CAPCO

# GETTING THE MIX RIGHT

## A LOOK AT THE ISSUES AROUND OUTSOURCING AND OPERATIONAL RESILIENCE

# SPEED READ

- The use of third parties to outsource elements of critical services brings challenges around the resilience of the service but can also improve the situation.
- The key is to ensure that the third party has the capability to respond to events and the firm has sufficient control over the recovery.
- Third parties should be fully integrated into firms' operational resilience plans.

# INTRODUCTION

As part of their efforts to improve the resilience of financial services, regulators are focusing on outsourcing to third parties and how firms manage the risks that arise when those third parties are incorporated into the processes that underpin the delivery of services.

Two specific developments over the last decade are coming under scrutiny in order to reach a better understanding of their impact on the resilience of the sector:

- Greater use of third parties such as fintechs in the delivery of key services
- Use of Cloud computing within technology architecturer

It was notable that the UK PRA published a consultation paper on Outsourcing and Third Party risk management on the same day as similar papers on operational resilience in December 2019.

In this paper we will focus on how firms should engage with third parties that are involved in the delivery of Important or Critical Business Services via Capco's three-phase approach to operational resilience – Prepare, Manage and Learn. We will look at practicable steps that firms can adopt to better align third parties with their operational resilience environment as well as meet the regulators' expectations of how those third parties are managed.

The engineering elements around improving resilience through the design of a firm's technology platform will be covered in a subsequent paper.

# DEFINITIONS

The UK regulators have defined outsourced third-party services as those that would ordinarily be carried out by the firm in the delivery of the services that it offers. They further define material outsourcing to be where the weakness or failure of the service would make it unlikely the firm could meet its regulatory obligations. This, by default, includes delivering Important Business Services within impact tolerances. As a result the incoming Operational Resilience regulation will raise the requirements relating to how firms engage with third-party outsourcing providers.

We suggest that firms can define third-party outsourcing providers as those entities directly involved in delivering any services that the firm itself does not control directly. This definition has a broader applicability covering internal outsourcing while also being applicable to all manner of regulated firms. It is also more coherent approach when viewed through the lens of the UK Senior Managers and Certification Regime.

# PRINCIPLES

From an operational resilience perspective, when stripped down to basics there are two primary elements that firms need to be cognizant and comfortable with when outsourcing to a third party:

- Capability – does the third party have the necessary resources and management in place to continue to satisfy the contractual agreements/SLAs when disruptive events strike?
- Control – in the event of disruption, will the needs of the firm be appropriately prioritized by the third party in terms of resuming services?

The key requirement is that where a firm uses a third party to deliver an Important Business Service , at a minimum the service provider should be able to offer the same level of preparedness and capability to cope with disruption as the firm itself were the function not outsourced. This is particularly relevant when the third party is not a regulated entity.

If a third party further outsources (sub-outsources) parts of the delivery process to a fourth party then the same standards should apply to that party. The service provision should be viewed end-to-end.

Internal third parties should be assessed in the same way as their external counterparts in terms of capability and control. A working definition for internal outsourcing is where the legal entity providing the services is different to that transacting the business. This can be tempered if the entity providing the service is regulated in the same jurisdiction, or if the service provider is a subsidiary.

From a control perspective, there should be a documented agreement around prioritisation that is defined at the level of management and covers both the reporting and servicing legal entity. Providing that the resilience capability is sufficient, this could be that the recovery time is common to all legal entities using the service; or that if a limited service is provided, then it should be in proportion to use of that service by each legal entity.

It should be recognized that, for firms that are headquartered outside the UK, greater control may be exercised contractually over an external third party than an internal one.

# PREPARE

Once Important Business Services have been identified and the delivery processes behind them mapped, the degree of involvement by third parties will become apparent. The first step is to ensure that any contractual agreements support the impact tolerances set for that service in terms of elements such as the agreed recovery time objectives (RTO). To understand the capabilities of the third party, firms should seek to understand:

- How is the service to be delivered? This is to identify the macro interaction with the firm if disruption strikes, so factors such as location, platform used and any sub-outsourcing need to be considered. These should be considered to reduce the impact of disruption as well as for inclusion in plans around incident management.

- What are the third party's plans to cope with disruption, including how it will be managed, what resources they can deploy, how often do they rehearse responding to disruptive events, what scenarios do they expect to be able to cope with in order to continue to deliver the service? This will give a good idea of whether they can meet their obligations as set out in the contract.

- Which other firms that use the service are covered by the same set of resources. While third party systemic concentration risk is primarily the responsibility of the regulators, it is prudent for firms to factor it into their planning. It is also important to understand how a third party will prioritise individual clients' recoveries if the service is disrupted.

These points should also be covered by any assurance activity (either commissioned by the firm or pooled) that reviews the third party and the effectiveness of its operational resilience capabilities. There should also be a mandatory requirement for the third party to notify the firm in good time of any material changes to how services are delivered or their resilience capability. It is worth pointing out that firms should inform their regulators of significant changes to their material outsourcing arrangements well in advance so that a review of the firm's new risk profile can take place.

Scenario Testing should actively – and transparently – include input from third parties where they perform part of the delivery process being assessed. The involvement of third parties in delivering important business services should be set out in the operational resilience self-assessment document.

The UK regulators are likely to mandate some form of f outsourcing register to address the concentration issue that will help with this. Proposals are contained within the EBA Guidelines on Outsourcing Arrangements in section 11 (published in February 2019) that the UK regulators are likely to adopt. The information fields required are listed in the Appendix (and due to come into force in the EU at the end of 2021). The register should be available for review by the regulators, and the PRA are looking at some form of online portal to allow the creation of a market wide picture.

Data security is a key consideration. It goes without saying that if a third party needs to hold sensitive data on behalf of the firm, then the controls around that data must be at least as strong as the firm's own controls. Testing should confirm this and can include techniques such as ethical hacking. This should not just cover the data storage and usage at the third party, but also the security of the transfer mechanism.

Many regulated firms will also provide services to other regulated firms, and accordingly will likely be receiving requests for details of their own resilience capabilities for the services they offer. This will push these firms to comply early with the regulation, as well as increasing the number of important business services to meet the needs to their clients. Sharing this level of detailed information required may make firms uncomfortable, at least initially, particularly where their client is also a potential competitor in another market.

Given the number of third parties (and potentially 4th and 5th parties) involved in the processes that deliver important business services, firms should not underestimate the amount of effort and time required to get third parties into the 'right place' to meet the operational resilience regulations.

# MANAGE

The key assumption underlying all aspects of operational resilience planning and execution is that disruptive events will happen – often in unpredictable and unforeseen ways and, for all the preparations made, some degree of disruption is inevitable and firms will be expected to remain within impact tolerances. If third parties are involved in delivering Important Business Services then they need to be properly integrated into the planning and response to potential events.

**Early identification of issues.** If there is disruption to a service, the more notice management can have of impending issues, the more likely it is that the impact tolerance will not be breached. To that end, upstream process performance metrics need to be fed from the third party to the firm, including indications of when the service is suffering from disruption. The nature of the service being provided will determine the exact nature of the metrics being shared, but they should be as far up the delivery process chain as possible. If that data is not received, this should be taken as an indication that the service is being disrupted, triggering management attention and action.

**Coordination.** Once disruption strikes, the team that is responsible for the recovery of the compromised process needs to act coherently and quickly, communicating effectively. Depending on nature of the process that is outsourced, a representative of the third party should ideally be part of the committees coordinating the response. At the very least, there should be a direct link between the teams within the firm coordinating the response and the team at the third party responsible for running and recovering the service. This should not be channeled through a relationship manager or helpdesk in ensure minimal delay in the flow of information.

**Redundancy.** In an ideal world if a third party fails to perform the services as contracted, a firm would be able to seamlessly 'fail over' to either an internal resource provider or a different provider altogether. This can be expensive and time consuming, so while it is an option that can and indeed should be considered for the most critical services, it is not going to be practicable for every third-party outsourcing engagement (and is particularly complex to execute for certain services such as cloud computing).

If this path is chosen there are several considerations that should be addressed:

- Maintaining currency. The back up system needs to be a mirror with the same functionality and data, and with very low latency of update, to be effective. The accuracy of the output needs to be validated on a very regular basis. Ideally the back-up and primary system should be 'swapped' on a frequent basis to ensure effectiveness.

- Contagion. In some circumstances, if there are common elements between the primary and back-up systems, then there is a risk that what effects one will affect both, thereby cancelling out the benefit of the back-up.

- Decision to cut over. Where a regular, scheduled cutover approach (as outlined in point one) is not adopted, then the delegation rights of who can trigger a cutover should be clearly delineated alongside the information triggers that would prompt such action.

If firms do not decide to maintain a 'mirror provider' for a third party in respect of a critical service, they should at the very least address what they would do if the third party fails to perform and is unable to restore services.

# LEARN

Identifying the lessons from previous events that have impacted the firm and other organisations is key to ensuring ongoing resilience. Once a relevant event or threat has been identified, the third parties that are involved in delivering Important Business Services should be included in the analysis of how the delivery process would be potentially impacted, and how any vulnerability could be mitigated.

The incoming UK operational resilience regulations mandate an annual self-assessment process. This should include a review of events and emerging threats as well as scenario testing. Third parties that are involved in delivering Important Business Services should by necessity be included in this process. They should also be asked to confirm that there have been no changes to the elements of the service that they had initially confirmed.

Firms should include the operational resilience criteria in their third party management policies and on-going management of these arrangements. These should clearly indicate who has responsibility for the control of the third party, including the approval process for change. The policy should also mandate the regular review of third party resilience metrics.

# CONCLUSION

The expansion in the use of third parties to deliver key services only looks set to continue as firms focus on competitive advantage and cost reduction. While this undoubtedly creates challenges in an operational resilience context, some changes – such as migration to the cloud – should have the effect of hardening delivery processes and improving overall resilience.

With careful management, and by incorporating operational resilience considerations into the conversation right from the outset, outsourcing to third parties is not inimical to the reliable delivery of important or critical services. However uplifting firms' engagement with their outsourced third parties is likely to be a significant undertaking for most firms, and they will need to give consideration as to how this is factored into their timelines and budgets in order to meet the incoming regulations.

# APPENDIX 1

## Key Operational Resilience Third Party Concerns

| **Prepare** for Operational Resilience | **Manage** a disruptive event | **Learn** from past events and threats |
|---|---|---|
| • How and where is the service being delivered by the third party? | • How is service/performance being monitored by the firm? | • How regular is service/ performance being monitored and assessed by the firm? |
| • What are the third party's plans to cope with disruptions? | • How is the third party involved in the management of a disruption? | • How is the third party involved in the improvement of controls/processes post analysis of a disruptive event/ threat? |
| • Which other firms utilise the third party for the same service? | • How does the firm deal with the third party's redundancy? | |
| • How can the third party be involved in scenario testing? | | |

**Key TPRM Considerations**

# APPENDIX 2

**Verbatim List of Information to be Included in Register of Outsourcing as per EBA Guidelines on Outsourcing Arrangements. The headings are a useful guide for firms of the basic information from third parties.**

**1.** The register should include at least the following information for all existing outsourcing arrangements:

**a.** a reference number for each outsourcing arrangement.

**b.** the start date and, as applicable, the next contract renewal date, the end date and/or notice periods for the service provider and for the institution or payment institution.

**c.** a brief description of the outsourced function, including the data that are outsourced and whether or not personal data (e.g. by providing a yes or no in a separate data field) have been transferred or if their processing is outsourced to a service provider.

**d.** a category assigned by the institution or payment institution that reflects the nature of the function as described under point (c) (e.g. information technology (IT), control function), which should facilitate the identification of different types of arrangements.

**e.** the name of the service provider, the corporate registration number, the legal entity identifier (where available), the registered address and other relevant contact details, and the name of its parent company (if any).

**f.** the country or countries where the service is to be performed, including the location (i.e. country or region) of the data.

**g.** whether or not (yes/no) the outsourced function is considered critical or important, including, where applicable, a brief summary of the reasons why the outsourced function is considered critical or important.

**h.** in the case of outsourcing to a cloud service provider, the cloud service and deployment models, i.e. public/private/hybrid/community, and the specific nature of the data to be held and the locations (i.e. countries or regions) where such data will be stored.

**i.** the date of the most recent assessment of the criticality or importance of the outsourced function**.**

**2.** For the outsourcing of critical or important functions, the register should include at least the following additional information:

**a.** the institutions, payment institutions and other firms within the scope of the prudential consolidation or institutional protection scheme, where applicable, that make use of the outsourcing.

**b.** whether or not the service provider or sub-service provider is part of the group or a member of the institutional protection scheme or is owned by institutions or payment institutions within the group or is owned by members of an institutional protection scheme.

**c.** the date of the most recent risk assessment and a brief summary of the main results.

**d.** the individual or decision-making body (e.g. the management body) in the institution or the payment institution that approved the outsourcing arrangement.

**e.** the governing law of the outsourcing agreement.

**f.** the dates of the most recent and next scheduled audits, where applicable.

**g.** where applicable, the names of any sub-contractors to which material parts of a critical or important function are sub-outsourced, including the country where the subcontractors are registered, where the service will be performed and, if applicable, the location (i.e. country or region) where the data will be stored.

**h.** an outcome of the assessment of the service provider's substitutability (as easy, difficult or impossible), the possibility of reintegrating a critical or important function into the institution or the payment institution or the impact of discontinuing the critical or important function.

**i.** identification of alternative service providers in line with point (h).

**j.** whether the outsourced critical or important function supports business operations that are time-critical.

**k.** the estimated annual budget cost.

# AUTHOR

**Will Packard,** Managing Principal
Will.Packard@capco.com

# ABOUT CAPCO

Capco is a global technology and management consultancy dedicated to the financial services industry. Our professionals combine innovative thinking with unrivalled industry knowledge to offer our clients consulting expertise, complex technology and package integration, transformation delivery, and managed services, to move their organizations forward.

Through our collaborative and efficient approach, we help our clients successfully innovate, increase revenue, manage risk and regulatory change, reduce costs, and enhance controls. We specialize primarily in banking, capital markets, wealth and asset management and insurance. We also have an energy consulting practice in the US. We serve our clients from offices in leading financial centers across the Americas, Europe, and Asia Pacific.

To learn more, visit our web site at www.capco.com, or follow us on Twitter, Facebook, YouTube, LinkedIn and Instagram.

# WORLDWIDE OFFICES

**APAC**
Bangalore
Bangkok
Gurgaon
Hong Kong
Kuala Lumpur
Mumbai
Pune
Singapore

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

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

**SOUTH AMERICA**
São Paulo

**WWW.CAPCO.COM**

CAPCO



JN_2921