Considerations for firms thinking of using third-party technology (off-the-shelf) banking solutions

Introduction

1. A firm has many choices when designing its operating model and setting its IT strategy. It may choose to develop and operate its own technology solutions but the choice of a third party to provide some or all of its technology needs is also a viable option. This market continues to evolve rapidly and new offerings and innovative ways of delivering these services appear regularly.

2. Where a third-party service is critical to a regulated firm's business operations, the service provider will be regarded as an outsource service provider (OSP) and the regulated firm is subject to a series of regulatory obligations.

3. In this document, we provide a list of questions for a firm to consider as part of its preparations for the use of and the evaluation of third parties in the delivery of technology services which are critical to the regulated firm's business operations (critical technology services).

4. It should be noted that this document does not represent a complete list of all matters that a firm should consider in preparing its third-party arrangements or all matters that will be considered by the regulator(s) when assessing an application for the delivery of regulated services.

5. This document does also not seek to replace the wider IT matters which are assessed by the regulator(s) when a firm submits an application for undertaking a new regulated business activity.

Outsource service regulatory requirements

6. From a business operating model perspective, the key formal regulatory requirements are that a firm can demonstrate that it meets our threshold conditions as described in COND 2.4 Appropriate Resources and COND 2.5 Suitability. Where a firm uses a third party for the delivery of critical banking services, then a firm must also comply with SYSC 8.1 General outsourcing requirements.

7. From an outsourcing perspective, the overall aim of these regulatory obligations is that a firm appropriately manages the operational risk associated with its use of third parties and the arrangements with third parties do not impair the regulator's ability to regulate the firm.

8. In practical terms, we are looking for the following outcomes:

- At the time of authorisation, a firm's regulated activities must be supported by IT services which are effective, resilient and secure and have been appropriately designed to meet expected future as well as current business needs so as to avoid risks to our objectives.

- The firm must have undertaken sufficient preparatory work to provide reasonable assurance that each OSP will deliver its services effectively, resiliently and securely.

- The firm has established appropriate arrangements for the on-going oversight of its OSPs and the management of any associated risks such that the firm meets all its regulatory requirements.

9. Above all, a regulated firm should be clear that it retains full accountability for discharging all of its regulatory responsibilities. It cannot delegate any part of its responsibility to a third party.

Considerations for firms

Decision to outsource critical technology services

Area of interest	Notes
Decision to outsource	Is there a clear business case or rationale supporting the decision to use one or more third parties for the delivery of critical technology services? Has this decision included consideration of the business risks associated with use of third parties?

Selection of Outsource Service Provider (OSP)

Area of interest	Notes
Commercial arrangements	What pricing model(s) does the service provider offer? How flexible are these? Do the arrangements include software upgrades or are these priced separately?
Solution selection	Many solutions require tailoring to meet UK and firm requirements. Is anyone else in the UK using the proposed solution? Will the service provider change its solutions to meet the firm's needs? What degree of change is required to meet the firm's needs? How long will it take to deliver the solution? Can data be readily extracted from a service provider's systems and downloaded to a firm's own systems? Do each service provider's solutions provide comprehensive and flexible reporting capabilities that can be readily used by a firm?

Area of interest	Notes
Relationship between service providers	Many service providers specialise in particular service offerings and do not provide a complete solution. This means that a firm may have more than one service provider. How will service providers work together (e.g. will the firm or one service provider take the lead systems integration role)? How easily will a service provider's solutions interface with a firm's internal systems or other third-party systems (such as agency banking arrangements for payments)? How will end to end testing of the proposed solution be carried out?
Change management	What provision has been made for making future changes to technology service provision? Who will own the intellectual property rights for changes? How will testing of changes be carried out?
Due diligence	Does each OSP have a sustainable business model (e.g. is the service provider financially and operationally viable)? Does each OSP have the ability, capacity and any authorisation required by law to perform the outsourced functions, services or activities reliably and professionally? Is there a cultural fit between the firm and the service supplier(s)?
Track record	Can each service provider demonstrate a track record of successful deployments in the UK? Are there reference sites which a firm can visit?
Multi-tenancy	A third-party provider of hosting services may propose that many customers share the same infrastructure to provide cost benefits. How will a firm ensure that its data is segregated and secure? How will a firm ensure that its systems are reliable and not at risk of performance impairment due to other clients of the service provider? How will a firm ensure that access to its systems is appropriately managed? What is the extent of the concentration risk (i.e. many competitors using the same service provider and technology) and is this acceptable?
Exit Plan	Firms should ensure there is an Exit Plan is in place for when their relationship with the supplier comes to an end. How will a firm transition to an alternate service provider? How will a firm get its data back? How will the data be removed from the service provider's systems?

Oversight and Governance

Area of interest	Notes
Oversight of service provider	A regulated firm retains full accountability for discharging all of its responsibilities under the regulatory system. It cannot delegate this responsibility to a service provider. How will a firm oversee the services provided by an OSP (this includes monitoring financial and operational performance, determining appropriate management actions where necessary to address any risks and issues, and the approach to the engagement with the supplier)? Who will have responsibility for the day-to-day and strategic management of the service supplier? Do the firm's staff have the appropriate skills to perform the oversight role effectively? What arrangements have been made for dispute resolution? What management information will be required to support management of the service provider and will this be available in a timely fashion? Will the service provider be subject to independent reviews or audits such as ISAE 3402? If not, will the firm conduct its own audits? What is the relationship between the firm and service provider (e.g. transactional or partnership) and is this appropriate for the firm's objectives?
Service levels	Are the arrangements with each service provider supported by service level agreements (SLAs)? Are the SLAs contractually agreed? Are SLA objectives SMART (Specific, Measurable, Appropriate, Realistic, Timely)? Can a service supplier demonstrate a history of performance against any proposed service levels? Does the service provider provide the capability for a firm's users to monitor performance against SLAs?
Risk management	How will a firm assess the operational risks associated with each service supplier and the overall operational risks associated with the regulated service for which the firm is responsible? Who will have responsibility to ensure that operational risks are managed appropriately?

Operational

Area of interest	Notes
Support	Who will support the technology solutions? Do the arrangements for support meet the firm's needs?
Maintenance and upgrades	Are there clear arrangements for systems maintenance and upgrades? Who authorises the application of patches and upgrades? Does the service provider propose to automatically apply any patches and upgrades?
Scalability	Can a service provider's solutions be readily scaled to meet the forecast increase in demand as the firm grows?
Quality of service	Has a target quality of service been agreed? Do arrangements with third parties support the realisation of the firm's quality of service objectives? Has responsibility for quality of service been assigned? What arrangements are in place to monitor service provider performance and overall quality of service? Are there appropriate tools to support monitoring of quality of service?
Incident management	Have the firm's and service provider's responsibilities been agreed in the event of an incident? Have responsibilities been agreed where there is more than one service provider?
User administration	Who administers user access to third-party service solutions? Are arrangements in place to ensure the administration of the access rights of joiners/movers/leavers is carried out in a timely manner?

Service protection

Area of interest	Notes
Security	Has a security risk assessment taken place which includes services provided by third parties and the firm's technology assets which are administered by third parties? Have an appropriate mix of measures been put in place to mitigate security risks such that the firm's overall security exposure is acceptable? Has responsibility for security been assigned? Are there appropriate tools to support monitoring of security?

Resilience/disaster recovery	Have service availability requirements been specified and agreed with service suppliers? What steps have been taken to prevent service outages? Do the firm and each service supplier have their own disaster recovery plans? Are the disaster recovery plans aligned with one another? Have all disaster recovery plan been successfully tested? Will all disaster recovery plans continue to be regularly (at least annually) tested and on major service changes? Do the disaster recovery plans meet the firm's needs (i.e. are recovery times acceptable)? Have the firm considered alternative arrangements should the service provider's disaster recovery plans not be effective when needed?
Penetration testing	Has penetration testing been carried out? Are there arrangements in place for regular penetration testing?

Data

Area of interest	Notes
Data protection	Is the firm's data segregated? Is the firm's data encrypted during transmission? Is the firm's stored data encrypted? Is data held in an acceptable jurisdiction? Is data processed in an acceptable jurisdiction? How will the data be removed from the service provider's systems when it is no longer needed? Is the data being held and processed in compliance with the Data Protection Act?