appendix 2).

**Recommended Approach**

- Move towards continuous monitoring activities
- Focus on leading indicators:
  - Financial distress
  - Deteriorating security posture
  - Performance issues
  - Emerging threats
- Focus on testing resilience plans:
  - Responding to tolerance breaches
  - Defining exit strategies
  - Testing validating of exit strategies
- Suppliers and subcontractors must be covered by these assessments

**Typical / Basic level**

**Required level for critical suppliers and services**

- Business Continuity Planning
- Third Party Oversight
- Supplier Risk Assessments
- Contingency Testing
- Performance / SLA Monitoring
- Financial Stability
- Negative Media
- Security Ratings
- Third Party Oversight
- Supplier Risk Assessments
11. Remediating Risk of Disruption

When organisational tolerance is breached, defined response measures should be in place to mitigate or limit the impact of disruption. Measures should be proportionate to the risk and differentiated depending on the severity of potential impact and the phase of the supplier relationship.

### Common pre-contract scenarios

- Define clear escalation and approval routes in event that contract decision may breach organisational appetite

#### Common Use Case

- **Supplier dependency / concentration** breached (e.g. too many critical processes being reliant on single supplier / subcontractor), such as with one of the major cloud service providers
- **Percentage of supplier turnover from a proposed engagement** breached, such as with a start-up engagement

#### Example Responses

- Implement mitigation strategies such:
  - heightened supplier continuity controls,
  - split services across multiple providers
  - introduce fail-over capacity with alternate providers
- **Defined contractual obligations**: written commitments aligned with exit strategies and/or target setting
- **Formal risk acceptance**

### Post-contract scenarios

Define clear escalation routes in event that supplier performance breaches organisational tolerance, aligned to ERMF risk mitigation processes

#### Requirement

1. **Root cause analysis and impact assessment to determine appropriate approach:**
   - Can tolerance breach be mitigated?
     - **Yes**? e.g. Identifying weaknesses in legacy systems, insufficient systems capacity, issues of availability, loss of key personnel. Implement programme of remediation tracked as part of SRM oversight routines
     - **No**? Consider invoking contingency strategies, including transitioning services in-house or to alternate provider

2. **Establish communication** with impacted stakeholder groups

3. **Identify any regulatory impacts** to ensure notification obligations are met

#### Example Mitigation Process
12. Managing Operational Resilience in the Supply Chain: Summary

Operational Resilience demands detailed assessment and continuous monitoring of suppliers supporting the delivery of critical and important business processes.

### Resilience Requirements

- Define organisational impact tolerance thresholds
- Review your supplier assessment processes and ensure they are accounting for likelihood, impact and aggregated factors
- Effective oversight should include continuous monitoring activities to provide true assurance on operational resilience
- Invest efforts in developing realistic and practical mitigation strategies to be deployed in the event of disruption events

### Supply Chain Impacts: Key Take-Aways

1. **Operational Resilience demands effective supply chain management:** be smart and coordinate work with Third Party / Supplier Management programmes
2. **Identify the really critical suppliers:** enhance understanding of services and suppliers and focus on the important few
3. **Leverage existing supplier management activities:** think creatively how to extract useful indicators for continuous monitoring
4. **Where monitoring activities do not happen today, invest wisely:** opportunities exist to invest in capability that will help with other supply chain challenges (e.g. Cyber/ Cloud/ Privacy)
5. **Test, test, test:** planning is not enough. Test overall resilience strategies and plans, not just supplier BCPs
<table>
<thead>
<tr>
<th>Factors</th>
<th>Questions</th>
<th>Where to capture</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Impact</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Process alignment</td>
<td>1. Are the processes being supported by the supplier business critical (i.e. would process failure cause material disruption to core business delivery in terms of income generation, client interaction, reputational damage, legal &amp; regulatory compliance or ability of organisation to realise strategic goals. Ideally this should map against an organisation’s ERMF impact and severity matrix) 2. How critical is the supplier to the operation of the process (i.e. could the process operate without the supplier or be transitioned to another supplier / internally within a reasonable timeframe)</td>
<td>Supplier Service Risk Assessment</td>
<td>Reliant upon mature business continuity function</td>
</tr>
<tr>
<td><strong>Concentration</strong></td>
<td>1. Does the supplier support multiple business processes as a 3rd / 4th+ party? (what is the aggregate dependency on the supplier across all processes?)</td>
<td>As part of enhanced DD if segmentation identifies supplier as critical</td>
<td>Capturing this detail is dependent on quality data to correctly identify the same supplier risk assessed for multiple engagements</td>
</tr>
<tr>
<td><strong>Service Complexity</strong></td>
<td>1. How complex is the service being provided? 2. Are there alternative providers that could support the provision of service? 3. How easily could the service be transitioned to either an alternative provider or internally?</td>
<td>Supplier Service Risk Assessment</td>
<td></td>
</tr>
<tr>
<td><strong>Geography</strong></td>
<td>1. What is the location of the supplier service provision? 2. Does service provision rely in operation across multiple countries / jurisdictions 3. How stable are the locations of operation? (consider political stability, including maturity of infrastructure and response to global events)</td>
<td>Supplier Service Risk Assessment</td>
<td>Location risks will obviously change constantly. Organisations should determine a data source that will reflect these changes</td>
</tr>
<tr>
<td><strong>Market</strong></td>
<td>1. Does the supplier operate in an industry sector that is prone to disruption? 2. What degree of specialism is involved in the provision of services (is there a degree of supplier IP and / or customisation involved in service provision not readily available in the market?)</td>
<td>Supplier Service Risk Assessment</td>
<td>Market sector risks will obviously change constantly and will overlap significantly with financial risk. Organisations should determine a data source that will reflect these changes</td>
</tr>
<tr>
<td><strong>Contract leverage</strong></td>
<td>1. Has the organisation negotiated appropriate contractual leverage with supplier? PH: I think this is probably about enhancing the contract review process for critical suppliers? 2. Does the supplier have significant dependency on the organisation to maintain turnover? (i.e. does the total contract value exceed X% of supplier’s income?)</td>
<td>Enhanced DD</td>
<td></td>
</tr>
</tbody>
</table>
Organisations must establish effective monitoring and oversight activities of their most critical suppliers, proportionate to the associated risks. Activities should enable a direct assessment of supplier performance against the organisation’s tolerance thresholds. The table below highlights example monitoring activities.

<table>
<thead>
<tr>
<th>Activity</th>
<th>Description</th>
<th>Applicability by Supplier Criticality</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Tier 4</td>
</tr>
<tr>
<td>Business Continuity Planning</td>
<td>Suppliers should maintain business continuity plans (BCPs) that outline measures to be taken to ensure continuity of service in the event of disruption • Do they meet requirements of consuming parties, aligned to contracts and internal BCPs of the consuming party? • Do they cover all plausible scenarios? • Are they being regularly tested to prove effectiveness?</td>
<td>N</td>
</tr>
<tr>
<td>Risk assessment</td>
<td>Periodic remote / onsite assessment of suppliers’ control environments to determine effectiveness and identify potential risks</td>
<td>N</td>
</tr>
<tr>
<td>Contingency Planning</td>
<td>Organisations should define alternative means by which processes can be operated in the event that suppliers are no longer able to support. This may include bringing services in-house, transitioning to alternative providers or changing the support profile</td>
<td>N</td>
</tr>
<tr>
<td>Performance / SLA Monitoring</td>
<td>Suppliers should be tracking performance indicators against agreed SLAs. • Is the supplier tracking an effective KPI set? • Do indicators suggest underlying issues with supplier that may lead to future disruption?</td>
<td>N</td>
</tr>
<tr>
<td>Financial Stability</td>
<td>Financial stability measures should be monitored to identify potential service disruptions • Are financial stability scores within appetite of consuming parties? • Does share price indicate investor concerns?</td>
<td>N</td>
</tr>
<tr>
<td>Security Ratings</td>
<td>Enable continuous monitoring of suppliers. Respond to changes significant changes in vector scores that may indicate changes in supplier circumstance and/or increased risk of disruption</td>
<td>N</td>
</tr>
<tr>
<td>Negative Media</td>
<td>Utilise news sources to monitor significant events that may indicate negative change in supplier circumstance, e.g.; • Turnover of key personnel • Sale of key assets • Delay in supplier payments</td>
<td>N</td>
</tr>
</tbody>
</table>

Dashboard

1. Dashboard should focus on most critical suppliers
2. Key metrics used to inform performance against organisational tolerance and indicate where intervention measures may be required
This document and any attachments are confidential and intended solely for the addressee and may also be privileged or exempt from disclosure under applicable law. If you are not the addressee, or have received this document in error, please notify 3VRM immediately, delete it from your system and do not copy, disclose or otherwise act upon any part of this document or its attachments.

Internet communications are not guaranteed to be secure or virus-free. 3VRM Limited does not accept responsibility for any loss arising from unauthorised access to, or interference with, any Internet communications by any third party, or from the transmission of any viruses.

3VRM Limited,
Registered in England and Wales (registered no. 10097443).