Finalised guidance

FG 16/5 Guidance for firms outsourcing to the 'cloud' and other third-party IT services

July 2018

1. Background

1.1 The purpose of this guidance is to clarify the requirements on firms[1] when outsourcing to the 'cloud' and other third-party IT services. This guidance is broader than, but includes issues covered in, 'Considerations for firms thinking of using third-party technology (off-the-shelf) banking solutions', which we published in July 2014 as part of our barriers-to-entry work for firms entering, or considering entering, the banking sector. While the July 2014 publication focused on banking solutions, this guidance is intended to help all firms to effectively oversee all aspects of the life cycle of their outsourcing arrangements: from making the decision to outsource, selecting an outsource provider, and monitoring outsourced activities on an ongoing basis, through to exit.

1.2 In October 2014, the FCA launched Project Innovate – an initiative to foster innovation in financial services aligned with our objective to promote effective competition. Innovation can be a driver of effective competition, so we want to support innovation and ensure that regulation unlocks these benefits, rather than blocks them. In producing this guidance, we have worked closely with Project Innovate to identify areas where our regulatory framework needs to adapt to enable further innovation in the interests of consumers.

[1] This guidance does not apply to a bank, building society, designated investment firm or IFPRU investment firm as defined in the FCA Handbook to whom the EBA Recommendations on outsourcing to cloud service providers are addressed. It is relevant to all other firms authorised under FSMA and will be of interest to those licensed under other regimes, such as the E-Money Regulations 2011. However, firms should ensure they comply with the specific requirements that apply to them based on their status.

1.3 Stakeholders, including firms and cloud service providers, have told us they are unsure about how we apply our rules relating to outsourcing to the cloud. Through roundtable discussions and other interactions with firms and cloud service providers, we understand that this uncertainty may be acting as a barrier to firms using the cloud.

1.4 'Cloud' is a broad term, and stakeholders have interpreted it differently. We see it as encompassing a range of IT services provided in various formats over the internet. This includes, for example, private, public or hybrid cloud, as well as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Cloud services are constantly evolving. Our aim is to avoid imposing inappropriate barriers to firms' ability to outsource to innovative and developing areas, while ensuring that risks are appropriately identified and managed.

1.5 Using the cloud can provide more flexibility to the service that firms receive, enabling innovation and bringing benefits to firms, their consumers, and the wider market. However it can also introduce risks that need to be identified, monitored and mitigated. These risks primarily affect the degree of control exercised by the firm and specific issues such as data security. Cloud customers may have less control of the supplier, for example the degree to which they can tailor the service provided, and of the data, such as where data are stored.

1.6 So we are setting out in more detail our approach to regulating firms which outsource to the cloud and other third-party IT services. We see no fundamental reason why cloud services (including public cloud services) cannot be implemented, with appropriate consideration, in a manner that complies with our rules.

1.7 We have successfully supported both new and existing firms to use cloud and other IT service solutions in a compliant manner.

1.8 This guidance is not binding and is intended to illustrate ways in which firms can comply with the relevant rules. We expect firms to take note of the guidance and, where appropriate, use it to inform their systems and controls on outsourcing.

1.9 The guidance is not exhaustive, nor should it be read in isolation. Firms should consider this guidance in the context of their overarching obligations under the regulatory system. Based on our statutory objectives, we think that complying with this guidance will generally indicate compliance with the FCA outsourcing requirements. The Prudential Regulation Authority (PRA) has different statutory objectives, and so firms that are subject to PRA regulation should confirm their approach with the PRA. FCA guidance on rules, the Act or other legislation represents our view, and does not bind the PRA or the courts.

1.10 The policy contained in this finalised guidance has been designed in the context of the existing UK and EU regulatory framework. We will keep this under review to assess whether any changes would be required due to any intervening changes in the UK regulatory framework, including as a result of any negotiations following the UK's vote to leave the EU.

2. Who does this guidance affect?

2.1 This guidance aims to help firms and service providers understand our expectations where firms are using, or are considering using, the cloud and other third-party IT services. Firms remain subject to FCA requirements even when they are subject to insolvency proceedings and so we would expect that, for example, a firm in administration would continue to comply with our outsourcing requirements.

2.2 This guidance does not apply to a bank, building society, designated investment firm or IFPRU investment firm as defined in the FCA Handbook to whom the EBA Recommendations on outsourcing to cloud service providers are addressed[2]. References to "firm" within this guidance do not include these institutions.

2.3 The guidance will also be of interest to:

(a) third-party IT providers seeking to provide services to financial services firms

(b) trade associations and consumer groups

(c) law firms and other advisers

(d) auditors of financial services firms.

3. Guidance for firms outsourcing to the 'cloud' and other third-party IT services

Introduction

3.1 A firm has many choices when designing its operating model and setting its IT strategy. It may choose to develop and operate its own services or use a third party to cater to some or all of its needs. This market continues to evolve rapidly, with frequent new offerings and innovative ways of delivering these services. Using third-party providers, including cloud providers, may bring benefits to firms such as cost efficiencies, increased security, and more flexible infrastructure capacity. These benefits can support more effective competition.

3.2 This guidance includes a list of areas that a firm should consider during its preparations for the use, evaluation and ongoing monitoring of third parties in the delivery of IT services that are essential to the effective functioning of the regulated firm's business operations.

[2] EBA Recommendations on outsourcing to cloud service providers https://www.eba.europa.eu/documents/10180/2170121/Final+draft+Recommendations+on+Cloud+Outsourcing+%28EBA-Rec-2017-03%29.pdf
Chapter 2(2) sets out that the Recommendations are addressed to "institutions as defined in point (3) of Article 4(1) of Regulation No 575/2013" (on prudential requirements for credit institutions and investment firms).

Cloud computing

3.3 As noted above, the term 'cloud' encompasses a range of different IT services. Each service has features and risks associated with it, and it is for firms to consider which outsourcing option is the best fit for their business. From a regulatory perspective, the exact form of the service used does not, in itself, alter the regulatory obligations placed on firms. It is important to note that where a third party delivers services on behalf of a regulated firm – including a cloud provider – this is considered **outsourcing** and firms need to consider the relevant regulatory obligations and how they comply with them.

Outsource service regulatory requirements

3.4 The overall aim of the high-level regulatory obligations on outsourcing, and the detailed requirements that underpin them, is that a firm appropriately identifies and manages the operational risks associated with its use of third parties, including undertaking due diligence before making a decision on outsourcing. Our approach is risk-based and proportionate, taking into account the nature, scale and complexity of a firm's operations. Regulated firms retain full responsibility and accountability for discharging all of their regulatory responsibilities. Firms cannot delegate any part of this responsibility to a third party.

3.5 For some firms, general outsourcing requirements are detailed in our Senior Management Arrangements, Systems and Controls sourcebook (SYSC). Firms should be aware of other specific requirements, including directly applicable obligations, that may apply to them based on their business. For example, the MiFID Org Regulation[3] contains detailed outsourcing provisions and the Solvency II regulation includes specific obligations for outsourcing for insurers, and domestically we have additional guidance relating to insurers in SYSC.[4]

3.6 Different requirements apply to different types of firm and may be determined by the type of function being outsourced. Of particular relevance is whether or not the function being outsourced is considered **critical or important**, whether it is **material** outsourcing, or for authorised payment institutions and authorised electronic money institutions whether it relates to **important operational functions**. These are specific terms in respect of outsourcing and are defined in the Handbook or Regulations as follows:

- *Critical or important* – an operational function is regarded as critical or important if a defect or failure in its performance would materially impair the continuing compliance of a firm (other than a common platform firm) with the conditions and obligations of its authorisation, its other obligations under the regulatory system, its financial performance, or the soundness or continuity of its relevant services

[3] See Articles 30 and 31 of Commission Delegated Regulation (EU) 2017/565 as regards organisational requirements and operating conditions for investment firms and defined terms for the purposes of MiFID.
[4] Although this document should not be taken as formal guidance on firms' obligations under the Solvency II regulations or the MiFID Org Regulations.

and activities (Senior Management Arrangements, Systems and Controls (SYSC 8.1.4R)).[5] A similar definition is now contained in Article 30 MiFID Org Regulation.

- *Material outsourcing* – defined in the FCA Handbook as outsourcing services of such importance that weakness or failure of the services would cast serious doubt upon the firm's continuing satisfaction of the threshold conditions or compliance with the Principles for Businesses (PRIN).

- *Important operational functions* – under the Electronic Money Regulations 2011 and the Payment Services Regulations 2017, an operational function is important if a defect or failure in its performance would materially impair: (a) the authorised institutions compliance with the Regulations and any requirement of its authorisation; (b) the financial performance of the authorised institution; or (c) the soundness or continuity of the authorised institution. We have published documents that describe our approach to interpreting and applying the regulations, including in relation to outsourcing.[6]

3.7 Firms are reminded of their obligations to notify us when entering into, or significantly changing, material or critical outsourcing arrangements[7].

3.8 The PRA has also published a supervisory statement on resolution planning which is relevant to dual-regulated firms.[8] This contains information needed to support the PRA's preferred resolution strategy, while ensuring that 'critical economic functions' are maintained. The PRA is also undertaking work on operational continuity and the requirement to ensure continuity of critical shared services in resolution[9].

[5] Third party materials such as MiFID Connect (http://www.mifidconnect.com/guidelines) provide some examples of services that may be considered critical or important.
[6] Payment Services and Electronic Money – Our Approach, September 2017
[7] As per obligations in SUP 15.3.8G(1)(e); and SYSC 8.1.12G (in respect to firms other than insurers). Note recital 44 to the MiFID Org Regulation.
[8] Supervisory Statement | SS19/13, Resolution Planning.
[9] Ensuring operational continuity in resolution – PRA Rulebook section on Operational Continuity and Supervisory Statement 9/16.

Areas that firms should consider in relation to outsourcing to the cloud and other third-party IT services

The table below sets out areas for firms to consider in outsourcing, including how they should discharge their oversight obligations.

Area of interest	Notes
Legal and regulatory considerations	Before acceptance, firms should review the contract with the outsource provider to ensure that it complies with our requirements. A firm should: • have a clear and documented business case or rationale in support of the decision to use one or more service providers for the delivery of critical or important operational functions or material outsourcing • ensure the service is suitable for the firm and consider any relevant legal or regulatory obligations, including where a firm is looking to change their existing outsourcing requirements • as part of the due diligence exercise, ensure that in entering into an outsource agreement, it does not worsen the firms operational risk • consider the relative risks of using one type of service over another e.g. public versus private 'cloud' • maintain an accurate record of contracts between the firm and its service provider(s) • know which jurisdiction the service provider's business premises are located in and how that affects the firm's outsource arrangements • know whether its contract with the service provider is governed by the law and subject to the jurisdiction of the United Kingdom. If it is not, it should still ensure effective access to data and business premises for the firm, auditor and relevant regulator (see below sections on access to data and business premises) • consider any additional legal or regulatory obligations and requirements that may arise such as through the General Data Protection Regulation (GDPR). • where these are related to the regulated activity being provided, identify all the service providers in the supply chain and ensure that the requirements on the firm can be complied with throughout the supply chain. Similarly, where multiple providers form part of an overall arrangement (as distinct from a chain) the requirements should be complied with across the arrangement.
Risk management	A fundamental principle of the rules and guidance on outsourcing is that firms identify and manage any risks introduced by their outsourcing arrangements. Accordingly firms should: • carry out a risk assessment to identify relevant risks and identify steps to mitigate them • document this assessment • identify current industry good practice, including data and information security management system requirements, cyber risks, as well as the

	relevant regulator's rules and guidance to then use this to support its decision making • review whether the legal and regulatory risks differ if the customers, firms and employees involved in providing or using the services are in different geographic or jurisdictional locations e.g. UK, EEA or non-EEA • assess the overall operational risks associated with the regulated service for which the firm is responsible and assign responsibility for managing them • monitor concentration risk and consider what action it would take if the outsource provider failed[10] • require prompt and appropriately detailed notification of any breaches or other relevant events arising including the invocation of business recovery arrangements • ensure the contract(s) provide for the remediation of breaches and other adverse events.
International standards	In conducting its due diligence on potential third-party providers, and as part of ongoing monitoring of service provision, a firm may wish to take account of the provider's adherence to international standards as relevant to the provision of IT services. Assurance obtained from international standards for the delivery of critical or important operational functions or material outsourcing is unlikely to be sufficient on its own. Nevertheless firms should: • take account of any external assurance that has already been provided when conducting their own due diligence. External assurance may be more relevant to a firm's consideration where: • it complies to well-understood standards (such as, for example, the ISO 27000 series) • the part of the service being assessed is relatively stable (such as physical controls in the data centre or staff vetting) • the service is uniform across the customer base (i.e. not particular or bespoke to the firm outsourcing) • the scope of the third-party audit is specific to the service a firm proposes to use (i.e. the audit is against the data centre you are using – not a similar data centre in another jurisdiction).
Oversight of service provider	Firms retain full accountability for discharging all of their responsibilities under the regulatory system and cannot delegate responsibility to the service provider. At a high level, a firm should: • be clear about the service being provided and where responsibility and accountability between the firm and its service provider(s) begins and ends • allocate responsibility for the day-to-day and strategic management of the service provider • ensure staff have sufficient skills and resources to oversee and test the outsourced activities; identify, monitor and mitigate against the risks arising; and properly manage an exit or transfer from an existing third-party provider

[10] 'Concentration risk' relates to the reliance that firms themselves may have on any single provider.

	• verify that suitable arrangements for dispute resolution exist.
Data security	Firms should carry out a security risk assessment that includes the service provider and the technology assets administered by the firm. A firm should: • agree a data residency policy with the provider upon commencing a relationship with them, which sets out the jurisdictions in which the firm's data can be stored, processed and managed. This policy should be reviewed periodically • understand the provider's data loss and breach notification processes and ensure they are aligned with the firm's risk appetite and legal or regulatory obligations • consider how data will be segregated (if using a public cloud) • take appropriate steps to mitigate security risks so that the firm's overall security exposure is acceptable • consider data sensitivity and how the data are transmitted, stored and encrypted, where necessary[11].
General Data Protection Regulation (GDPR)	A firm should comply with the General Data Protection Regulation (GDPR) and where necessary the Data Protection Act 2018. Data protection requirements are separate from FCA Handbook requirements and each must be met separately. The GDPR is overseen and regulated by the Information Commissioner's Office (ICO). Firms should therefore follow the ICO's guidance on cloud computing: https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf and other relevant guidance. Where relevant, firms should also consult ICO guidance on sending personal data outside the European Economic Area: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/
Effective access to data	Specific regulatory requirements for some firms (e.g. SYSC 8.1.8R(9) for UCITS investment firms and Article 31(2)(i) MiFID Org Regulation for common platform firms[12]) require effective access to data related to the outsourced activities for regulated firms, their auditors, regulators and relevant competent authorities. The term "data" has a wide meaning. It includes but is not limited to firm, personal customer and transactional data, but also system and process data: for example Human Resource vetting procedures or system audit trails and logs. A firm should: • ensure that notification requirements on accessing data, as agreed with the service provider are reasonable and not overly restrictive

[11] Where data are encrypted, firms should ensure that any encryption keys or similar forms of authentication are kept secure and accessible to the regulator in accordance with Principle 11

[12] The FCA has extended the application of certain parts of the MiFID Org Regulation to common platform firms. For further guidance see MG2 The MiFID 2 Guide and the detailed application provisions in SYSC 1, Annex 1. In relation to the application of SYSC 8, see SYSC 8.1.-2G. Note however the scope of this Guidance set out at paragraph 2.2. This document should not be taken as formal guidance on firms' obligations under the MiFID Org Regulation.

	• ensure there are no restrictions on the number of requests the firm, its auditor or the regulator can make to access or receive data[13] • advise the service provider that the regulator will not enter into a non-disclosure agreement with the service provider but will treat any information disclosed in accordance with the confidentiality obligation set out in the Financial Services and Markets Act (FSMA), sections 348 to 349 • ensure that, where a firm cannot disclose data for any reason, the contract enables the regulator or the firm's auditor to contact the service provider directly • ensure that data are not stored in jurisdictions that may inhibit effective access to data for UK regulators. Considerations should include the wider political and security stability of the jurisdiction; the law in force in the jurisdiction in question (including data protection); and the international obligations of the jurisdiction[14]. This should include consideration of the law enforcement provisions within a jurisdiction.[15]
Access to business premises	SYSC 8.1.8R(9) requires UCITS investment firms to have "effective access to data related to the outsourced activities, as well as to the business premises of the service provider". Separately, Article 31(2)(i) MiFID Org Regulation requires that "the investment firm, its auditors and the relevant competent authorities have effective access to data related to the outsourced functions, as well as to the relevant business premises of the service provider, where necessary for the purpose of effective oversight in accordance with this article, and the competent authorities are able to exercise those rights of access"[16] We regard 'business premises' as a broad term, encompassing a range of premises. This may include head offices, operations centres, but does not necessarily include data centres. For firms where these requirements apply as rules or directly applicable provisions, their contracts must allow for access to business premises[17]. The focus should therefore be on which business premises are relevant for the exercise of effective oversight; this does not necessarily require access to all business premises. For example, service providers may, for legitimate security reasons, limit access to some sites - such as data centres. Firms should also be aware of specific requirements in other relevant legislation. For example, Article 274 of the Solvency II Regulation requires the insurance or reinsurance undertaking to have "effective access to all information relating to the

[13] Under the Financial Services and Markets Act 2000, the FCA has certain powers to require information. These requirements compel the disclosure of information or documents from authorised persons or those believed to be in possession of information relevant to an FCA investigation. In some cases, this information could be stored in the cloud. Regardless of the ultimate location of information, a firm or individual in possession of the information will be expected to comply with such a requirement.
[14] For example international co-operation agreements such as the IOSCO Multilateral Memorandum of Understanding.
[15] These considerations may change over time, and so firms should keep this under review.
[16] The FCA has extended the application of Article 31(2)(i) MiFID Org Regulation to common platform firms. For further guidance see MG2 The MiFID 2 Guide and the detailed application provisions in SYSC 1, Annex 1. Note however the scope of this Guidance as set out at paragraph 2.2.
[17] This document should not be taken as formal guidance on firms' obligations under the MiFID Org Regulation.

	outsourced functions and activities, including carrying out on-site inspections of the business premises of the service provider". Particular considerations include: **Firm and auditor access** • A firm should be able to request an onsite visit to the relevant business premises, in accordance with applicable legal and regulatory requirements. This right should not be restricted • A firm can provide reasonable prior written notice of this visit, except when there is an emergency or crisis situation • A firm may elect its auditor to undertake the visit. Note that this must be the firm's auditor and not an auditor appointed by the outsourcing provider • The scope of the firm and/or auditor visit can be limited to those services that the firm and the entities in the firm's group are using, as required by applicable legal and regulatory requirements. **Regulator access**[18] • A regulator visit to an outsource provider's business premises will only take place if the regulator deems it necessary and required under applicable legal and regulatory requirements. Firms should not stipulate further conditions beyond this • The outsource provider should commit to cooperate with the reasonable requests of the regulator during such a visit • The regulator can commit to visits occurring during business hours and at a time specified by the outsourcing provider or with reasonable notice, except in an emergency or crisis situation • There can be no restrictions regarding employees who attend from the regulator. However, regulators can and will provide relevant information about individuals who will attend • During the visit, the regulator should be permitted to view the provision of services to the regulated firm or any affiliate within the group, as required under applicable financial services legislation. The regulator can commit to minimising, disruption to outsourcing providers' operations.
Relationship between service providers	Outsourcing supply chains are often complex. • If the regulated firm does not directly contract with the outsource provider, it should review sub-contracting arrangements relevant to the provision of the regulated activity to determine whether these enable the regulated firm to continue to comply with its regulatory requirements. Firms should consider, for example, security requirements and effective access to data and business premises. The regulated firm must be able to comply with

[18] These also apply to any other relevant competent authorities, as per requirements in SYSC 8.1.8R(9) for UCITS investment firms and Article 31(2)(i) MiFID Org Regulation.

	these regulatory requirements even if it does not directly contract with the outsource provider • The Contracts (Rights of Third Parties) Act 1999 may be relevant to these considerations • The regulated firm should consider how service providers work together. For example will the firm or one service provider take the lead systems integration role? Firms should consider how easily a service provider's services will interface with a firm's internal systems or other third-party systems (such as agency banking arrangements for payments).
Change management	Risks can be introduced when changes are made to processes and procedures – even where these are well established. We expect firms to have in place a comprehensive change management process, but particular note should be taken of the following points: • establishing what provision has been made for making future changes to technology service provision • establishing how the testing of changes will be carried out.
Continuity and business planning	A firm should have in place appropriate arrangements to ensure that it can continue to function and meet its regulatory obligations in the event of an unforeseen interruption of the outsourced services. Firms should: • consider the likelihood and impact of an unexpected disruption to the continuity of its operations • document its strategy for maintaining continuity of its operations, including recovery from an event, and its plans for communicating and regularly testing the adequacy and effectiveness of this strategy • regularly update and test arrangements to ensure their effectiveness • put in place arrangements to ensure the regulator has access to data in the event of insolvency or other disruption.
Resolution (where applicable)	• Any services should be organised in such a way that they do not become a barrier to the resolution or orderly wind-down of a firm, or create additional complexity in a resolution • For firms where stabilisation powers will, or may, be applied, this will mean that the outsourcing provider and any subcontractor should agree that neither the entry into resolution nor a subsequent change in control arising from the firm's entry into resolution shall constitute a termination event. The outsourcing provider should also agree not to delete, revoke, alter or change any data and to continue to provide services to the firm (or such other entity as necessary) for an appropriate transitional period following the resolution • For firms where insolvency procedures will be used, services should be set up in such a way that supports the rapid return of the firms' deposits or client assets. For example, services should be organised in such a way that would not impede the production of a Single Customer View (SCV) file in a Bank Insolvency Procedure (BIP) or the production of accurate data around client assets in a Special Administration Regime (SAR).

Exit plan	Firms need to ensure that they are able to exit outsourcing plans, should they wish to, without undue disruption to their provision of services, or their compliance with the regulatory regime. Firms should: • have exit plans and termination arrangements that are understood, documented and fully tested • know how it would transition to an alternative service provider and maintain business continuity • have a specific obligation put on the outsourcing provider to cooperate fully with both the firm and any new outsource provider(s) to ensure there is a smooth transition • know how it would remove data from the service provider's systems on exit • monitor concentration risk and consider what action it would take if the outsource provider failed.

Annex – Feedback Statement

1.1 In November 2015 we published a guidance consultation (GC15/6[19]) to invite stakeholder views on our expectations for when firms outsource to the cloud and other third-party IT services. The main points from feedback we received on GC15/6, along with our responses to the feedback, are summarised below[20].

General comments and definitions of 'the cloud'

1.2 Some respondents asked us to clarify how the guidelines apply to different types of cloud services, noting that 'cloud' is a generic term and a variety of different models may be used by firms. In particular, some respondents suggested we clarify the differences between, and the regulatory obligations that apply to, the use of public, private and hybrid clouds, and others suggested highlighting different service models (such as Infrastructure as a Service, and Software as a Service). Some suggested clarifying the different risks and issues that may arise from using different models.

1.3 A few respondents asked us to be clearer about what type of functions constitute critical, important or material outsourcing, asking for examples of relevant services, and examples of services that would be considered non-critical, important or material.

1.4 We note that we use the term 'cloud' broadly in the guidelines but we do not consider any detailed consideration of different types of service models to be beneficial. While there is some commonly used terminology, there are no standardised definitions, and we consider it important for firms to make an assessment of what services are, for example, critical, important or material, in the context of their own outsourcing arrangements.

1.5 To provide further clarity, we have made reference to existing materials (for example the material on MiFID Connect) which provide some non-exhaustive examples of the types of services that may be considered critical or important.

Legal and regulatory considerations

1.6 Some respondents did not agree with the guidance that outsourcing arrangements should be entered into only when "it does not erode, impair or worsen the firms operational risk", suggesting that arrangements should fit with the firm's risk appetite, which may not necessarily mean that operational risk does not worsen.

[19] GC15/6: Proposed guidance for firms outsourcing to the 'cloud' and other third-party IT services.
[20] In addition to the changes explained in this section, we have made a few other minor technical amendments to the guidance to further clarify its content. For example, we have referenced certain FSMA requirements where firms need to provide data to the regulator; and remind firms to ensure that data are not stored in jurisdictions that may inhibit effective access for UK regulators.

1.7 A few providers felt that the wording of the guidance that relates to our expectations if a contract is governed by UK law (or not) lacks clarity and implies that a contract governed by UK law will *de facto* allow effective access, with some respondents telling us this is not necessarily the case.

1.8 Many respondents considered that the expectation for firms to identify all the service providers in the supply chain, and ensure the requirements on the firm can be complied with throughout the supply chain, was impractical and unduly burdensome, noting that supply chains can be large and complex, and would include suppliers who are not relevant to the regulated activity undertaken.

1.9 With regards to operational risk, we are not modifying our guidelines. Our requirements in SYSC state that firms need to take reasonable steps to ensure that outsourcing arrangements "avoid undue additional operational risk", and we consider our position to be in line with this.

1.10 We also consider that, if a contract is governed by UK law, effective access is required, and so we do not consider this expectation requires any amendments.

1.11 We note the concerns about firms identifying all providers in the supply chain may not always be necessary or relevant. Therefore we have amended our guidelines to make clear that this consideration relates to services related to the regulated activity being provided, and therefore does not necessarily include all providers in the supply chain.

Risk management

1.12 Two respondents suggested that expecting firms to consider industry good practice may unhelpfully confer a status on existing industry materials that is inappropriate, and may dissuade organisations from producing good practice in the future.

1.13 Several firms asked for clarity on what "concentration risk" referred to, and noted that if this relates to the risk of many firms using the same provider, this would be difficult for firms to be aware of and monitor, due to likely confidentiality restrictions.

1.14 Many respondents suggested the expectation that firms should require providers to notify them of "any breaches" was unduly burdensome, and that a threshold for breach notification should be determined.

1.15 With regard to the reference to best practice, we note other respondents were keen we include more examples of good practice to support their decision making. We consider that the wording in the guidance, taken together with the guidance on international standards, effectively balances these views without implying any undue status on industry good practice.

1.16 We note that the reference to "concentration risk" may be interpreted in different ways. In our guidance, this term refers to our expectation that firms should monitor any reliance they themselves have on a single provider, consider the action they would take if this provider failed, and whether any concentration risk is within their risk tolerance.

1.17 We consider that requirements for the notification of breaches to the firm to be an important part of risk management. While we accept that the wording in the guidance is high-level, we consider that the current wording gives firms some scope to agree with the provider exactly what constitutes a breach (which is generally not a defined term in our rules) or other relevant events, in the context of the service being provided.

International standards

1.18 We received very few comments on this section. Some respondents asked for further clarity on what further assurance would be required if the use of international standards were unlikely to be sufficient on their own. A couple of respondents suggested adding further examples of relevant international standards and other quality assurance frameworks. On balance, we are not including further examples in this section, as we consider it should be for firms to consider whether and how external assurance may be obtained when conducting their own due diligence.

Oversight of service provider

1.19 Some respondents suggested that firms having the sufficient skills and resources to test outsourced activity was unnecessary, arguing that the testing of arrangements should be left to the outsourced provider. One respondent suggested that it would be difficult for firms to negotiate specific dispute resolution arrangements in contracts with providers.

1.20 We consider it is appropriate for firms to have the skills and resources to test outsourced activity. We consider it an important part of a firm's oversight of their provider to have sufficient in-house ability to supervise their outsourcing arrangements, and to take control of the relevant functions if things go wrong. This may become even more relevant in the future as IT services become more innovative. We also consider it important for firms to have an agreed mechanism with the provider to resolve disputes, and note that "dispute resolution" is not a defined term and enables the firm and the provider to put in place arrangements appropriate to them.

Data security

1.21 Many providers, as well as some firms, had concerns about firms having "choice and control" regarding the jurisdiction in which the firm's data are stored, processed and managed, and several respondents questioned the relationship between this and the data residency policy. Many argued that choice and control was impractical and may stifle provider innovation, suggesting that transparency about where the data were being stored was more appropriate than expecting firms to have choice and control.

1.22 A few respondents suggested it would be helpful for the guidelines to consider arrangements for when data are being transferred outside the EU.

1.23 We note that other organisations also have responsibility for aspects of data security, including the Information Commissioner's Office (ICO). We agree it would be helpful to reference specific considerations with transferring data outside the EU and therefore have

included a short statement in the guidelines, signposting existing guidance from the ICO. Firms may also wish to consult the ICO's "Guide to data protection" which provides further guidance on jurisdictional aspects of data security.

1.24 We want to ensure firms are able to determine which jurisdictions their data are held but we recognise that many cloud providers are not able to allow firms full control of this. In light of this, we have modified our guidelines, to make clear that firms should agree a data residency policy with the provider, which sets out the jurisdictions where their data can be stored, processed, and managed. Providers should have discretion to store, process and control data in the jurisdictions outlined in this policy which are considered acceptable by the firm.

Data Protection Act 1998

1.25 Two respondents commented on this section, one suggesting that firms should disclose to customers when their data are being stored outside the EU, and another suggesting we make reference to the upcoming EU General Data Protection Regulation.

1.26 Data Protection is overseen by the ICO and we believe this section already signposts the relevant considerations that firms should comply with. As discussed above, we have also referenced ICO guidance for transferring data outside the EU.

Effective access to Data

1.27 Both providers and firms raised concerns about the expectation that firms have "no restrictions" on the number of requests they can make of the provider to access or receive data. These respondents suggested this could be onerous and impractical for the provider to comply with. Some also noted there may be legal impediments to accessing or receiving data in certain circumstances. Some firms felt this would be difficult to agree with providers.

1.28 One respondent believed it would be difficult for a contract to be negotiated to allow the regulator to contact the provider directly.

1.29 The concept of "effective access" is broad and wide-ranging, and we do not consider it appropriate to seek to narrow the scope of this requirement. We do not think there should be limits of the number of requests firms make, which could undermine the ability to have effective access. There may be circumstances in which the data cannot be provided, but we do not consider this inconsistent with the wording in the guidelines. With regard to the regulator being able to contact the provider directly, our rules make clear that providers need to co-operate with the regulator, and believe this is in keeping with these requirements.

Access to business premises

1.30 Many respondents had concerns about this section of the guidelines. These concerns centred around the expectation of a firm having physical access to a provider's business

premises, in particular to their data centres, was impractical, creating significant security concerns, and many regarded it unnecessary for the purposes of ensuring effective access.

1.31 We note the concerns around this point. We agree that physical access to data centres may not always be necessary to provide effective access, but we also consider there may be circumstances where physical access to data centres is necessary for a firm to meet its regulatory requirements. We also note that other regulatory requirements will be applicable for certain firms. Solvency II, for example, requires relevant firms to have "on site" access to business premises.

1.32 We have amended our guidance to make clear the relevant SYSC rules that firms need to take into account, and to clarify that our view is that 'business premises' is a broad term which may include head offices, operations centres, but does not necessarily include data centres.

Relationship between service providers

1.33 Around half of respondents commented on this section, most of which focused on concerns that expecting firms to review all sub-contracting arrangements was unnecessary and very difficult, given that many of these arrangements may be confidential between the sub-contractor and provider. Some respondents suggested that assurance could be provided through the attestations of a third party auditor, rather than the firm itself.

1.34 We agree that our expectations should be clarified, and have amended the guidelines to make clear that this should apply to those arrangements relevant to the provision of the regulated activity.

Change management

1.35 A few firms commented on this section. Comments mostly noted that in practice firms will have little control over a provider changing their processes and procedures. Some respondents also suggested specific reference should be made about system and software updates providers make.

1.36 We consider these points are reflected satisfactorily in the guidelines, and are not making any modifications as a result.

Continuity and business planning

1.37 A few respondents suggested some additional points it would be helpful to reference, for example to consider the resilience of the provider's systems. Some respondents sought greater clarity on what information firms need to document, and a couple of respondents noted that these provisions are generally standardised clauses in contracts and providers are unlikely to be able to accommodate bespoke changes.

1.38 We consider the flexibility in the guidelines is appropriate to allow firms and providers to agree appropriate continuity and business planning arrangements which reflect the specifics of the outsourcing arrangements.

Resolution (where applicable)

1.39 This section saw very few comments from respondents, none of which we considered substantive, and therefore we have not made any modifications to these guidelines.

Exit plan

1.40 Several respondents commented that expecting exit plans to be "regularly rehearsed" meant the firm was reliant on the provider, with others suggesting this expectation was unduly onerous.

1.41 We agree with comments on the extent exit plans need to be regularly rehearsed. We have therefore amended this to expect plans to be "fully tested".