Operational Resilience and third party service provision and outsourcing – the new normal

January 2020

CharlesRussell Speechlys

In December 2019, the Bank of England, Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA) published consultation papers to implement a stronger regulatory framework to promote greater operational resilience of regulated firms and financial market infrastructures (FMIs).

The papers build on the joint discussion paper 18/04 published in July 2018 "Building the UK financial sector's operational resilience" and also recent initiatives by other regulators, including final guidance by the European Banking Authority (EBA) on outsourcing (February 2019) and ICT and security risk management (November 2019).

The papers will be carefully scrutinised by regulated firms, but also have important consequences for vendors who will provide services to regulated firms (directly or indirectly) with regard to important services, and also potentially extend the reach of regulation on outsourcing into the PRA regulated sector in a manner consistent with recent changes to the banking and payments sectors.

What are the new papers?

Instead of a single paper building on the July 2018 discussion paper, the supervisory authorities published the following:

- Overarching joint paper issued by Bank of England, PRA and FCA "Building Operational Resilience: Impact Tolerances for Important Business Services" - This contains a summary of the supervisory authorities' objectives to protect and enhance the financial stability of the United Kingdom. The real economy relies on the wider financial sector, particularly providing the main mechanism for paying for goods services and financial assets, intermediating between savers and borrowings and channelling savings into investment, and ensuring against and disbursing risk
- CP29/19 issued by the PRA "Operational Resilience: Impact Tolerances for Important Business Services"
- CP30/19 issued by the PRA "Outsourcing and Third Party Risk Management"
- FCA CP19/32 issued by the FCA "Building Operational Resilience: Impact Tolerances for Important Business Services and Feedback to DP18/04".

In addition, there are individual consultation papers and draft supervisory statements issued by the Bank of England for central counterparties and central securities depositories, and a further consultation paper and draft supervisory statement and chapter of the Code of Practice for recognised payment systems operators and specified service providers, but these are not within the scope of this note.

To whom do the papers apply?

The PRA paper is relevant to firms regulated by the PRA being:

- **Banks** - UK banks, Building Societies and PRA designated investment firms
- **Insurers** - Solvency II firms and the Society of Lloyds and its managing agents.

The FCA paper is relevant to Banks, Building Societies, PRA designated investment firms, Solvency II firms recognised investment exchanges enhanced scope senior managers and certification regime (SM&CR) firms and entities authorised or registered under the Payment Services Regulations 2017 and/or Electronic Money Regulations 2011.

The scope of the papers relates to the UK, and not to EEA firms. There are different versions of the draft instruments at the end of the paper according to Brexit impact.

The FCA estimates approximately 1050 regulated firms and 1,100 firms and institutions affected by payments regulations will be covered by its regulation.

The papers are open for consultation responses due on 3 April 2020.

What is the purpose of the papers?

Financial services is not only critical to the health of UK economy as an important business sector (that constitutes critical national infrastructure), but it also provides the means by which the economy transacts business, and manages wealth. Recent IT failures including the TSB IT failures on the cut-over of systems to the new bank, together with concerns at a macro level on power and energy shortages, and cyber risks have prompted a greater focus on resilience within the financial services sector.

The joint paper specifically mentions the Treasury Select Committee report on "IT failures in the financial services sector" which was published following the recent IT failures, including TSB, which included recommendations to improve operational resilience in the financial sector. The supervisory authorities have promised to provide a full response to the Treasury Select Committee's recommendations in due course, indicating that the operational resilience agenda will continue to develop and require continuous improvement from firms in the years to come.

According to this joint paper (paragraph 1.12) "*The result of implementing the proposals should be that when a disruption occurs, firms and FMIs will have robust and reliable arrangements in place to deal with it. These arrangements will have previously been tested. Firms and FMIs will also be able to show that they are operationally resilient, both to themselves and to the supervisory authorities. The proposals are designed to promote stronger and more effective governance of operational resilience and more organisation and co-operation between market participants*".

Consistent with data protection obligations for data protection by design and by default in systems which process personal data, it may be that more robust definitions of "operational resilience by design" or similar concepts creating a mind-set of resilience may emerge. It is obvious but important to note that the regulators each frame their resilience requirements in the light of the fundamental obligations which they exist to protect.

Vendors will need to address these fundamentals also in the design and operation of systems in order to address real risks and resilience requirements in the financial sector. It is clear that the regulators recognise the danger of IT and other operational disruptions to the financial services regime more explicitly, and have set clear goals to address system resilience. This does not just include technology failures but also covers changes to systems and transformation projects, mergers and acquisitions, outsourcing and insourcing, as well as events which are outside the direct control of regulators, including cyber, communications risks, power failure and (although not explicit) potentially energy shortages (which will affect the infrastructure which operates the financial services).

Perhaps the greatest change resulting from operational resilience is the cultural change required to address operational resilience. This requires improved oversight and governance, and creates an outcome-based approach to business resilience. Therefore the papers identify the outcome of operational resilience, and not just the activities of what organisations must do on a day-to-day basis to run their business.

Operational resilience is defined in broad terms. In the FCA consultation paper "*operational resilience is the ability of firms and the financial sector as a whole to prevent, adapt, respond to, recover and learn from operational disruptions. Operational disruptions on the unavailability of important business services have the potential to cause wide-reaching harm to consumers and market integrity, threaten the viability of firms and cause instability in the financial system. This will require a proportionate approach from regulated firms*".

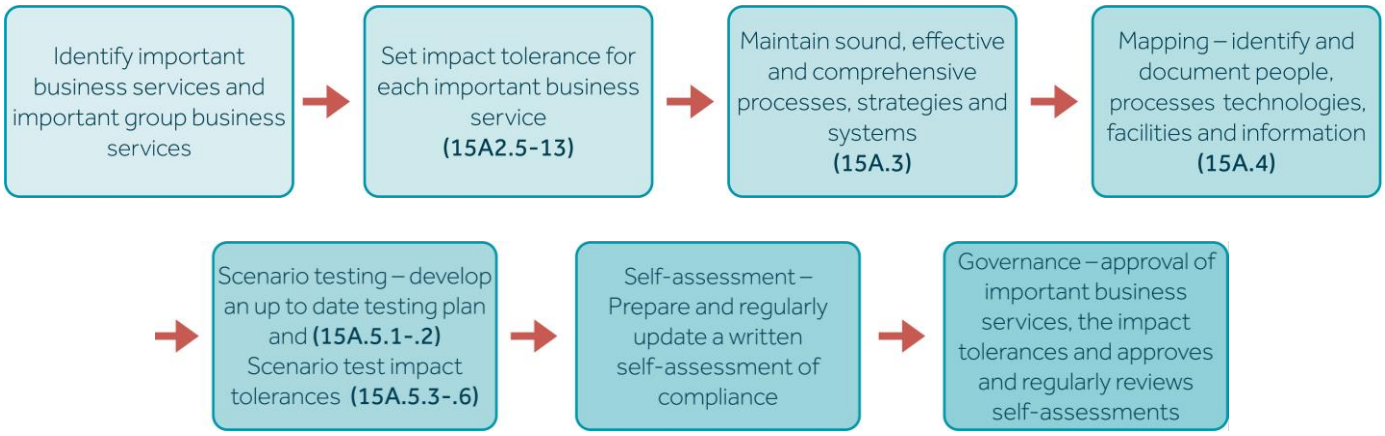
This is totally desirable but will mean that vendors providing services to regulated firms will have to adapt their services to individual customer requirements and tolerances, and no "one size fits all" or "operational resilience in a box" is likely to result. Vendors will have to address issues regarding outsourcing, supply chain risk and concentration risk in a more formalised manner. These requirements are well understood from the previous regulatory regime but the outcome-based nature of the results will clearly require improved governance within firms and the financial ecosystem, as well as perhaps more constructive ways of working between vendor and customer communities. While there may not be many additional contractual requirements solely as a result of the operational risk agenda (as distinguished from outsourcing), the level of scrutiny, and perhaps frequency of audits and information requests and requirements to gather evidence for self-assessment could add to cost and overhead for vendors, all of which will have to be paid for ultimately by firms, and thereby the public at large.

Vendors should scrutinise the papers to look at the cost of acquiring new business, increased scrutiny at bid stage, and scrutiny on changes in supply chain e.g. changes to subcontractors will become more burdensome to administer during the life of contracts.

It is hoped that while each regulated firm will take a proportionate approach to the operational resilience agenda, the outcome-based nature of the requirements may lead to some "gold plating" by firms, and will require new metrics to be developed to measure failure risk, and outsourcing risk. Suppliers covering both insurance and prudential services as well as FCA businesses may find benefits in a more harmonised regime overall.

What do the papers cover?

Both PRA and FCA papers adopt a similar approach to the requirements. The diagram below shows a summary of the requirements, taken from the FCA's draft SYSC Handbook wording. The PRA requirements are similar but do not have express communication requirements.



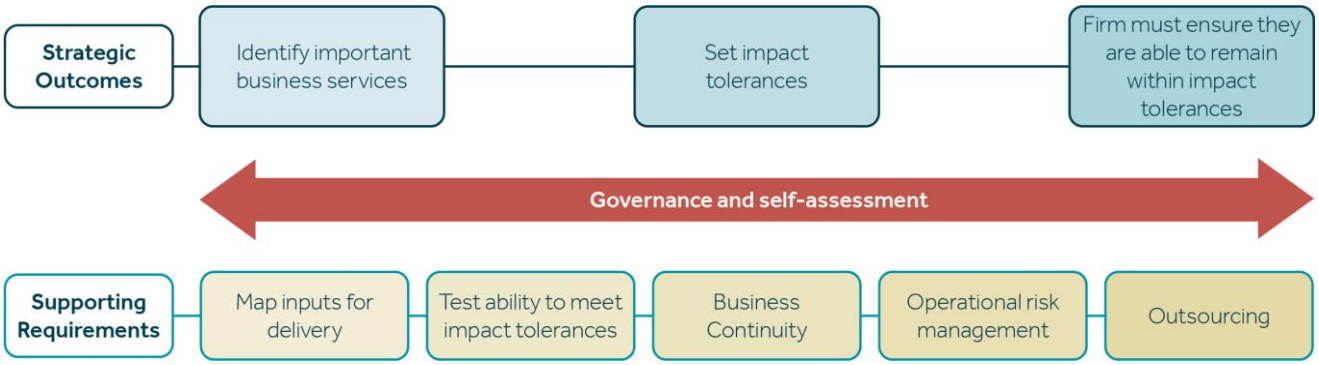


**Diagram taken from Figure 1: Startegic outcomes and supporting requirements for operational resilience policy, CP29/19 issued by the PRA "Operational Resilience: Impact Tolerances for Important Business Services", page 3*

The PRA includes a very helpful visualisation of operational resilience, setting out the strategic outcomes and supporting requirements to achieve these. This gives a clearer visualisation of the outcomes of operational resilience, compared with the process based approach that the PRA and FCA rulebook text.

Summary of requirements
Firms must:

- identify their important business services, services that if disrupted could cause harm to consumers or market integrity (FCA) or which could pose a risk to a firm's safety and soundness or the stability of the UK's financial system or, in the case of insurers, appropriate policy holder protection (PRA). The rulebook for the FCA contains specific factors that the FCA regulated firms should consider in assessing important business services
- set impact tolerances for each important business service (thresholds for maximum tolerable disruption)
- set measures to remain within impact tolerances
- manage and measure compliance regularly using self-assessment and where outsourcing or using third party providers, comply with detailed outsourcing and supply chain controls.

These requirements will be subject to full governance and self-assessment by the regulated firms. They are summarised in the diagram above but involve both mapping, testing, and integration of the operational resilience within business continuity, disaster recovery, operational risk and outsourcing thresholds. The emphasis of the regulators is that the cycle should be perpetual, enabling firms to test the ability to remain within impact tolerances through disruption scenarios, to then conduct lessons learned exercises and self-assessment which will identify, prioritise and invest in the ability to respond and recover from disruptions as effectively as possible.

Identify Important Business Services
Operational risk is determined by reference to "important business services which will need to be formally identified and mapped". In the proposals, an important business service will be:

Important Business Service: means a service provided by a firm or FMI to an external end user or participant where a disruption to the provision of the service could cause intolerable harm to consumers or market participants; harm market integrity; threaten policy holder protection; safety and soundness; or financial stability.

It is important to note that business services are not just single functions, and therefore each firm will have a significant task to identify these services – a business service is a service that a firm provides to an external end user or participant. These

services deliver a specific outcome or service, and therefore will not necessarily be the same as lines of business e.g. retail mortgages, which can comprise a collection of services and activities.

There is no specific number of important business activities that a firm must identify, but a recent UK Finance webinar suggested perhaps as many as 50 important business functions for a larger firm and 10 to 20 important business functions for a smaller market participant would not be surprising.

Set impact tolerances

Once the important business services have been identified, impact tolerances must be set. These are a firm's maximum tolerance for disruption to a particular business service.

The regulators' aim is to increase board level engagement to set these tolerances, moving away from traditional risk management (business continuity/ disaster recovery) towards the need to accept that disruption to business functions is inevitable, and will need to be managed actively when it occurs.

Whilst the aim of most businesses should be to design services to prevent risk occurring in the first place, the regulators wisely acknowledge that some business disruption is inevitable, and therefore that maximum tolerable disruption impact tolerances will need to be set by a "clear metric", in the PRA's words. These will obviously be determined according to the business function but can be set according to appropriate factors such as numbers (e.g. numbers of consumers affected), financial loss, time to recover, but also softer factors such as reputational impact, and in the PRA's case to be set according to "other relevant factors". In essence, the impact tolerances should be set at the point of which disruption to a firm's important business services could constitute a risk either to the firm's safety or soundness or financial stability or similar factors. Firms will set and review impact tolerances once a year, or more frequently on material change to the business or economic environment.

Note that it remains the obligation of the firm to meet its regulatory requirements, but vendors will no doubt be expected to provide assistance with definition of these impact tolerances, but this will be without prejudice to the wider obligations of the regulated firm to set its broader business continuity and risk management objectives. However, firms relying on outsourced platforms or single points of failure in systems will expect strong SLAs and impact tolerances to be replicated in contracts.

This will mean potentially entrusting suppliers with very confidential information of what these tolerances are, and therefore suppliers will have - in some cases - a better view of the overall impact tolerances in the industry than individual firms. The regulator may have a similar macro view if the information it receives is sufficient and consistent. There may need to be a robust addressing of who holds the balance of power in the relationship (whether this is vendor or customer) and how much vendors will engage with the regulatory agenda in spirit as well as according to strict contractual requirements.

Mapping and scenario testing

An operationally resilient firm will be expected to have "a comprehensive understanding and mapping of the systems and processes that support their business processes" (FCA paper 6.1). This expressly includes outsourcing and third party service provision relationships. Many businesses will have conducted some mapping as a result of GDPR or for recovery and resolution objectives, but the exercise expected here is potentially different. Mapping will require firms to identify and document people, processes, technology, facilities and information ("resources") needed to deliver important business services. The aim is to identify vulnerabilities within the set impact tolerances and then to take steps to remedy these.

It is clear that there will be significant argument in contract negotiations on who pays to resolve vulnerabilities, and whether these vulnerabilities will be in scope for a particular vendor or group of vendors given that contracts will not map easily to business services. Vendors will have to pay careful attention to how vulnerabilities are addressed as in many cases, as they will not be in full control of the systems that deliver specific important business functions. However, the guidance does offer

detailed assistance here in relation to issues that can constitute vulnerabilities, and therefore these will form a useful ground for negotiations on this difficult subject. Vulnerabilities include lack of substitutability, high complexity of services, single points of failure, concentration risk, third party relationships and force majeure/circumstances beyond the control of customers.

Once mapped, scenario testing will be necessary to confirm that firms are able to meet impact tolerances. Assistance with scenario testing may also need to be built into contracts as an obligation similar to audit obligations. The regulators recommend that firms develop testing plans to detail how they will gain assurance so that they can remain within impact tolerances. The testing plan should consider the following (according to the FCA):

- the type of scenario testing, for example whether paper based simulation or live system (scenarios which the firm expects to be able to remain within their impact tolerances and which ones may not)
- the number of important business services tested
- testing the availability and integrity of resources.

Business services that remain available but with compromised integrity will not be deemed to remain within impact tolerances.

Communications, governance and self-assessment
Firms must act quickly and effectively to reduce disruption by providing clear, timely and relevant information.

This will be supported by continuous lessons learned exercises to make continuous improvement and address deficiencies.

In its consultation paper, the FCA considers that firms will be best placed to determine the scenarios used for testing. This is logical on a firm by firm basis, but perhaps for further consideration in the consultation responses, as the regulators will have a macro view on the risks affecting the sector, and may have access to information not available to firms (for example, potentially from Treasury and National Cyber Security Centre). Certain vendors may also have a greater industry view because of the concentration risks that develop, and may also have more advanced understandings of threats and risks from external factors, as well as an understanding of the limitations of their own systems and operations.

Communications, governance and self-assessment are not covered in detail in this paper, but governance and self-assessment will form an essential layer of senior executive review to oversee and set priorities for the firm and that ally with the SM&CR regime. It is important to note that communications will not be limited to internal communications, but there is a full expectation of internal and external communications in order to manage operational resilience.

GDPR already requires firms to have data breach protocols, where communications are already employed in crisis management processes, but often underlying contracts are not clear on who controls the communications aspect of incidents, as against the basic regulatory reporting obligations. Similar issues may arise for operational resilience. Some dialogue with insurers may also be necessary here to assess who may be responsible for communication, and the extent to which communication and crisis management which involves third party outsourcings and supply chain can be effectively conducted without adverse impacts on the liability position under insurance policies. We are beginning to see some evidence of this being addressed in contracts to a limited degree where control of communications is asserted by a regulated firm, but the implications of this may need to be addressed in more detail.

Outsourcing and third party service provision
The relationship between operational resilience and outsourcing has been carefully defined. Under outsourcing rules, firms remain responsible for their obligations when functions are outsourced to a third party. The FCA provides (8.14) that regulated firms retain full responsibility and accountability for managing all their regulatory responsibilities.

According to the regulators' operational resilience requirements, the regulators will expect firms to be operationally resilient regardless of any outsourcing arrangements or use of third parties. Firms are under an obligation not to allow their ability to deliver their important business services within impact tolerances to be undermined when they are delivered wholly or in part by third parties, whether the third parties are external providers or other group entities.

All regulators recognise that cloud computing, and other technologies, particularly AI/ machine learning will be necessary to delivery financial efficiency, but will place additional burdens on outsourcing requirements. For FCA regulated firms at least, outsourcing has already been subject of a detailed focus with FCA guidance on cloud and outsourcing superseded by the EBA guidelines. Fortunately, the FCA does not propose changes to its handbook rules and guidance on outsourcing or third party service provision as part of the current consultation. Its focus will be on the effective governance and management of outsourcing and third party provisions and/or making sure firms actually implement according to the supervisory requirements and expectations.

For PRA regulated firms, there will be a more material change (see below).

Outsourcing does generate risk, primarily by way of concentration risk, supplier "dominance" and concentration of cyber risk in vendor IT systems. The factors that the regulators have identified are set out in the box below. There is a clear requirement for firms to maintain control over service providers, and perhaps to be in control of the relationship. Vendors and firms can reflect during the consultation period how trust and effective relationship building can be fostered by means of mature relationship and contract governance, as the operational resilience objectives of firms will be prejudiced if trust and good faith cannot be maintained with the vendor community. Vendors can offer technical solutions at scale which cannot possibly be replicated by individual firms, and therefore this balance of relationship will be essential to foster a culture of setting and managing appropriate impact tolerances in collaboration with vendors, who will be encouraged to engage fully, to report vulnerabilities and near misses but without the fear of contract termination or blame where the firm's wider obligations beyond the outsourcing or third party service provision can impact the tolerance risk. If this is not appropriate, then consultation responses are necessary to guide the regulators.

8.8. Additionally, we have observed other areas of concern in relation to outsourcing and third-party service provision that can affect operational resilience of a firm's business services, including:

- harms and risks that can arise from high levels of concentration within third party service provider arrangements. For example, high dependency on a single third-party service provider by multiple firms can present additional challenges if more than 1 firm wishes to exit an arrangement at the same or similar time, or if the service provider has an operational resilience failure affecting multiple firms simultaneously. This may particularly be the case where it takes a long time to migrate a large outsourcing relationship.
- high levels of concentration within third-party service provider arrangements, reducing or undermining firms' ability to exert sufficient influence and control over their third-parties.
- some third-party service suppliers operating in multiple jurisdictions with different, or lower quality, resilience requirements than expected by us.
- reduced cyber resilience within the firm due to cyber risks that originate from within the third-party service provider.
- how intra-group outsourcing arrangements are managed.

Source: FCA CP 19/32 chapter 8

The FCA emphasises (8.16) that "there can be no substitute for reading rules and guidance that apply to the firm based on the firm's regulatory status". The message should be the same for vendors to absorb fully the guidance, as a full

understanding of the regulatory obligations of its customers, and perhaps most importantly, sympathy with them, will enable mature conversations and suggestions of workable controls and solutions to firms.

Perhaps "reg tech" solutions could also emerge for risk measurement and management, documentation retention of information needed to monitor compliance and on best practice for creation of associated registers of outsourcings and risk management.

Vendors may also need to be more interested in the data they process, as regulatory expectations "extend to the amount and criticality of firm data being stored, processed or transmitted by outsources or other third-party service providers". This will not only include an appreciation of the management of configuration of data, but also the confidentiality integrity and availability of data, particularly within cloud environments.

PRA CP30/19 Outsourcing and third party risk management

Accompanying the PRA's consultation paper is a further detailed consultation paper "Outsourcing and Third Party Risk Management" and accompanying draft supervisory statement. The paper will require detailed review by PRA regulated firms and their service providers, as the outsourcing regime is effectively harmonised with the existing FCA regime, in large part based on the EBA guidelines.

In addition, the PRA guidance also takes into account the draft European Insurance and Occupational Pensions Authority (EIOPA) guidelines on outsourcing to Cloud Service Providers (1 July 2019).

The synchronisation of the regulatory regimes will help to create more unified standards, but for firms only regulated by PRA and not subject to EBA guidelines, there is a significant additional level of detail to assess. We have written previously on the EBA guidelines, so please see our paper dated 25 March 2019.

The definition of outsourcing is consistent across the regulations in large part, the PRA defining "*outsourcing is an arrangement of any form between the firm and a service provider, with a supervised entity or not, by which that service provider performs a process, a service or an activity, whether directly or by sub-outsourcing which would otherwise be undertaken by the firm itself*".

In the EBA guidelines, there is a list of activities which regulators do not regard as "outsourcing", which are effectively functions that are commonly relied on, such as related to market data, global network infrastructure (e.g. Visa, Mastercard), or messaging standards. There is no similar list in the PRA paper. However, importantly, the PRA expects firms to start from the assumption that all activities, functions and services performed or provided by third parties "in a prudential context" are outsourcing. The PRA also notes that other activities that are not "outsourcing" but which are material "third party arrangements" also need appropriate governance and internal controls. The paper gives examples (paragraph 2.6 of draft supervisory statement) which include:

- a purchase of "certain software products or technology solutions" e.g. "off-the-shelf" machine learning models, open source software and machine learning libraries developed by third party providers;
- sharing of data with third parties, including through API's as part of open banking or the purchase of data collected by third parties for analytical purposes,
- agreements between a third party and a firm to offer financial products or services, e.g. credit cards using the third party's brand and
- in the case of insurers, the use of aggregators and delegated underwriting.

While a proportionate approach is taken to outsourcing, consistent with other regulatory guidelines, these examples potentially significantly increase the scope of the analysis that is required as to whether outsourcing is to be effected. As with other previous regulatory guidelines, intragroup outsourcing is subject to the same rules and expectations.

There is a requirement for firms to maintain a written outsourcing policy drawn from other relevant firm practices and strategy, and to make service providers aware of relevant internal policies, for example, outsourcing, ICT, information security or operational resilience guidelines.

The guidelines generally follow a similar form to the EBA outsourcing guidelines, which emphasise the ability of a whole life cycle approach to outsourcing. This includes requirements for governance and record keeping (Chapter 4) pre outsourcing phase assessment; outsourcing agreements content; data security; access, audit and information rights; sub-outsourcing; business continuity and exit plans. There is an express requirement to maintain a detailed outsourcing register.

The consultation paper specifically mentions systemic concentration risks caused by a single service provider or small numbers of service providers which are difficult to substitute and who may dominate the provision of certain outsourced services to a large number of PRA regulated firms.

The PRA acknowledges that a failure or a prolonged significant disruption at a systemic third party (as they are defined) could have adverse consequences on financial stability. This focus is because of a general increase in firm's reliance on third party service providers, as well as the emergence of new forms of outsourcing such as Cloud, which has increased systemic concentration risk, and also the increased cyber risk from concentration of data in larger scale Cloud and infrastructure providers.

It is clear that the data in firms' outsourcing registers "if produced in and submitted in a clear and comparable format, could provide a valuable tool for the identification, monitoring and mapping of systemic third parties" (paragraph 2.51). There is a potential conflict of interest between the interests of the regulator here and the interest of systemically important vendors, and therefore it will remain to be seen whether standard contract language or approaches to requirements for information should require firms to coordinate in relation to the requests for information from vendors in a "comparable format".

The draft supervisory statement itself sets out in reasonable detail the existing regulatory regime both for PRA authorised banks and insurers, and therefore provides a useful starting point for firms to analyse their existing arrangements against the new requirements on outsourcing. Key requirements of the paper are as follows:

Governance and Record Keeping
Boards and senior management are responsible for oversight of outsourcing arrangements and for compliance with regulatory obligations. The PRA will expect boards to receive adequate information, and has emphasised in particular that management information and outsourcing provided to the board must be "clear, consistent, robust, timely, well-targeted and contain an appropriate level of technical detail to facilitate effective oversight and challenge by the board". The information to be provided will rely on vendor cooperation, but the complex nature of many technical services will mean that the balance will be hard to achieve for the appropriate level of technical detail to be included in these reports without overburdening less technical board members.

Outsourcing Policy
Each firm will be then responsible for maintaining and developing an outsourcing policy that is appropriate to their complexity, organisational structure and size. This outsourcing policy, consistent with operational resilience will be principles based and may then be supported but must be sufficiently detailed to provide adequate "guidance for firm's staff on how to apply its requirements in practice".

The policy must align to and draw upon other relevant firm policies and strategies, which may include:

- business model and strategy
- business continuity
- conflicts of interest
- data protection
- information and communications technology (ICT)
- information security
- operational resilience
- operational continuity in resolution (OCIR)
- (if applicable) ring-fencing
- risk management.

Contents of the outsourcing policy

General	• The responsibilities of the board, including its involvement, as appropriate, in decisions about material outsourcing.
	• The involvement of business lines, internal control functions and other individuals (in particular, SMFs) in respect of outsourcing arrangements.29
	• Links to other relevant policies (see paragraph 4.8).
	• Documentation and record-keeping.
	• Procedures for the identification, assessment, management and mitigation of potential relevant conflicts of interest.
	• Business continuity planning (BCP) (see paragraph 4.9).
	• Differences, if any, between the approach to:
	  • intra-group outsourcing vs outsourcing to external service providers;
	  • material vs non-material outsourcing;
	  • outsourcing to service providers regulated or overseen by the Bank, PRA or FCA vs unregulated service providers; and
	  • outsourcing to service providers in specific jurisdictions outside the UK.

Pre-outsourcing & on-boarding	The processes for vendor due diligence and for assessing the materiality and risks of outsourcing arrangements (including notification to the PRA where required). Responsibility for signing-off new outsourcing arrangements. In particular material outsourcing arrangements.
Oversight	Procedures for the ongoing assessment of service providers' performance including where appropriate: • day-to-day oversight, including incident reporting; periodic performance assessment against service level agreements; and periodic strategic assessments; • being notified and responding to changes to an outsourcing arrangement or service provider (e.g. to its financial position, organisational or ownership structures, sub-outsourcing); • independent review and audit of compliance with legal and regulatory requirements and policies; and • renewal processes.

Termination	Exit strategies and termination processes, including a requirement for a documented exit plan for material outsourcing arrangement where such an exit is considered possible taking into account possible service interruptions (and the firm's impact tolerance for important business services) or the unexpected termination of an outsourcing agreement (see Chapter 10).

**source CP29/19 issued by the PRA "Operational Resilience: Impact Tolerances for Important Business Services", p30-31*

Pre-outsourcing phase

The PRA will expect firms to have detailed processes to determine the materiality of each outsourcing relationship, to perform "appropriate and proportionate" due diligence on all potential service providers, and to assess the risks of every outsourcing irrespective of materiality. Materiality will be assessed under specific criteria in the following table (table 4 from the guidance).

Materiality criteria

Direct connection to the performance of a regulated activity	
Size and complexity of relevant business area(s) or function(s)	
The potential impact of a disruption, failure or inadequate performance on the firm's:	business continuity, operational resilience and operational risk, including: • conduct risk; • information and communication technology (ICT) risk; • legal risk; and • reputational risk.
	ability to: • comply with legal and regulatory requirements; • conduct appropriate audits of the relevant function, service or service provider; and • identify, monitor and manage all risks.
	obligations under • the PRA Rulebook; • the General Data Protection Regulation (GDPR); and • Data Protection Act 2018 (DPA).
	counterparties, customers or policyholders.
	early intervention, recovery and resolution planning OCIR and resolvability.
The firm's ability to scale up the outsourced service.	
Ability to substitute the service provider or bring the outsourced service back in-house , including estimated costs, operational impact, risks and timeframe of an exit in stressed and non-stressed scenarios.	

**source CP29/19 issued by the PRA "Operational Resilience: Impact Tolerances for Important Business Services", p34*

Appropriate due diligence will be necessary in relation to the service providers, including compliance with their own regulatory and legal requirements in relation to data protection and other authorisations, and the ability to demonstrate certified adherence to recognised relevant industry standards. This may include appropriate ISO and public audit report standards, which will have an impact on smaller vendors who are at an early stage of maturity in relation to their business being able to complete for business.

The outsourcing agreements must contain certain minimum requirements which are largely consistent with the obligations under the EBA guidelines with an additional requirement:

If relevant:

- appropriate and proportionate information security related objectives and measures including requirements such as minimum cybersecurity requirements, specifications of firms' data life cycle, and any requirements regarding to data security (see Chapter 7), network security and security monitoring processes, and
- operational and security incident handling procedures including escalation and reporting.

These provisions will be "common sense" for vendors but will require careful checking in the appropriate agreement by the regulated firm.

Data Security
Data security is obviously described in detail, with a further "shared responsibility model" for Cloud outsourcing. This develops on a principle originating in the cloud industry for differentiating between "security of the Cloud" - which is the responsibility for the provision of the Cloud, and "security in the Cloud" - which is the responsibility for the protection of the data in the chosen cloud service, where firms remain responsible for classifying their own data and configuring and monitoring their own data. Specific responsibility will then devolve according to the particular cloud service model chosen e.g. software as a service (SaaS) or infrastructure as a service (IaaS).

Data security measures are not limited to technological measures, and extend to physical and personnel measures, including staff training, and monitoring maintenance of appropriate policies and procedures.

Access, audit and information rights
These are provided in significant detail, and in practice, have constituted one of the major barriers to vendors in the adoption of outsourcing guidelines. The access and audit rights are, of necessity, broad, but are resisted by vendors where over-prescriptive or involving access to multitenant environments (the draft guidelines are an improvement on the EBA draft guidelines in that respect).

The PRA expects firms to adopt a risk-based approach to access audit and information rights in respect of non-material outsourcing arrangements and for reasonable steps to be taken to ensure written agreements effectively monitor and provide appropriate audit rights for regulatory compliance and risk management.

As is usual, these arrangements do not specify who is expected to pay for them.

Fortunately, there is more information in the PRA paper on the use of third party certificates in reports, e.g. public audit and similar reports where the approach taken by the EBA with regard to the reliance that firms could place on reports was more confrontational, where it was implied that the provision of public audit reports alone may not be satisfactory as a means of compliance. The language here does place responsibility on the firms to assess the adequacy of the information and to

meet certain scope, content and process requirements lines but is more helpful to firms. Pooled audits are also possible where organised by groups of firms sharing service providers. These can potentially be less disruptive for multitenant environments and also spread costs.

Sub-Outsourcing
This is a particular feature of complex outsourcings, where there may be multiple layers of sub providers who are providing services to systems integrators or vendor, e.g. telecommunications, data centres, managed IT or similar services. Firms must obtain up to date lists of sub outsource providers from their vendors. Firms must monitor at a minimum sub-outsource service providers involved in the provision of important business services, including their ability to stay within a firm's impact tolerances.

Firms are only able to agree to sub-outsourcing if the sub outsourcing will not give rise to undue operational risk for the firm, in line with outsourcing requirements and a sub-outsource service provider undertakes to comply with all applicable laws, regulatory requirements and contractual obligations and grant to the firm, Bank of England and PRA equivalent contractual access, audit and information rights to those granted by the service provider.

Business continuity and exit plans
Finally, business continuity and documented exit strategies must be reviewed and exit scenarios planned for in advance. This includes scenarios for so-called stressed exits which occur following failure or insolvency of a service provider. This is consistent with current best practice in relation to business continuity and exit management, for example, in the new iteration of ISO 22301:2019, where different exit scenarios should be covered into contingency planning.

Interestingly, the PRA also expects firms to give "meaningful consideration" to all available tools that can facilitate an orderly stressed exit from a material outsourcing. These tools, it notes, are continually evolving, and may include new potential service providers, technology solutions and tools to facilitate the switching and portability of data and applications and industries, codes and standards.

The guidance is realistic and practical, particularly with considerations on collaborative action with other organisations who may be similarly affected, and the practicality of contractual remedies, such as step-in rights where these may be difficult to in fact effect given technical complexity.

Conclusion

The operational resilience and outsourcing/third party management agenda will require significant additional resources and effort from firms. Firms will have to assess for themselves if the costs by firm type in the impact assessment are underestimated.

There is a strong recognition that disasters may occur and that the planning must be focussed on addressing tolerances within such failures but also, focus on planning should hopefully enable the selection of service providers who are able to perform the necessary obligations for the duration of their contracts. There is no comment in the papers as to whether the barriers to entry for new providers could become so high that the operational resilience agenda may dissuade firms from engaging with new FinTechs or service providers. It is also possible that a number of the larger vendors could acquire the more innovative start-ups and businesses who will find the cost of compliance very significant but who may be competitive within a wider service offering. This could in fact increase complexity and concentration risk in the medium to longer term, and therefore the regulators will have to keep a close eye on these developments. In an M&A context, the guidelines could be used as a measure for determining compliance for due diligence in mergers and acquisitions, as there are detailed checklists of obligations that can be used as reference.

However, for both firms and by implication for vendors, the regulators have made their intentions very clear. Vendors will have to spend more time on pre procurement, and also accept what appear to them to be onerous contractual provisions. Due diligence on businesses of this nature during investment rounds and during M&A will have to accommodate this, focusing on the inevitability of onerous contract terms in due diligence, whilst recognising that the customer firm's operations in practice and relationships with other vendors in the ecosystem could have a strong bearing on the actual resilience of the services provided. Having all the paper processes and procedures required by the regulations will not of themselves lead to compliant businesses.

The vendor community will need to scrutinise these papers in detail. If the measures are simply impossible to achieve, too costly or too burdensome, the vendor community may need to consider responses to the consultation papers, but also be very mindful of the negative impact of consultation responses to the EBA outsourcing guidelines, where the quasi monopoly role of large scale cloud providers in particular did not meet with a sympathetic response as regards the performance of regulated obligations by firms reliant on outsourced providers.

There will inevitably also be business opportunity, as the supervisory authorities fully expect that the mapping exercises will reveal vulnerabilities and deficiencies in existing infrastructures "*Delivering operational resilience" for example, requires firms and FMIs to take decisive and effective actions to improve operational resilience, for example replacing outdated or weak infrastructure, increasing system capacity, achieving full fail-over capability, addressing key person dependencies, and being able to communicate with all affected parties. This would include taking action to address vulnerabilities in legacy systems*"[1].

[1] The joint supervisory authority paper paragraph 4.2