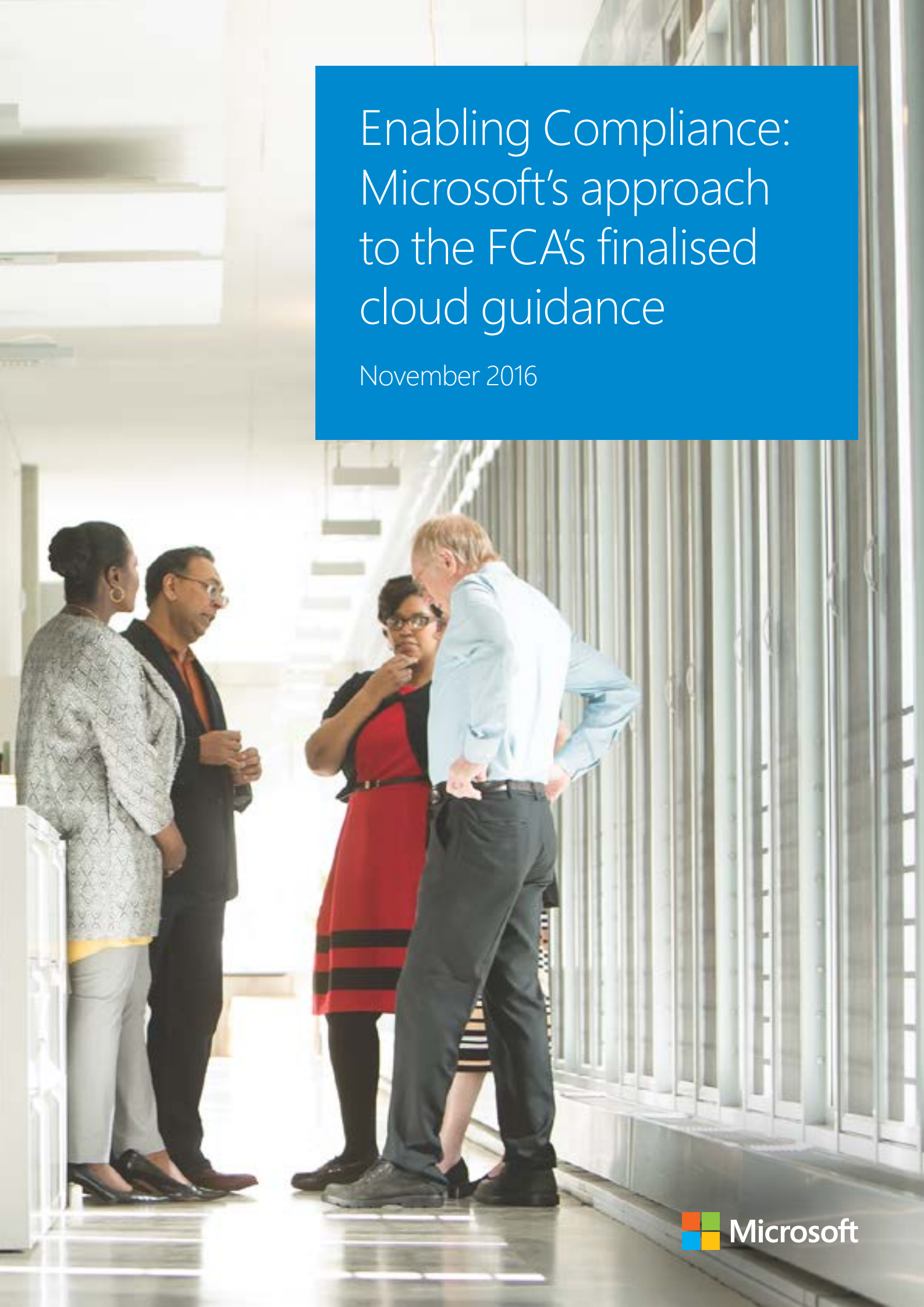
Enabling Compliance: Microsoft's approach to the FCA's finalised cloud guidance

November 2016



Microsoft

Contents

1. Introduction

In July 2016, the United Kingdom's Financial Conduct Authority ("FCA") published "FG 16/5 – Guidance for firms outsourcing to the 'cloud' and other third-party IT services" (the "Guidance").

To help enable firms which are authorised and regulated by the FCA and the Prudential Regulation Authority ("PRA") to comply with their regulatory obligations, Microsoft offers its considered approach in this paper (the "paper") to the Guidance detailing how as a cloud service provider ("CSP") it helps them to meet the standards set out in the Guidance.

While Microsoft provides a range of tools and information for customers and potential customers on its Trust Center and Service Trust Portal to support firms through their regulatory due diligence and risk assessments, the Guidance has provided an opportunity to further empower those interested in or using Microsoft cloud services.

As a CSP, Microsoft is not a financial services business regulated by the FCA and PRA to carry on any of the regulated activities for which prior authorisation is required. However, we provide specific information where we are able to support firms to meet their specific regulatory obligations for most areas of the Guidance. The sections in this paper track the "Area of Interest" titles found in the Guidance for ease of reference and navigation.

Microsoft has always been a leader in providing innovative and secure information technology services – it was the first CSP to adopt ISO27018 (code of practice for the protection of personally identifiable information in the public cloud) and it was also the first CSP to obtain validation from the Article 29 Working Party on its cross border data transfer approach. We are a leading supplier of hyperscale IT services to the financial services sector, and agree with the FCA that there are benefits associated with the cloud. Cloud services can be the key to innovation for financial services businesses and we welcome the FCA's acknowledgement that there is no specific regulatory bar to firms implementing cloud services and support the FCA's "risk based and proportionate" approach to risk management.

This paper is a continuation of our support to financial services businesses in their due diligence and risk assessment activities. Indeed, we believe one of the keys to successful cloud deployment is financial services businesses and CSPs working together to identify, monitor and mitigate risk. You will find in this paper, amongst other things, our commitment to comply with numerous recognised international standards, our transparency around how customer data is handled to allow customers to make informed choices and the contractual provisions to address specific regulatory requirements of the industry.

We hope you find this paper useful, and we look forward to continuing the cloud conversation with you.

2. Legal and regulatory considerations

Firms are required to assess the risks to their businesses involved in any proposed outsourcing and, to this end, are expected to carry out a full due diligence exercise in relation to the arrangement. The Guidance recommends that regulated firms review any contract with the outsource provider to ensure that it complies with regulatory requirements before entering into any cloud outsourcing arrangement.

FCA Guidance	Microsoft's approach
As part of this process, the Guidance specifies that the FCA expects firms: a) 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; b) 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; c) as part of the due diligence exercise, to ensure that in entering into an outsource agreement, it does not worsen the firms operational risk;	Microsoft collaborates with firms throughout their outsourcing due diligence process and risk assessment activities and provides a range of resources to firms to ensure that they have the necessary information with which to make a fully informed decision as to whether the cloud service is suitable for them. We believe that working with you to identify, monitor and mitigate risk is one of the keys to a successful cloud adoption – we can best contribute to your due diligence process by being involved early and having visibility of relevant aspects of your assessment. We offer a range of resources to support you through this process, including recent audit reports, ISO Certificates and a wealth of more general user-friendly information in our contractual framework. We also offer relevant background information to assist you in your assessment, such as on our supply chain and robust data security procedures. All of this is located in the Microsoft Trust Center which includes our Service Trust Portal offering access to a deep set of security, privacy and compliance resources. From a strategic perspective we also agree with the FCA that you should plan and document clearly any decision to outsource. As part of the initial due diligence phase, you should clarify the expected benefits for your business of moving to the cloud. In our experience such benefits may include a reduction in your infrastructure costs, the ability to modernise service delivery, taking advantage of enhanced security and an ability to redirect ICT staff to more value-added work. Whilst reviewing whether the proposed outsourcing is suitable, you should consider how moving to the cloud might affect the internal fabric of the firm. Adopting the cloud may have structural, cultural and/or technological consequences for the firm. Such issues may be pinpointed through looking into some of the following: • Which business units and processes would be affected by the solution being considered? • Are there any resource limitations? • How flexible is the organisation to structural change and resource reassignment? • Is the workforce receptive or resistant to technology innovation? • What is the staff awareness of risk and security process? • What IT systems are in place now and how will the cloud service be integrated into any existing IT assets?
d) consider the relative risks of using one type of service over another e.g. public versus private 'cloud';	Microsoft offers hyperscale, multi-tenant public cloud services, but also on-premises and hybrid solutions to customers. Our hybrid solutions that integrate cloud services into on-premises IT infrastructure are particularly helpful for firms within the financial services industry as they allow them to leverage their existing investments and know-how to design an environment that takes account of their specific risk tolerance and readiness for the cloud. We would welcome the opportunity to engage with firms to discuss what works best for their needs. Our services have a proven track record in the financial services sector as shown by our list of blue-chip customers. As of today the majority of the global systemically important financial institutions across the world have chosen to use our cloud services. This is also true of many PRA and FCA authorised banks, insurers, wealth and asset managers and other financial institutions in the UK.
e) maintain an accurate record of contracts between the firm and its service provider(s);	Upon execution, a copy of the contract is available to the firm from Microsoft.
f) know which jurisdiction the service provider's business premises are located in and how that affects the firm's outsource arrangements; g) 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;	Azure, Office 365, Dynamics CRM Online Services and Intune Online Services are available from our EU data centers and we make specific contractual commitments in the Online Services Terms to store data at rest within the EU. Microsoft also provides cloud service offerings from UK datacentres for customers who require UK deployment. Extensive data location information can be found on our Trust Center. In addition, we have business premises to which effective access for regulators, auditors and customers may be granted as required for our regulated financial services customers. (Please see our approach in the sections below on "Effective Access to Data" and "Access to Business Premises" for more information.) This option is specifically tailored to help mitigate jurisdictional and compliance risks that the FCA is concerned with under these two paragraphs 2 f) and g).

h) consider any additional legal or regulatory obligations and requirements that may arise such as through the Data Protection Act 1998;	Microsoft commits to comply with all laws and regulations applicable to the provision of the Online Services and to collaborate with customers to understand how future laws or regulations may impact their use of the online services. (See the following sections below for more information: "Data Security" and "Data Protection Act (DPA) 1998".)
i) 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.	When Microsoft does use subcontractors it only does so on terms no less protective than those it enters into with you. We also provide information identifying our subcontractors and the contractual obligations we impose on them. • We commit to provide 180 days notice of any new subcontractors that may have access to customer data. • Our Online Service Terms are clear that such subcontractors must abide individually by privacy and security commitments no less protective than those we commit directly to our customers. • Under our control framework, such subcontractors are subject to audits as part of our annual audit cycle. • Every subcontractor is subject to a rigorous vetting process. Where Microsoft does enter into contractual arrangements on data processing with subcontractors that process personal information, such arrangements clearly specify the minimum technical and organisational measures that meet the information security and personal information protection obligations of Microsoft. Such measures are not subject to unilateral reduction by the subcontractor. Microsoft establishes and agrees to relevant information security requirements with each supplier that may access, process, store, communicate, or provide IT infrastructure components for the organisation's information. • Microsoft requires that providers of external information system services comply with organisational information security requirements and employ security controls in accordance with applicable laws, directives, regulations, standards, and guidance. • Microsoft requires external information system service providers to sign a Microsoft Master Vendor Agreement (MMVA) and Interconnection Security Agreements (ISAs). The MMVA and ISAs requires them to comply with applicable security policies and implement security procedures to prevent the disclosure of Microsoft Confidential Information. Microsoft includes provisions in the MMVA and any associated Statement of Work (SOW) with each subcontractor addressing the need to use the appropriate security controls. Subcontractors that handle sensitive data must be in compliance with Microsoft's vendor privacy practices and data protection requirements. • Any subcontractors to whom Microsoft transfers customer data, even those used for storage purposes, will have entered into written agreements with Microsoft that are no less protective than the Data Processing Terms of the Microsoft Online Services Terms (see Appendix).

3. Risk management

A key overarching aspect of the regulatory requirements surrounding outsourcing by financial services firms is that they must "identify and manage" any risks which their outsourcing will introduce into their businesses.

FCA Guidance	Microsoft's approach
The Guidance advises firms to: a) carry out a risk assessment to identify relevant risks and identify steps to mitigate them;	When a financial services customer chooses Microsoft enterprise cloud services, we help them to assess the relevant risks and make available a wide range of resources to facilitate the customer's due diligence as available in the Trust Center (See "Legal and Regulatory Considerations" above).
b) document this assessment;	We can provide resources and information to our customers to assist them in documenting their assessment, see the Appendix.
c) 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;	To help organisations comply with national, regional, and industry-specific requirements governing the collection and use of individuals' data, Microsoft offers a comprehensive set of certifications and attestations for its cloud services. Microsoft accomplishes this breadth of compliance offerings with a two-pronged approach: • First, a team of Microsoft experts works with our engineering and operations teams to track existing standards and regulations, developing hundreds of controls for the product teams to build into our cloud services. • Second, because regulations and standards are always evolving, our compliance experts also plan for upcoming changes to help ensure continuing compliance. We revise and update the Trust Center and in particular the news and events sections to help you identify new or emerging issues.

d) 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;	Microsoft provides information on jurisdiction and geographical location in relation to its data centres and processing procedures via the Trust Center. In addition, as stated above, Microsoft provides further information via the Trust Center on service features and controls that enable customers to assess risks.
e) assess the overall operational risks associated with the regulated service for which the firm is responsible and assign responsibility for managing them;	Microsoft offers a combination of tools and resources which are specifically designed to facilitate this risk assessment, including the Service Trust Portal which offers access to a deep set of security, privacy and compliance resources.
f) monitor concentration risk and consider what action it would take if the outsource provider failed;	The hyperscale computing market remains highly competitive and firms may choose from a number of hyperscale vendors. As for Microsoft itself, it is one of the leading information technology companies and we are able to highlight the following points to help firms when reviewing this issue: • Microsoft has a global data centre footprint and provides resilient data portability, together with flexible hybrid options (including the ability to locate the services infrastructure on-premises if necessary) to mitigate any risks connected with outage and failure. • Customers will always have access to their data under our cloud services. • Microsoft also provides specific terms for business continuity in its contractual framework (see "Continuity and Business Planning" section below).
g) require prompt and appropriately detailed notification of any breaches or other relevant events arising including the invocation of business recovery arrangements; h) ensure the contract(s) provide for the remediation of breaches and other adverse events;	Microsoft contractually commits to provide notification of security breaches and to investigate any incidents and provide the customer with detailed information for all services covered by the Online Service Terms. We commit to taking mitigating steps to deal with the effects and minimise any damage caused. Please see the white papers on security in the Appendix.

4. International standards

The Guidance reiterates the importance for financial services firms when conducting their due diligence on potential cloud service providers, and taking into account whether the particular service provider in question adheres to relevant international standards with regard to IT services.

FCA Guidance

The FCA explains that whilst this is unlikely to be sufficient on its own, firms should:

a) 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).

Microsoft's approach

The Trust Center gives customers access to many external assurances that Microsoft has made, including the latest audit reports for our services, which are carried out at least annually, so that they can gain regular insight into the effectiveness of the controls we have implemented to meet the requirements of industry-leading control frameworks such as ISO/IEC 27001, ISO/IEC 27018, SOC 1 and SOC 2. Microsoft was the first cloud service provider to adopt ISO 270018 and is committed to continue meeting the required standards in relation to compliance with these frameworks.

5. 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.

FCA Guidance	Microsoft's approach
At a high level, a firm should: a) be clear about the service being provided and where responsibility and accountability between the firm and its service provider(s) begins and ends; b) 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;	Microsoft provides an optional tailored fee-based compliance program to financial services customers which provides even greater access to information related to Microsoft's online services and Microsoft subject matter experts, including the ability to suggest additional controls to be included in the future scope of an audit.
c) allocate responsibility for the day-to-day and strategic management of the service provider;	Microsoft makes a range of information available to our customers about our cloud services, such as on the Trust Center, to help firms to meet their regulatory obligations.
d) verify that suitable arrangements for dispute resolution exist.	Microsoft provides for dispute resolution in its contractual framework.

6. Data security

The FCA expects firms to carry out a security risk assessment that includes the service provider and the technology assets administered by the firm.

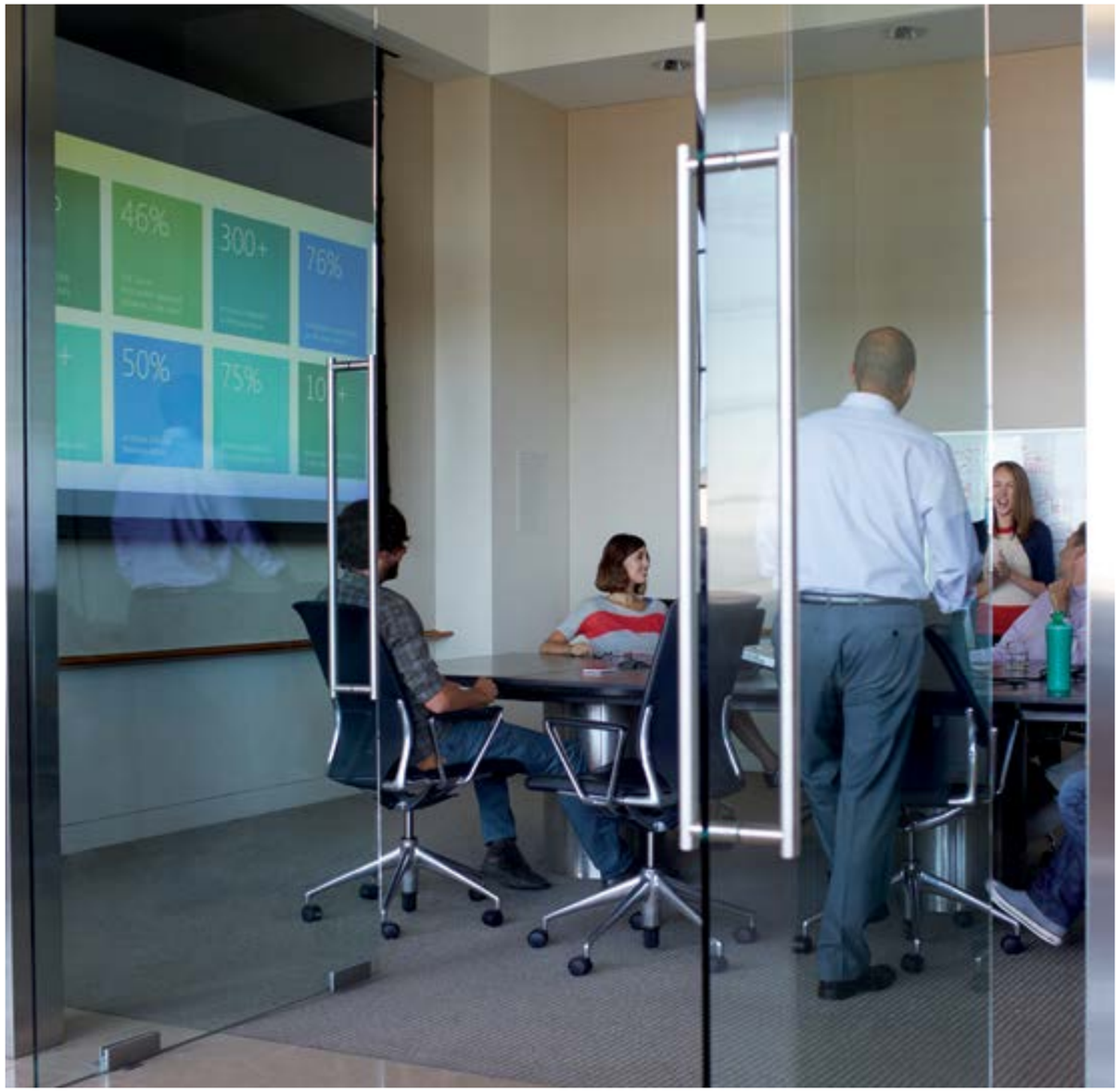
FCA Guidance	Microsoft's approach
A firm should: a) agree a data residency policy with the provider upon commencing a relationship with them, which sets out the jurisdictions in which the firm's data can be stored, processed and managed. This policy should be reviewed periodically;	Microsoft provides clear data processing provisions within the Microsoft Online Services Terms which specify where customer data is stored and include the EU Model Clauses by default. In addition, Microsoft provides information on jurisdiction and geographical location in relation to its data centres and processing procedures via the Trust Center. We were also the first company to receive approval from the Article 29 Working Party (which represents the data protection regulators from each of the 28 EU Member States) that our implementation of the EU Model Clauses meets the high standards of EU data protection legislation.
b) 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;	Microsoft contractually commits to provide notification of security breaches, significant events and to investigate any incidents and provide the customer with detailed information. Microsoft also commits to taking mitigating steps to deal with the effects and minimise any damage caused. In addition, Microsoft's Online Service Terms set out how Microsoft regularly audits its security systems and data centres. The Service Trust Portal gives customers access to the latest audit reports for our services, so that they can gain regular insight into the effectiveness of the controls we have implemented to meet the requirements of industry-leading control frameworks such as ISO/IEC 27001, ISO/IEC 27018, SOC 1 and SOC 2.
c) consider how data will be segregated (if using a public cloud);	Your customer data will always be isolated and subject to a standard of protection which is no lower than that required by EU data protection authorities wherever it is stored throughout the world. We also routinely carry out annual third party penetration testing against the online services including evidence of data isolation among tenants in multi-tenanted services. Whilst it is a matter for the regulated firm to consider what data it wishes to put into the cloud, Microsoft will always apply high levels of security to protect such data. Indeed, Microsoft maintains that multi-tenanted public cloud enables customers to take advantage of the advanced security capabilities and innovations available at hyperscale.

d) take appropriate steps to mitigate security risks so that the firm's overall security exposure is acceptable;

e) consider data sensitivity and how the data are transmitted, stored and encrypted, where necessary.

Microsoft provides customers with the ability to carry on penetration testing as already described in the paragraph above. In addition, the optional tailored fee-based compliance program for financial services customers provides for the ability to suggest additional controls to be included in the future scope of an audit.

Microsoft provides security features across its range of cloud services, including encryption which has long featured in many of our products. Information on security and encryption is set out in the Trust Center, including in our white papers on security for individual products such as Office 365 and Azure. Microsoft's Online Service Terms provide the contractual specifics in relation to security. The relevant white papers are listed within the Appendix at the back of this document.



7. Data Protection Act (DPA) 1998

In the Guidance the FCA reaffirms its belief that data protection and compliance with the DPA and associated guidance is crucial to any outsourcing arrangement.

FCA Guidance

Data protection is fundamental and firms must comply with the eight principles of the DPA as well as any associated guidance. This includes the guidance provided by the Information Commissioner's Office (ICO) which oversees and regulates compliance with the DPA:

https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf

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-data-protection/principle-8-international/

(Links taken from the FCA Guidance).

Microsoft's approach

It is a matter for firms to ensure that they comply with the DPA themselves and we believe that there is nothing in the cloud services offered by Microsoft that impedes this.

Two of Microsoft's foundational principles through which it builds its cloud services are (i) security and (ii) privacy and control. We devote resources to understanding the proposed and existing regulations that apply to our customers including the DPA so that we can develop controls to help our customers address them. We also hold a comprehensive set of certifications and attestations including ISO/IEC 27001, ISO/IEC 27018, and SOC 1 and SOC 2.

Microsoft provides clear data processing provisions within the Microsoft Online Service Terms which specify how customer data is stored and include the EU Model Clauses by default. In addition, rigorous third-party audits, such as by the British Standards Institution and Deloitte, validate the adherence of our cloud services to the strict requirements these standards mandate.

Microsoft welcomes regulation with a consistent framework across the EU which is essential for growth and innovation in the EU, and would benefit both consumers and industry. We have been building privacy by design into the development of our services thereby ensuring we are well placed to meet any requirements coming out of the GDPR and we will comply with the GDPR requirements that apply to us in provisioning online services.

8. Effective access to data

Microsoft understands that allowing a regulated firm, its auditors and the regulators effective access to data connected with the specific outsourced functions is a "red line" requirement if the firm is a certain type of financial services business (particularly a bank, asset manager or an insurer).

FCA Guidance

The Guidance expands on what "data" might mean, including within its definition the following:

- firm, personal customer and transactional data; and
- system and process data such as Human Resource vetting procedures or system audit trails and logs;

With this in mind, the Guidance recommends that firms should:

a) ensure that notification requirements on accessing data, as agreed with the service provider are reasonable and not overly restrictive; b) ensure there are no restrictions on the number of requests the firm, its auditor or the regulator can make to access or receive data; c) 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;	First, it is important to reiterate that customer data stored in our cloud services belongs to our customers. Accordingly, as our customer, you will at all times have direct access to your data, including your virtual machines and applications deployed in our cloud services. You have the ability to delegate and enable access to your data to your auditors or regulators where necessary for compliance purposes. Second, for financial services customers, we make contractual commitments to provide you, your auditors and your regulators with effective access to information related to the cloud services you are using, as well as to Microsoft's business premises. We provide such access through a combination of publicly available websites, the standard features of our cloud services, and processes developed specifically for financial services customers to meet their compliance needs.
d) 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 2000 (FSMA), sections 348 to 349;	We understand that the regulators are bound by a statutory duty of confidentiality in relation to any information they receive from firms they supervise, whether as a result of a request for information or in connection with certain other regulatory obligations. Given the statutory requirements and confidentiality arrangements in place at the regulators, we do not require either the FCA or PRA to enter into non-disclosure agreements.
e) 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. This should include consideration of the law enforcement provisions within a jurisdiction.	One of Microsoft's foundational principles on which we build our cloud solutions is always to allow customers to have visibility into where their data is located. The Trust Center provides information on the location of our primary and backup data centres in each region - we have invested $15 billion to build a global cloud infrastructure that encompasses more than 100 data centres in over 40 countries. The customer is able to choose which particular geographic region it wishes to store data. The Online Service Terms specify more particularly which data from which specific service may be stored. Regardless of the region in which data is stored, your data belongs to you and you will always have access to it during your subscription. This guarantees, at minimum, that a UK-based regulator can gain effective access to data through you and your access to that data. If you choose for your data to be stored in Microsoft's EU data centres, then this area of interest should not be a concern because none of the jurisdictions in which Microsoft has data centres in the EU may inhibit effective access to data by UK regulators and, even if one region were to become a concern, Microsoft has copies of all data in multiple jurisdictions. Further information is available on this topic in the sections on "Legal and Regulatory Considerations", "Risk Management" and "Data Security".

9. Access to business premises

Microsoft understands that access to business premises is a key regulatory requirement as it is crucial for oversight and supervision purposes. Microsoft welcomes the clarification of the Guidance that regulators 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.**

FCA Guidance

For firms where these requirements apply as rules, their contracts must allow for access to business premises, in line with the relevant PRA and FCA rules. The focus should therefore be on which business premises are relevant for the exercise of effective oversight. The FCA clarifies that to oversee matters effectively 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. The Guidance provides specific considerations for both firms and their auditors and the regulators.

Firm and auditor access

a) 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;

b) A firm can provide reasonable prior written notice of this visit, except when there is an emergency or crisis situation;

c) 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;

d) 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.

Microsoft's approach

Microsoft provides specific rights of access to business premises for financial services customers via special contractual provisions, including an optional tailored fee-based compliance program, designed for regulated customers in the financial services sector. These rights enable such customers to comply with their regulatory obligations through direct access to business premises, to information, Microsoft personnel and Microsoft's external auditor. Such rights and processes are designed to provide the customer with the same access to information and personnel that Microsoft would provide to the regulators.

Microsoft is flexible with regard to access requirements and allows that any necessary examination or monitoring required may occur at Microsoft's offices or at other locations where activities relating to the online services are performed. The customer will also have the right to elect its auditor to undertake any such visit if necessary under these provisions.

In line with the recommendations in the Guidance and our rigorous approach to security, we will only ever allow access to those premises which are relevant to the services provided to the customer. Through the optional tailored fee-based compliance program, the customer will also have access to additional Microsoft support throughout the life of its subscription to this service.

Regulator access

a) 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;

b) The outsource provider should commit to cooperate with the reasonable requests of the regulator during such a visit;

c) 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;

d) 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;

e) 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.

Microsoft commits to cooperate with regulatory authorities to allow them access to its business premises through contractual provisions available for our regulated financial services customers. The regulators would be allowed to conduct an on-site examination, to review the online services and gain access to any related information, records, reports and documents. We will also work closely with the customer to resolve any requests from the regulator.

10. Relationship between service providers

The Guidance provides much needed clarity on outsourcing chains and the use of subcontractors to carry out certain services or parts of services.

FCA Guidance

The FCA recommends the following:

a) If the regulated firm does not directly contract with the outsource provider, it should review subcontracting 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 these regulatory requirements even if it does not directly contract with the outsource provider;

b) The Contracts (Rights of Third Parties) Act 1999 may be relevant to these considerations;

c) 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?

d) 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).

Microsoft's approach

With input from customers and the industry Microsoft has developed unique contractual commitments and processes to address fully this requirement by providing our financial services customers, their auditors and their regulators with effective access to data and business premises as necessary to ensure effective oversight of Microsoft and any contractors it may use to provide any of its services to a financial services customer. The Trust Center provides further information on our subcontractors, and our response to paragraph 2 h) of the "Legal and Regulatory Considerations" section of this document sets out how Microsoft deals with and enters into arrangements with such subcontractors.

11. Change management

The Guidance highlights the FCA's concern that risks may be introduced to financial services firms when changes are made to processes and procedures.

FCA Guidance

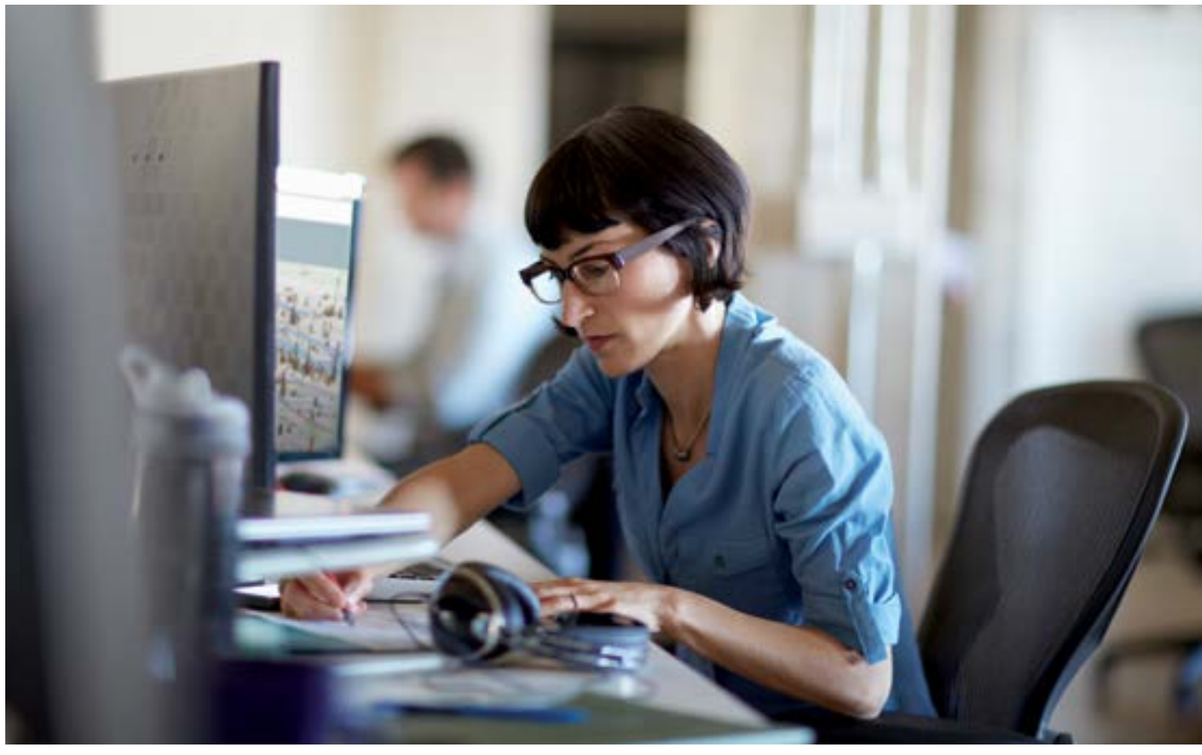
The FCA expects firms to have comprehensive change management processes in place, but in particular:

a) establishing what provision has been made for making future changes to technology service provisions;

b) establishing how the testing of changes will be carried out.

Microsoft's approach

Microsoft has change management processes and procedures. In particular, Microsoft enables financial services customers to engage with Microsoft through the optional tailored fee-based compliance program available to regulated customers. This allows customers to provide structured feedback on the services and have input into future developments and changes to the services. It also allows financial services customers the right to obtain advanced details on existing and future certifications, audit plans and scope. Microsoft will also engage actively with customers to solicit feedback on potential changes to current certifications.



12. Continuity and business planning

The Guidance confirms that a regulated firm 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.

FCA Guidance	Microsoft's approach
A firm should: a) consider the likelihood and impact of an unexpected disruption to the continuity of its operations; b) 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;	We make information available to our customers on data resiliency and service resiliency in the Trust Center to assist them to develop their own continuity and recovery strategies. Microsoft also commits to maintain regularly audited emergency and contingency plans for the facilities in which Microsoft information systems that process customer data are located under the Online Service Terms. Microsoft provides details on business continuity and resiliency on the Service Trust Portal.
c) regularly update and test arrangements to ensure their effectiveness;	Testing of the Microsoft online services business continuity and disaster recovery plans, per the defined testing schedule for each loss scenario takes place at least annually. Issues identified during testing are noted and managed to a resolution. In addition to our own rigorous program of recovery across our cloud infrastructure, we also provide mechanisms for customers to control backup and recovery themselves. For example, in Office 365, document versions and email can be backed up and recovered by your in-house administrator. Azure Backup provides the ability to back up and restore virtual machines, and the Azure Import/Export service can be used to transfer large quantities of data residing in Azure Blob Storage to your on-premises installations. This gives you control over how you choose to archive or even replicate data within your shared computing services. It is important to evaluate the sensitivity of your data along with your backup and integrity requirements. You may well find that the mechanisms for backup and recovery within a service like Office 365 are entirely capable of addressing your requirements. But you can also extend that service by configuring additional backup, recovery or integrity mechanisms to meet compliance or other obligations.
d) put in place arrangements to ensure the regulator has access to data in the event of insolvency or other disruption.	Microsoft provides specific terms on business continuity for financial services customers in the event of (i) regulatory or other legal action impacting them (such as insolvency, reorganisation, liquidation), or (ii) termination or the expiration of any agreement. These provide that Microsoft will not end the provision of such services in such circumstances and will actively cooperate with the firm in any transfer of services to a third party.

13. Resolution (where applicable)

Since the financial crisis the PRA and FCA have increased focus on resolution and the ability of firms to wind down in an orderly fashion. Microsoft understands how important this requirement is to the stability of financial markets and offers financial services customers contractual terms dealing with continuity and resolution issues.

FCA Guidance	Microsoft's approach
The Guidance provides the following on resolution requirements where these apply to regulated firms: a) 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. b) 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. c) 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).	Microsoft provides specific terms on business continuity for financial services customers in the event of (i) regulatory or other legal action impacting them (such as insolvency, reorganisation, liquidation), or (ii) termination or the expiration of any agreement. These provide that Microsoft will not end the provision of such services in such circumstances and will actively cooperate with the firm in any transfer of services to a third party.

14. Exit plan

The Guidance expands on the FCA's concerns connected with termination of outsourcing arrangements. The FCA explains that firms need to ensure that they are able to exit outsourcing arrangements, should they wish to, without undue disruption to their provision of services, or their compliance with the regulatory regime.

FCA Guidance

A firm should:

a) have exit plans and termination arrangements that are understood, documented and fully tested;

b) know how it would transition to an alternative service provider and maintain business continuity;

c) 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;

d) know how it would remove data from the service provider's systems on exit;

e) monitor concentration risk and consider what action it would take if the outsource provider failed.

Microsoft's approach

Microsoft provides specific terms on business continuity for financial services customers in the event of (i) regulatory or other legal action impacting them, or (ii) termination or the expiration of any agreement to enable them to comply with their regulatory obligations. The terms provide that Microsoft will not end the provision of such services abruptly in such circumstances and will actively cooperate with the firm in any transfer of services to a third party. The Online Service Terms set out how Microsoft ensures that data can be recovered including the fact that it retains multiple copies of the data. In addition, Microsoft stores copies of customer data and data recovery procedures in a different place from where the primary computer equipment processing the customer data is located.

Whilst the issue of concentration risk is one for the particular firm to identify, Microsoft provides specific information which can help firms with their determination. In addition to being one of the world's leading information technology companies, we have a global data centre footprint and provide resilient data portability, together with flexible hybrid options (including the ability to locate the services infrastructure on-premises if necessary) to mitigate any risks connected with outage and failure. Section 3 on Risk Management, and more specifically, our response to 3 f) contains further information on our approach to helping firms with their monitoring of concentration risk, as well as highlighting the competitive nature of the hyperscale market, resulting in the availability to firms of a number of vendors from which to choose.

Appendix 1. Microsoft resources

Microsoft provides a number of tools, products and information online to inform customers. This Appendix contains a non-exhaustive list of resources relevant for financial services regulated entities compliance, security and data protection procedures.

Products	**Microsoft Dynamics CRM Online**
	Office 365 Services
	Microsoft Azure Services
	Microsoft Intune Online Services
Deeper Insight	**Online Services Terms**
	Microsoft Trust Center
	Service Trust Portal
White Papers and Offline Resources for due diligence and risk assessment	**Transparency and Assurance: How Microsoft is helping financial institutions move to the cloud**
	Microsoft's commitments, including DPA cooperation, under the EU-U.S. Privacy Shield
	Data location
	In the cloud we trust
	UK Cloud Security principles for Azure
	Cloud Assurance
	Office 365 Security White Paper
	Office 365 Compliance Framework for Industry Standards and Regulations
	Office 365 innovations in enterprise security and compliance
	Exchange Online Advanced Threat Protection
	Microsoft Compliance Framework for Online Services
	Protecting Data and Privacy in the Cloud
	Security, Audits, and Certifications
	Privacy at Microsoft
	Keeping Trust at the Heart of Technology - Open Letter
	Microsoft National Clouds
	Microsoft Big Data Solution Brief