Microsoft

A Compliance Checklist for financial institutions in Luxembourg

March 2023

Contents

Introduction: A compliance checklist for financial institutions in Luxembourg

OVERVIEW

Cloud computing is fast becoming the norm, not the exception, for financial institutions in Luxembourg.

Like all technological advancements, cloud computing provides substantial benefits – but it also creates a complex new environment for financial institutions to navigate. These financial institutions rightly want and expect an unprecedented level of assurance from cloud service providers before they move to the cloud.

Microsoft is committed to providing a trusted set of cloud services to financial institutions in Luxembourg. Our extensive industry experience, customer understanding, research, and broad partnerships give us a valuable perspective and unique ability to deliver the assurance that our financial institutions customers need.

This checklist is part of Microsoft's commitment to financial institutions in Luxembourg. We developed it to help financial institutions in Luxembourg adopt Microsoft cloud services with confidence that they are meeting the applicable regulatory requirements.

WHAT DOES THIS CHECKLIST CONTAIN?

This checklist contains:

1. an Overview of the Regulatory Landscape, which introduces the relevant regulatory requirements in Luxembourg;
2. a Compliance Checklist, which lists the regulatory issues that need to be addressed and maps Microsoft's cloud services against those issues; and
3. details of where you can find Further Information.

WHO IS THIS CHECKLIST FOR?

This checklist is aimed at financial institutions in Luxembourg who want to use Microsoft cloud services. We use the term "financial institutions" broadly, to include any entity that is regulated by the Commission de Surveillance du Secteur Financier (the CSSF) under the Financial Sector Act 1993 and the Payment Services Act 2009. These entities include banks, financial holding companies, investment firms, payment and e-money institutions, credit institutions and professionals of the financial sector (PFS), and including the branches of said entities. This checklist also applies to POST Luxembourg, investment fund managers, undertakings for collective investment in transferable securities subject to Part I of the UCITS Law, central counterparties, approved publication arrangements and authorised reporting mechanisms, market operators operating a trading venue, central securities depositories and administrators of critical benchmarks.

Introduction: A compliance checklist for financial institutions in Luxembourg (continued)

WHAT MICROSOFT CLOUD SERVICES DOES THIS CHECKLIST APPLY TO?

This checklist applies to Microsoft Office 365, Microsoft Dynamics 365 and Microsoft Azure. You can access relevant information about each of these services at any time via the Microsoft Trust Center:

Office 365: microsoft.com/en-us/trustcenter/cloudservices/office365

Dynamics 365: microsoft.com/en-us/trustcenter/cloudservices/dynamics365

Azure: microsoft.com/en-us/trustcenter/cloudservices/azure

IS IT MANDATORY TO COMPLETE THE CHECKLIST?

Not anymore. Nevertheless, this checklist will enable you to

- put in place your register of outsourced IT activities based on a cloud computing infrastructure, which you are obliged to keep and
- for the outsourcing of critical or important functions: to fill in the applicable notification form that must be communicated to the CSSF of your IT outsourcing on the basis of a cloud computing infrastructure. Further detail on notification is given in the section "Overview of the Regulatory Landscape".

HOW SHOULD WE USE THE CHECKLIST?

1. We suggest you begin by reviewing the Overview of the Regulatory Landscape in the next section. This will provide useful context for the sections that follow.

2. Having done so, we suggest that you review the questions set out in the Compliance Checklist and the information provided as a tool to measure compliance against the regulatory framework. The information in this document is provided to help you conduct your risk assessment. It is not intended to replace, or be a substitute for, the work you must perform in conducting an appropriate risk assessment but rather to aid you in that process. Additionally, there are a variety of resources Microsoft makes available to you to obtain relevant information as part of conducting your risk assessment, as well as maintaining ongoing supervision of our services. The information is accessible via the Service Trust Portal and, in particular, use of the Compliance Manager.

   Microsoft provides extensive information enabling self-service audit and due diligence on performance of risk assessments through the Compliance Manager. This includes extensive detail on the security controls including implementation details and explanation of how the third-party auditors evaluated each control. More specifically, Compliance Manager:

   - Enables customers to conduct risk assessments of Microsoft Cloud services. Combines the detailed information provided by Microsoft to auditors and regulators as part of various third-party audits of Microsoft's cloud services against various

Continued Next Page »

Introduction: A compliance checklist for financial institutions in Luxembourg (continued)

standards (such as International Organisation for Standardisation 27001:2013 and ISO 27018:2014) and information that Microsoft compiles internally for its compliance with regulations (such as the EU General Data Protection Regulation or mapping to other required controls) with the customer's own self-assessment of its organisation's compliance with applicable standards and regulations.

- Provides customers with recommended actions and detailed guidance to improve controls and capabilities that can help them meet regulatory requirements for areas they are responsible for.
- Simplifies compliance workflow and enables customers to assign, track, and record compliance and assessment-related activities, which can help an organisation cross team barriers to achieve their compliance goals. It also provides a secure repository for customers to upload and manage evidence and other artifacts related compliance activities, so that it can produce richly detailed reports in Microsoft Excel that document the compliance activities performed by Microsoft and a customer's organisation, which can be provided to auditors, regulators, and other compliance stakeholders.

3. If you need any additional support or have any questions, Microsoft's expert team is on hand to support you throughout your cloud project, right from the earliest stages of initial stakeholder engagement through assisting in any required consultation with the relevant regulators. You can also access more detailed information online, as set out in the Further Information section.

This document is intended to serve as a guidepost for customers conducting due diligence, including risk assessments, of Microsoft Online Services. Customers are responsible for conducting appropriate due diligence, and this document does not serve as a substitute for such diligence or for a customer's risk assessment. While this paper focuses principally on Azure Core Services (referred to as "Azure"), Office 365 Services (referred to as "Office 365") and Dynamics 365 Services (referred to as "Dynamics 365"), unless otherwise specified, these principles apply equally to all Online Services as defined and referenced in the Data Processing Terms ("DPA") of Microsoft Online Services Terms.

Please be aware that this document is based on the current situation at the time of the creation of the document. Taking into account that the regulatory environment as well as our catalogue of products and services and their respective technical features are continuously evolving, we recommend to always visit the Microsoft Trust Center (https://www.microsoft.com/en-us/trust-center) where Microsoft posts the most recent information related to its products and services.

Overview of the Regulatory Landscape

Are cloud services permitted?	Yes. This means that you can consider Microsoft cloud services for the full range of use-cases across your financial institution.
Who are the relevant regulators and authorities?	The Commission de Surveillance du Secteur Financier (the CSSF). Regulated entities in the Luxembourg financial sector are regulated by the CSSF. The CSSF supervises, regulates, authorises, informs, and, where appropriate, carries out on-site inspections and issues sanctions. The CSSF website at http://www.cssf.lu/en/ provides links to underlying regulation.
What regulations and guidance are relevant? (continued)	In Luxembourg, the main regulation containing specific rules for financial institutions wishing to outsource to a cloud computing infrastructure provided by an external provider is the CSSF Circular 22/806 on outsourcing arrangements (the Circular). The Circular implements and complements the EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02 or the EBA Guidelines). Specific requirements for ICT outsourcing relying on a cloud computing infrastructure are included in Part II, Chapter 2 of the Circular. This part has a well-defined scope and applies to outsourced services that are purely IT in nature and limited to cloud computing within the meaning of this Circular (i.e. the NIST criteria "on-demand self-service", "broad network access", "resource pooling", "rapid elasticity", "measured service" plus two specific criteria: "no unmonitored/uncontrolled access to data by the cloud computing service provider" and "no manual interaction by the cloud computing service provider"). ICT outsourcings that do not meet those criteria, or where the cloud service provider is also the resource operator without those activities being properly segregated, are subject to a different set of rules (Part II, Chapter 1 of the Circular). The Circular is applicable regardless of whether the cloud computing service provider is established in Luxembourg or in any third country. A publicly available copy of the Circular can be found at: https://www.cssf.lu/en/Document/circular-cssf-22-806/

Continued Next Page »

Overview of the Regulatory Landscape (Continued)

What regulations and guidance are relevant? (continued)

Please note that the Circular may be subject to some changes over time.

Furthermore, the Circular must be read together with the relevant legal provisions such as Articles 36-2 or 37-1(5) Financial Sector Act 1993 and Articles 11(4) or 24-7(4) Payment Services Act 2009 as well as the CSSF Circulars on central administration, internal governance and risk management, such as the CSSF Circular 12/552 for credit institutions, as amended and CSSF Circular 20/750 on the requirements regarding ICT and security risk management, implementing the EBA Guidelines on ICT (EBA/GL/2019/04) and the CSSF Circular 20/758 for investment firms.

The Circular applies in full to

- credit institutions, including their branches, within the meaning of the Financial Sector Act 1993;
- investment firms, including their branches, within the meaning of the Financial Sector Act 1993;
- payment institutions and electronic money institutions including their branches within the meaning of the Payment Services Act 2009;
- other professionals of the financial sector (PFS) including their branches within the meaning of the Financial Sector Act 1993; and
- POST Luxembourg governed by the Law of 15 December 2000 on postal financial services.

When performing ICT outsourcing, the Circular also applies in full to

- investment fund managers within the meaning of the CSSF Circular 18/698;
- undertakings for collective investment in transferable securities subject to Part I (UCITS) of the UCITS Law;
- central counterparties (CCPs) within the meaning of the EMIR Regulation (EU) 648/2012;
- approved publication arrangements (APAs) with a derogation and authorised reporting mechanisms with a derogation within the meaning of the Financial Sector Act 1993;

Continued Next Page »

Overview of the Regulatory Landscape (Continued)

What regulators and guidance are relevant?	market operators operating a trading venue with the meaning of the Financial Sector Act 1993; • central securities depositories (CSDs) within the meaning of the CSDR Regulation (EU) 909/2014; and • administrators of critical benchmarks within the meaning of the Benchmark Regulation (EU) 2016/1011. Throughout this checklist the notion "financial institutions" shall be interpreted broadly and refer to all in-scope entities as listed above. Please note that all financial institutions also must comply with their legal obligations in terms of professional secrecy which in principle requires that they have to seek consent from their end-clients.
Is regulatory approval required?	No. Prior notification to the CSSF is required in case of critical or important ICT outsourcing relying on cloud computing infrastructure. Such notification must be submitted in principle at least three months before the planned outsourcing comes into effect. If the financial institution resorts to a Luxembourg support PFS, the notice period is reduced to one month. However, where an IT systems and communication networks operator (authorized under Article 29-3 LFS) acts as an intermediary and not as a resource operator between the financial institution and a cloud computing service provider, the notice period remains three months for the outsourcing of critical or important functions to a cloud computing service provider. The notification form must be completed and transmitted to the CSSF electronically at the starting phase of the project. Financial institutions subject to CSSF supervision must also maintain a register of all their outsourcing arrangements, including cloud computing infrastructure-based IT outsourcing, regardless of whether the outsourced functions are "critical or important".

Overview of the Regulatory Landscape (Continued)

What is a "critical or important operational function"?

Financial institutions must consider a function as critical or important in the following situations:

- where a defect or failure in its performance would materially impair:
  i. their continuing compliance with the conditions of their authorisation and/or their other legal and regulatory obligations;
  ii. their financial performance; or
  iii. the soundness or continuity of their services and activities;
- when operational tasks of internal control functions, of the financial and accounting function and of core business activities are outsourced;
- when credit institutions and payment institutions intend to outsource functions of banking activities or payment services to an extent that would require authorisation by the CSSF.

The Circular provides further guidance on what must be taken into account when assessing whether an outsourcing arrangement relates to a function that is critical or important.

Should a function be deemed not "critical or important" and is unlikely to become critical or important, financial institutions may justify not applying certain requirements from the Circular.

Overview of the Regulatory Landscape (Continued)

What information needs to be transmitted to the CSSF? (continued)

Information to be transmitted to the CSSF in case of notification:

The CSSF will want to understand the background and the circumstances under which financial institutions wish to outsource to a cloud computing service provider as well as their compliance with the requirements set forth by the Circular. Financial institutions are therefore required to provide a set of relevant information in the notification form, including, inter alia, an explanation why the applicant considers the outsourcing to be based on a cloud infrastructure within the meaning of the Circular and why it is deemed to be critical or important, the exact cloud computing services to be used (i.e. exact product types and names), the activities and systems affected by the outsourcing, the country where the services are performed, the name and function of the cloud officer, the type and classification of the data stored/processed, the exit strategy as well as the details of the technical training on cloud resource management and security in relation to the cloud service provider.

Financial institutions must furthermore put in place a sound governance which enables an effective monitoring of the outsourced activities (the entity that manages the cloud resources needs a cloud officer) and justify compliance with the contractual clauses listed from paragraphs 77 to 80 and 143 of the Circular.

Financial institutions must also evidence that the financial institution's risk analysis is in accordance with the requirements of the Circular. The risk analysis of the financial institution must take into consideration various factors, including the risks linked to the use of cloud computing technologies (e.g. failure of telecommunications or lack of systems portability), the political stability and security situation of the jurisdictions involved, oversight limitations where the outsourced services or data are located abroad, the laws applicable in the foreign country including the law on data protection, concentration or dependence risks which may arise when large parts of the institutions' activities or important functions are outsourced to a single cloud computing service provider, risks associated with sub-outsourcing or the risk that the outsourcing might result in a relocation of the institution's central administration.

To assist financial institutions in demonstrating their compliance in accordance with the above, the CSSF recommends a report on cloud computing risk assessment proposed by the European Network and Information Security Agency as a means of guidance for financial institutions. The report mainly sets out the main cloud-specific risks and further proceeds to recommendations to financial institutions to address such risks. A full version of the report can be found via the second link provided in this section below.

Continued Next Page »

Overview of the Regulatory Landscape (Continued)

What information needs to be transmitted to the CSSF?

In addition to confirming in writing their compliance with the Circular, financial institutions must further formalise in a register the key characteristics of all their outsourcing arrangements. In case of cloud outsourcing, the register must include information on the cloud service, deployment models, the specific nature of the data to be held and the locations where such data will be stored.

The CSSF has issued a template register. The template can be found via the third link provided in this section below.

Relevant links:

- Link to the CSSF's forms to be transmitted by a financial institution wishing to outsource to the cloud: https://www.cssf.lu/en/Document/notification-for-outsourcing-of-material-it-activities/ (Notification)
- Link to website of the European Network and Information Security Agency where the report on cloud computing risk assessment can be found: https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment
- Link to the CSSF website where the template issued by the CSSF for the register that must be kept, can be found: https://www.cssf.lu/en/Document/register-of-cloud-computing-outsourcing/ (the currently available template is based on the old cloud circular and might still be amended or renewed in accordance with the Circular 22/806)

Are transfers of data outside of Luxembourg permitted? (continued)

Yes, however restrictions apply.

The GDPR, which entered into force on 25 May 2018, allows trans-border dataflows, subject to certain restrictions. More information regarding GDPR compliance can be found here.

Notification and approval of national regulator (including notification of use of Model Contracts)

In general, there is no need for prior approval from a supervisory authority. However, this depends on the justification for the transfer.

Continued Next Page »

Overview of the Regulatory Landscape (Continued)

Are transfers of data outside of Luxembourg permitted?

For example, there will be no obligation to get approval for the use of Model Contracts (though it is possible some supervisory authorities may want to be notified of their use). In contrast, it will be necessary to get approval to rely on binding corporate rules, and the supervisory authority must be informed of transfers made using the minor transfers exemption.

Use of binding corporate rules

Binding corporate rules are a set of binding obligations under which a group of undertakings commit to process personal data in accordance with GDPR: The GDPR places binding corporate rules on a statutory footing. It will be possible to obtain authorization from one supervisory authority that will cover transfers from anywhere in the EU. Please note that binding corporate rules do not cover data transfers made to third parties.

Considerations following from *Schrems II*

The Court of Justice of the European Union emphasized in the "Schrems II" ruling that exporters and importers may need to adopt additional safeguards (supplementary measures) when using Standard Contractual Clauses to transfer personal data from the EU to third countries ensuring an adequate level of protection.

In addition, following the European Data Protection Board's (EDPB) recommendations on such supplementary measures that companies can implement as a result of the *Schrems II* decision, Microsoft announced and further elaborated on organisational, technical and contractual measures, which extends beyond the EDPB's recommendations.

Overview of the Regulatory Landscape (Continued)

Are public cloud services sufficiently secure?	Yes. Several financial institutions in Luxembourg are already using public cloud services. In fact, public cloud typically enables customers to take advantage of the most advanced security capabilities and innovations because public cloud services generally adopt those innovations first and have a much larger pool of threat intelligence data to draw upon. An example of this type of innovation in Microsoft cloud services is Office 365 Advanced Threat Protection and the Azure Web Application Firewall, which provide a very sophisticated model to detect and mitigate previously unknown malware and provide customers with information security protections and analytics information.
Are there any terms that must be included in the contract with the services provider?	Yes. The Circular prescribes a minimum set of terms to be reflected in the outsourcing agreement. In Part 2 of the Compliance Checklist, below, we have mapped these against the sections in the Microsoft contractual documents where you will find them addressed.
How do more general privacy laws apply to the use of cloud services by financial institutions? (continued)	Microsoft is committed to protect the privacy of its customers and is constantly working to help strengthen privacy and compliance protections for its customers. Not only does Microsoft have robust and industry leading security practices in place to protect its customers' data and robust data protection clauses included, as standard, in its Product Terms, Microsoft has gone further. Notably, Microsoft has taken two important and industry first steps to prove its commitment to privacy. First, in April 2014, all EU's data protection authorities acted through their "Article 29 Working Party" to validate that Microsoft's contractual commitments meet the requirements of the EU's "model clauses". Europe's privacy regulators have said, in effect, that personal data stored in Microsoft's enterprise cloud is subject to Europe's rigorous privacy standards no matter where that data is located. For more information on this, follow this link. Continued Next Page »

Overview of the Regulatory Landscape (Continued)

How do more general privacy laws apply to the use of cloud services by insurance and reinsurance undertakings?

Second, in February 2015, Microsoft became the first major cloud provider to adopt the world's first international standard for cloud privacy, ISO/IEC 27018. The standard was developed by the International Organization for Standardisation (ISO) to establish a uniform, international approach to protecting privacy for personal data stored in the cloud.

Additionally, a European privacy law, the General Data Protection Regulation (GDPR) has taken effect. The GDPR imposes new rules on companies, government agencies, non-profits, and other organisations that offer goods and services to people in the European Union (EU), or that collect and analyse data tied to EU residents. The GDPR applies no matter where you are located. Microsoft is committed to GDPR compliance across its cloud services and provides GDPR related assurances in its contractual commitments.

Finally, following the European Data Protection Board's (EDPB) recommendations on measures that companies should implement as a result of the *Schrems II* decision, Microsoft announced its Defending Your Data initiative, which extends beyond the EDPB recommendations, and has since begun working on a plan to meet EU data obligations through Microsoft's EU Data Boundary for the Microsoft Cloud. We have also launched the Tech Fit for Europe initiative to develop digital solutions based on European values and rules.

Compliance Checklist

HOW DOES THIS COMPLIANCE CHECKLIST WORK?

In the "Question/requirement" column, we outline the regulatory requirement that needs to be addressed, based on the underlying requirements, along with other questions that our customers and regulators globally often expect to be addressed.

In the "Guidance" column, we explain how the use of Microsoft cloud services address the requirement. Where applicable, we also provide guidance as to where the underlying requirement comes from and other issues you may need to consider.

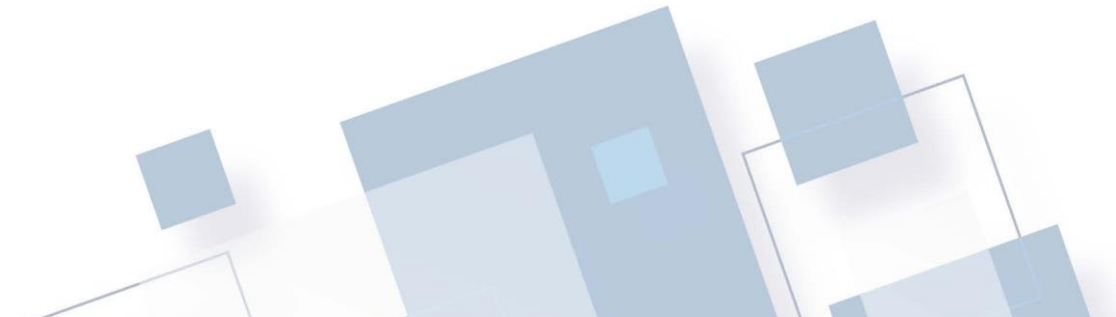
HOW SHOULD WE USE THE COMPLIANCE CHECKLIST?

Every financial institution and every cloud services project is different. We suggest that you tailor and build on the guidance provided to develop your own responses based on your financial institution and its proposed use of cloud services.

WHICH PART(S) DO WE NEED TO LOOK AT?

There are two parts to this Compliance Checklist:

- in Part 1, we address the key compliance considerations that apply; and
- in Part 2, we list the contractual terms that must be addressed and we indicate where these can be found in Microsoft's contract documents.



Part 1: Key Considerations

WHO DOES THIS PART 1 APPLY TO?

This Part 1 applies to all deployments of Microsoft cloud services (particularly, Office 365, Dynamics 365 and Azure) by financial institutions in Luxembourg.

REF.	QUESTION / REQUIREMENT	GUIDANCE
	A. OVERVIEW This section provides a general overview of the Microsoft cloud services	
1	Who is the service provider?	The service provider is the regional licensing entity for, and wholly-owned subsidiary of, Microsoft Corporation, a global provider of information technology devices and services, which is publicly listed in the USA (NASDAQ: MSFT). Microsoft's full company profile is available here: microsoft.com/en-us/investor/ Microsoft's Annual Reports are available here: microsoft.com/en-us/Investor/annual-reports.aspx
2	What cloud services are you using? Please specify the exact types and products to be provided (i.e. IaaS (Infrastructure as a Service), PaaS (Platform as a Service) or SaaS (Software as a Service).	Part I, point 54(h) of the Circular. • Microsoft Office 365: microsoft.com/en-us/trustcenter/cloudservices/office365 • Microsoft Dynamics 365: microsoft.com/en-us/trustcenter/cloudservices/dynamics365 • Microsoft Azure: microsoft.com/en-us/trustcenter/cloudservices/azure

REF.	QUESTION / REQUIREMENT	GUIDANCE
3	What activities and operations will be outsourced to the service provider?	This Compliance Checklist is designed for financial institutions using Office 365, Dynamics 365 and/or Azure. Each service is different and there are many different options and configurations available within each service. The response below will need to be tailored depending on how you intend to use Microsoft cloud services. Your Microsoft contact can assist as needed. If using Office 365, services would typically include: • Microsoft Office applications (Outlook, Word, Excel, PowerPoint, OneNote and Access) • Exchange Online • OneDrive for Business, SharePoint Online, Microsoft Teams, Yammer Enterprise • Skype for Business If using Dynamics 365, services would typically include: • Microsoft Dynamics 365 for Customer Service, Microsoft Dynamics 365 for Field Service, Microsoft Dynamics 365 for Project Service Automation, Microsoft Dynamics 365 for Sales and Microsoft Social Engagement • Microsoft Dynamics 365 for Finance and Operations (Enterprise and Business Editions), Microsoft Dynamics 365 for Retail and Microsoft Dynamics 365 for Talent If using Microsoft Azure, services would typically include: • Virtual Machines, App Service, Cloud Services • Virtual Network, Azure DNS, VPN Gateway • File Storage, Disk Storage, Site Recovery • SQL Database, Machine Learning • IoT Hub, IoT Edge • Data Catalog, Data Factory, API Management • Security Center, Key Vault, Multi-Factor Authentication • Azure Blockchain Service

REF.	QUESTION / REQUIREMENT	GUIDANCE
4	What type of cloud services would your organisation be using? Please specify what type of cloud computing deployment model will be used (i.e. private cloud, community cloud, public cloud or hybrid cloud).	Part I, point 1 and 54(h) of the Circular. With Microsoft cloud services, a range of options exists, including public and hybrid cloud, but given the operational and commercial benefits to customers, public cloud is increasingly seen as the standard deployment model for most institutions. If using public cloud: Microsoft Azure, on which most Microsoft business cloud services are built, hosts multiple tenants in a highly-secure way through logical data isolation. Data storage and processing for our tenant is isolated from each other tenants as described in section E. (Technical and Operational Risk Q&A) below. If using hybrid cloud: By using Microsoft hybrid cloud, customers can move to multi-tenant cloud at their own pace. Tenants may wish to identify the categories of data that they will store on their own servers using Windows Server virtual machines. All other categories of data will be stored in the multi-tenant cloud. Microsoft Azure, on which most Microsoft business cloud services are built, hosts multiple tenants in a highly-secure way through logical data isolation. Data storage and processing for our tenants is isolated from each other tenant as described in section E. (Technical and Operational Risk Q&A) below.
5	What data will be processed by the service provider on behalf of the insurance or reinsurance undertaking? (continued)	It is important to understand what data will be processed through Microsoft cloud services. You will need to tailor this section depending on what data you intend to store or process within Microsoft cloud services. The following are common categories of data that our customers choose to store and process in the Microsoft cloud services. • Customer data (including customer name, contact details, product information and correspondence). • Employee data (including employee name, contact details, internal and external correspondence by email and other means and personal information relating to their employment with the organisation). Continued Next Page »

REF.	QUESTION / REQUIREMENT	GUIDANCE
5	What data will be processed by the service provider on behalf of the insurance or reinsurance undertaking?	• Transaction data (data relating to transactions in which the organisation is involved). • Indices (for example, marketfeeds). • Other personal and non-personal data relating to the organisation's business operations as an insurance or reinsurance undertaking. Pursuant to the terms of the contract in place with Microsoft, all data is treated with the highest level of security so that you can continue to comply with your legal and regulatory obligations and your commitments to customers. You will only collect and process data that is necessary for your business operations in compliance with all applicable laws and regulation and this applies whether you process the data on your own systems or via a cloud solution.
6	How is the issue of counterparty risk addressed through your choice of service provider? (continued)	The following is a summary of the factors that our customers typically tell us are important. To access more information about Microsoft, visit the Trust Center. a. Competence. Microsoft is an industry leader in cloud computing. Microsoft cloud services were built based on ISO/IEC 27001 and ISO/IEC 27018 standards, a rigorous set of global standards covering physical, logical, process and management controls. Microsoft offers the most comprehensive set of compliance offerings of any cloud service provider. A list of its current certifications is available at microsoft.com/en-us/trustcenter/compliance/complianceofferings. From a risk assurance perspective, Microsoft's technical and organisational measures are designed to meet the needs of insurance and reinsurance undertakings globally. Microsoft also makes specific commitments across its Online Services in its Product Terms available at https://www.microsoft.com/en-sg/Licensing/product-licensing/products.aspx. b. Track-record. Many of the world's top companies use Microsoft cloud services. There are various case studies relating to the use of Microsoft cloud services at customers.microsoft.com. Customers have obtained regulatory approvals (when required) and are using Online Services in all regions of the globe including Asia, North America, Latin America, Europe, Middle East and Africa. Key countries of adoption include, by way of example: the United States, Canada, Hong Kong, Singapore, Australia, Japan, Taiwan, Indonesia, United Arab Emirates, Malaysia, the United Kingdom, France, Germany, Italy, Spain, the Netherlands, Poland, Belgium, Denmark, Norway, Sweden, Czech Republic, Brazil, Luxembourg, Hungary, Mexico, Chile, Peru, Argentina, South Africa, and Israel. Office 365 has grown to have over 300 million users, including some of the world's largest organisations and financial institutions. Azure continues to experience rapid growth and has over 400 million users, and over 85% of the largest financial institutions use or have committed to use Azure services.

Continued Next Page »

REF.	QUESTION / REQUIREMENT	GUIDANCE
6	How is the issue of counterparty risk addressed through your choice of service provider?	c. Specific financial services credentials. Financial institution customers in leading markets, including in the UK, France, Germany, Australia, Singapore, Canada, the United States and many other countries have performed their due diligence and, working with their regulators, are satisfied that Microsoft cloud services meet their respective regulatory requirements. This gives customers confidence that Microsoft can help meet the high burden of financial services regulation and is experienced in meeting these requirements. d. Financial strength of Microsoft. Microsoft Corporation is publicly-listed in the United States and is amongst the world's largest companies by market capitalisation. Microsoft has a strong track record of stable profits. Its market capitalisation is in excess of USD $2 trillion as of July, 2021 (stock tracker available here), making it one of the top three capitalised companies on the planet, Microsoft has been in the top 10 global market capitalised countries since 2000, and, indeed, is the only company in the world to consistently place in the top 10 of global market capitalised firms in the past twenty years. Its full company profile is available here: microsoft.com/en-us/investor/ and its Annual Reports are available here: microsoft.com/en-us/Investor/annual-reports.aspx. Accordingly, customers should have no concerns regarding its financial strength.
7	Will the cloud services fulfil the following essential characteristics: i. Is the service an on-demand service? (continued)	Part II, Chapter 2, point 135 and 136 of the Circular. i. Yes. Access to the infrastructure configuration is remotely available for customer or its resource operator via a dedicated dashboard provided by Microsoft. Such access is granted via (1) user name, password, and (2) a Microsoft Command Line Interface (CLI) via access token, via which the customer or its resource operator can unilaterally provision computing capabilities without there being a need to a human interaction with Microsoft. ii. Yes. The remote access takes place over the public Internet or via a private network connection using ExpressRoute technology. iii. Yes. Microsoft Online Services typically offers multi-tenant public cloud services serving multiple customers within the region(s) selected by the customer. iv. Yes. Microsoft offers hyperscale cloud services offer high elasticity allowing customers to rapidly scale outwards and inward without any human intervention. Software automation and auto-scaling of services ensure that our services can meet sudden changes in demand. In addition, our global network and data center footprint is one of the largest in the world and keeps growing. See: https://azure.microsoft.com/en-us/global-infrastructure/global-network/ Office 365, Dynamics 365 and Azure all offer public cloud services that are made available at scale and which can meet these other requirements as provisioned. Each service is different and there are many different options and configurations available within each service. The compliance offerings of each service are described at: Continued Next Page »

REF.	QUESTION / REQUIREMENT	GUIDANCE
7	ii. Is it provided via broad network access? iii. Are the computing resources of the service provider pooled to serve multiple financial institutions using a multi-tenant model? iv. Can capabilities be elastically provisioned and released to scale rapidly outward and inward commensurate with demand?	• Microsoft Office 365: microsoft.com/en-us/trustcenter/cloudservices/office365 • Microsoft Dynamics 365: microsoft.com/en-us/trustcenter/cloudservices/dynamics365 • Microsoft Azure: microsoft.com/en-us/trustcenter/cloudservices/azure v. Yes. All public cloud services are individually monitored on a 24/7 basis. Microsoft automatically controls and optimises resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g. storage, processing, bandwidth and active user accounts). Usage can be monitored, controlled and reported via the service health dashboard, providing transparency for both Microsoft and the customer of the utilised service. vi. Yes. Operational processes underlying to our cloud services have been maximally automated with the objective of minimizing the need for accessing customer data by humans. Microsoft business cloud services take strong measures to help protect your customer data from inappropriate access or use by unauthorized persons. This includes restricting access by Microsoft personnel and subcontractors, and carefully defining requirements for responding to government requests for customer data. Microsoft engineers do not have default standing access to cloud customer data. Instead, they are granted access, under management oversight, only when necessary. A monitoring mechanism is available to the customer or its resource operator to control the accesses. This is contractually ensured. Microsoft personnel will use customer data only for purposes compatible with providing you the contracted services, such as troubleshooting and improving features, such as protection from malware. See Question 84. For more info see "Who can access your data and on what terms?". vii. Correct. There is no manual interaction by Microsoft as to the day-to-day management of the used cloud resources, it being understood that Microsoft may intervene manually: • for global management of IT systems supporting the cloud computing infrastructure (e.g. maintenance of physical equipment, deployment of new non customer-specific solutions); or • within the context of a specific request by the customer or its resource operator (e.g. network issues or services performing insufficiently). See Question 84.
8	Do you wish the cloud computing service provider to act as "resource operator"? A "resource operator" means a natural or legal person that uses the client interface to manage the cloud computing resources.	Part II, Chapter 2, point 138 to 139 of the Circular. Microsoft does not act as a "resource operator".

REF.	QUESTION / REQUIREMENT	GUIDANCE
	B. OFFSHORING Microsoft gives customers the opportunity to choose that certain core categories of data will be stored at-rest within specified regions as chosen by the customer. Within Europe, such regions (also referred to as "Geos"), include the Netherlands, Ireland and other jurisdictions within the European Union. This section only applies to the extent that data and services will be hosted outside of the European Union. This will depend on the configuration of Microsoft cloud services that you select. Your responses will need to be tailored accordingly.	
9	Will the proposed outsourcing require offshoring? If so, from which territory(ies) will the outsourced cloud services be provided?	If using Office 365 and/or Dynamics 365: Where the customer is in the European Union, Microsoft will store core categories of data at rest within the European Union. These categories of data are described in the interactive datacenters map at https://www.microsoft.com/en-us/TrustCenter/Privacy/where-your-data-is-located. If using Azure: Customers can configure the service such that core categories of data are stored at rest within the European Union. These categories of data are described in the interactive datacenters map at: https://www.microsoft.com/en-us/TrustCenter/Privacy/where-your-data-is-located.

REF.	QUESTION / REQUIREMENT	GUIDANCE
10	What risks have been considered in relation to the proposed offshoring arrangement?	The following are risk areas that our customers typically tell us are important. a. Political (i.e. cross-border conflict, political unrest etc.) Our customers know where their data is hosted. The relevant jurisdictions offer stable political enviorenment. b. Country/socioeconomic Microsoft's datacenters are strategically located around the world, taking into account country and socioeconomic factors. The relevant locations constitute stable socioeconomic environments. c. Infrastructure/security/terrorism Microsoft's datacenters around the world are secured to the same exacting standards, designed to protect customer data from harm and unauthorised access. This is outlined in more detail at microsoft.com/en-us/trustcenter/security. d. Environmental (i.e. earthquakes, typhoons, floods) Microsoft datacenters are built in seismically safe zones. Environmental controls have been implemented to protect the datacenters including temperature control, heating, ventilation and air-conditioning, fire detection and suppression systems and power management systems, 24-hour monitored physical hardware and seismically-braced racks. These requirements are covered by Microsoft's ISO/IEC 27001 accreditation. e. Legal Customers will have in place a binding negotiated contractual agreement with Microsoft in relation to the outsourced service, giving them direct contractual rights and maintaining regulatory oversight. The terms are summarised in Part 2.

REF.	QUESTION / REQUIREMENT	GUIDANCE
C. COMPLIANCE WITHIN YOUR ORGANISATION Financial institutions should have internal mechanisms and controls in place to properly manage the outsourcing. Although this is a matter for each financial institution, Microsoft provides some guidance, based on its experience of approaches taken by its customers. Ultimately this will need to be tailored for your financial institution to reflect its compliance practices.		
11	Does the financial institution maintain a register of all cloud computing infrastructure outsourcing, which can be transmitted to the CSSF upon request, for outsourced functions that are critical or importance as well as for other outsourced functions?	Part I, point 53 to 56 of the Circular. The register includes precisions on the cloud service and deployment models, i.e. public/private/hybrid/community, and the specific nature of the data to be held and the locations where such data will be stored. For critical or important functions outsourced, the register mentions the date of the prior notification to the CSSF

REF.	QUESTION / REQUIREMENT	GUIDANCE
12	How does the financial institution demonstrate that in assessing the options for outsourcing to a third party, it has undertaken certain steps by way of due diligence?	Part I, point 7 and 33 and Section 4.3.1 of the Circular.

Our customers and regulators in other jurisdictions generally expect all or some of the following points to be addressed in the due diligence process:

(a) prepared a business case for outsourcing critical or important business functions;

You should prepare a business case for the use of Microsoft cloud services. Where appropriate, this could include references to some of the key benefits of Microsoft cloud services, which are described at:

- Microsoft Office 365: microsoft.com/en-us/trustcenter/cloudservices/office365
- Microsoft Dynamics 365: microsoft.com/en- us/trustcenter/cloudservices/dynamics365
- Microsoft Azure: microsoft.com/en-us/trustcenter/cloudservices/azure

The factors listed below may be used to prepare a business case for the use of Microsoft Online Services:

- Affordability. Microsoft Online Services make enterprise-class technologies available at an affordable price for small and mid-sized companies.
- Security. Microsoft Online Services include extensive security to protect customer data.
- Availability. Microsoft's datacenters provide first-rate disaster recovery capabilities, are fully redundant, and are geographically dispersed to ensure the availability of data, thereby protecting data from natural disasters and other unforeseen complications. Microsoft also provides a financially backed guarantee of 99.9% uptime for most of its Online Services.
- IT control and efficiency. Microsoft Online Services perform basic IT management tasks—such as retaining security updates and upgrading back-end systems—that allow company IT employees to focus their energy on more important business priorities. IT staff retain control over user management and service configuration. The continuous nature of Microsoft Online Services in terms of managing updates, addressing security threats, and providing real-time improvements to the service are unmatched relative to traditional legacy private hosted cloud environments.
- User familiarity and productivity. Because programs like Microsoft Office, Outlook, and SharePoint are hosted on the cloud, company employees can access information remotely from a laptop, PC, or Smartphone.

How does the financial institution ensure that the service provider has the business reputation, appropriate and sufficient abilities, the expertise, the capacity, the resources (e.g. human, ICT, financial), the organisational structure and, if applicable, the required regulatory authorisations or registrations?

Will the financial institution base its decision on prior, in-depth and formalised analysis demonstrating that the outsourcing does not result in (i) the relocation of the central administration or (ii) delegation of the responsibilities of the management body? (continued)

REF.	QUESTION / REQUIREMENT	GUIDANCE	
13		(b) undertaken a tender or other selection process for selecting the service provider;	You will need to describe what selection process you had in place. The factors listed in (a) may be used in the description of the selection process used to select the service provider (e.g. Microsoft's track record and reputation).
14		(c) undertaken a due diligence review of the chosen service provides, including the ability of the service provider to conduct the business activity on an ongoing basis;	You will need to describe your due diligence process. Microsoft provides various materials to help you to perform and assess the compliance of Microsoft cloud services – including audit reports, security assessment documents, in-depth details of security and privacy controls, FAQs and technical white papers – at: microsoft.com/en-us/trustcenter/guidance/risk-assessment.
15		(d) involved the Board of the regulated institution, Board committee of the regulated institution, or senior manager of the institution with delegated authority from the Board, in approving the agreement;	We would suggest having a list, setting out the position of the key people involved in the selection and any decision-making and approvals processes used.
16		(e) considered all of the minimum contractual requirements required by the CSSF;	See Part 2 of this Compliance Checklist.

REF.	QUESTION / REQUIREMENT	GUIDANCE	
17		(f) established procedures for monitoring performance under the outsourcing agreement on a continuing basis;	See Questions 36 and 37 for relevant information about the measures offered by Microsoft to enable customers to monitor performance.
18		(g) addressed the renewal process for outsourcing agreements and how the renewal will be conducted;	Yes. The outsourcing agreement with Microsoft runs on an ongoing basis. Customers may also terminate an Online Service at the express direction of a regulator with reasonable notice or to ensure regulatory compliance and giving 60 days' prior written notice. Microsoft's contractual documents anticipate renewal.
19		(h) developed contingency plans that would enable the outsourced business activity to be provided by an alternative service provider or brought in-house if required?	While your financial institution is ultimately responsible for developing its own contingency plans, based on its circumstances, Microsoft has developed a template that can be used to help develop a plan. This is available from the Microsoft Service Trust Portal or from your Microsoft contact upon request. Yes. The outsourcing agreement with Microsoft provides customers with the ability to access and extract their customer data always stored in each Online Service during their subscription. Microsoft will retain customer data stored in the Online Service in a limited function account for 90 days after expiration or termination of customer's subscription so that the customer may extract the data. No more than 180 days after expiration or termination of the customer's use of an Online Service, Microsoft will disable the account and delete customer data from the account.

REF.	QUESTION / REQUIREMENT	GUIDANCE
20	Did the financial institution identify and assess all relevant risks of the outsourcing arrangement by means of a prior risk assessment including at least the following: • the identification and classification of the relevant functions, data and systems as regards their risk sensitivity and required security measures; • an in-depth evaluation of the risks of the outsourcing project as regards operational risks, including legal ICT, compliance and reputational risks, and the oversight limitations related to the countries where the outsourced services are provided and where the data are stored as well as risks specific to the use of cloud computing technologies[1]; (continued)	Part I, point 66 to 70 and Part II, point 138 (b) of the Circular. See Section E and question 10.

Continued Next Page »

[1] E.g.: isolation failure in multi-tenant environments, the various legislations that are applicable, interception of data-in-transit, failure of telecommunications (e.g. Internet connection), the use of the cloud as "shadow IT" (which is the use of ICT resources that is non-controlled by the ICT department), the lack of systems portability once they have been deployed on a cloud computing infrastructure or the failure of the continuity of cloud computing services.

REF.	QUESTION / REQUIREMENT	GUIDANCE
20	• an evaluation of the consequences of the location of the service provider and whether the service provider is supervised by the CSSF; • an evaluation of the political stability and security situation of the jurisdictions involved, including the laws in force, law enforcement provisions in place, insolvency law provisions; • a definition and decision on an appropriate level of protection of data confidentiality, continuity of the activities outsourced and of the integrity and traceability of data and systems as well as an evaluation of the specific measures for data in memory and data in rest; • an evaluation whether the service provider is a subsidiary or parent undertaking or is included in the scope of accounting consolidation; (continued)	

Continued Next Page »

REF.	QUESTION / REQUIREMENT	GUIDANCE
20	• the expected benefits and costs of the outsourcing arrangement, taking into account concentration risks and aggregated risks resulting from outsourcing several functions across the financial institution, the step-in risk and the measures implemented to manage and mitigate the risks? Where sub-outsourcing of critical or important functions is permitted, will the financial institution take into account the risks associated with sub-outsourcing and the risk that long and complex chains of sub-outsourcing reduce overseeing and supervising abilities?	

REF.	QUESTION / REQUIREMENT	GUIDANCE
21	Is the proportionality analysis documented in writing and are the conclusions of such analysis approved by the management body of the financial institution?	Part I, point 6 of the Circular.
22	Will the financial institution notify the CSSF before the contemplated outsourcing comes into effect?	Part I, point 59 and Part II, Chapter 2, point 141 of the Circular. Such notification must be submitted in principle at least three months before the planned outsourcing comes into effect. If the financial institution resorts to a Luxembourg support PFS, the notice period is reduced to one month. However, where an IT systems and communication networks operator (authorized under Article 29-3 LFS) acts as an intermediary and not as a resource operator between the financial institution and a cloud computing service provider, the notice period remains three months for the outsourcing of critical or important functions to a cloud computing service provider
23	Is the financial institution in a position to inform the CSSF with no delay of material changes and/or severe events regarding the outsourcing arrangements that could have a material impact on the continuing provision of its business activities to allow the CSSF to assess whether regulatory action is needed?	Part I, point 110 of the Circular. See Questions 36 and 37 below.

REF.	QUESTION / REQUIREMENT	GUIDANCE
24	Has the financial institution designated a sufficiently senior staff member who is directly accountable to the management body and responsible for overseeing the risks of outsourcing arrangements and additionally for each outsourced activity, from among its employees, a person who will be in charge of managing the outsourcing relationship and managing access to confidential data?	Part I, point 36(c) and (d) of the Circular. If the resource operation is performed by the financial institution, the cloud officer may cumulate the responsibility for the outsourcing relationship management.

REF.	QUESTION / REQUIREMENT	GUIDANCE
25	Will the financial institution act as "resource operator"? In the negative, which third party shall act as "resource operator"?	Part II, Chapter 2, point 138 to 139 of the Circular. You should consider whether you will act, or appoint a third party to act, as the "resource operator". Microsoft does not act in this role.
26	Provided that the "resource operation" function will be carried out by the financial institution, will the financial institution appoint one person among its employees to act as "cloud officer"?	Part II, Chapter 2, point 140 of the Circular. A cloud officer should be appointed within the entity managing cloud computing resources. This person will be in charge of monitoring the provided services and should have sufficient knowledge to understand the challenges behind a cloud computing infrastructure, and to be the ultimate guarantor for employees' skills at the service provider. The cloud officer may cumulate the responsibility for the outsourcing relationship management.

REF.	QUESTION / REQUIREMENT	GUIDANCE
27	Provided that the "resource operation" function will be carried out by the financial institution, how does the financial institution ensure that staff in charge of cloud computing resources management have sufficient competences to take on their functions based on appropriate training in management and security of cloud computing resources that are specific to the cloud computing service provider?	Part II, Chapter 2, point 142 of the Circular. The responsible staff includes the "cloud officer", the risk management function (including the information security officer) and the internal audit function.
28	Is the resource operation sub-outsourced?	[if yes: the configuration with the different resource operators should be explained]
29	Does the project involve several sub-contracted cloud computing service providers?	[if yes: the configuration with the different resource operators should be explained]

REF.	QUESTION / REQUIREMENT	GUIDANCE
30	What is the rationale confirming the criticality or importance of the activities, where applicable?	Part I, point 65(a) of the Circular. Part I, point 47 of the Circular.
31	Is the financial institution able to continue its critical functions in case of exceptional events or crisis?	Part I, point 38(f) and Section 4.3.4 of the Circular.
32	In the event that critical or important functions are outsourced, did the financial institution document its exit plans and is it able to undertake at least one of the following actions within an appropriate timeframe: • transfer the function to an alternative service provider; • reintegrate the function; • discontinue the business activities that are depending on the function?	

REF.	QUESTION / REQUIREMENT	GUIDANCE
33	Does the financial institution have a policy, approved by the Board, relating to the outsourcing and including the main phases of the life cycle of outsourcing arrangements, contingency plans, exit strategies, approval process, involvement of business lines and internal control functions and, effects of critical or important outsourcing etc.? Does the Board reapprove and update on a regular basis the outsourcing policy while ensuring that appropriate changes are rapidly implemented?	Part I, section 4.2.3 of the Circular. The appropriate policy will depend on the type of organisation and the Online Services in question, and will be proportional to the organisation's risk profile and the specific workloads, data, and purpose for using the Online Services. It will typically include: • a framework to identify, assess, manage, mitigate and report on risks associated with the outsourcing to ensure that the organisation can meet its financial and service obligations to its depositors, policyholders and other stakeholders; • the appropriate approval authorities for outsourcing depending on the nature of the risks in and criticality or importance of the outsourcing (the policy itself needing to be approved by the board); • assessing management competencies for developing sound and responsive outsourcing risk management policies and procedures; • undertaking regular review of outsourcing strategies and arrangements for their continued relevance, safety and soundness; • ensuring that contingency plans, based on realistic and probable disruptive scenarios, are in place and tested; and • ensuring that there is independent review and audit for compliance with the policies. You could use the information set out in Question 12 to develop your Board-approved policy. For example, in describing the service provider selection process, you could include in your policy analysis of the factors listed above with respect to Microsoft's reputation and track record. In addition, you may consider including in the policy that, as part of Microsoft's certification requirements, Microsoft is required to undergo regular, independent third-party audits. As a matter of course, Microsoft already commits to annual audits and makes available those independent audit reports to customers.

REF.	QUESTION / REQUIREMENT	GUIDANCE
34	How does the financial institution identify, assess and manage conflicts of interests with regard to its outsourcing arrangements? How does the financial institution ensure that the service provider is independent from the statutory auditor (accredited auditors or audit firm) in charge?	Part I, Section 4.2.4 of the Circular.
35	What procedures does the financial institution have in place to ensure that all its relevant business units are fully aware of, and comply with, the outsourcing policy?	You will need to explain how the relevant business units are brought under the scope of the outsourcing policy.

REF.	QUESTION / REQUIREMENT	GUIDANCE
36	What monitoring processes does the financial institution have in place to manage the outsourcing?	The guidance below explains how certain features of Microsoft cloud services can make monitoring easier for you. In addition, you may sign up for Premier Support, in which a designated Technical Account Manager serves as a point of contact for day-to-day management of the Online Services and your overall relationship with Microsoft. Microsoft provides access to "service health" dashboards (Office 365 Service Health Dashboard and Azure Status Dashboard) providing real-time and continuous updates on the status of Microsoft Online Services. This provides your IT administrators with information about the current availability of each service or tool (and history of availability status), details about service disruption or outage and scheduled maintenance times. The information is provided online and via an RSS feed. As part of its certification requirements, Microsoft is required to undergo independent third-party auditing, and it shares with the customer the independent third party audit reports. As part of the Financial Services Amendment that Microsoft offers to regulated financial services institutions, Microsoft gives them a right to examine, monitor and audit its provision of Microsoft cloud services. Specifically, Microsoft: (i) makes available a written data security policy that complies with certain control standards and frameworks, along with descriptions of the security controls in place for Microsoft cloud services and other information that the customer reasonably requests regarding Microsoft's security practices and policies; and (ii) causes the performance of audits, on the customer's behalf, of the security of the computers, computing environment and physical datacenters that it uses in processing their data (including personal data) for Microsoft cloud services, and provides the audit report to the customer upon request. Such arrangements should provide the customer with the appropriate level of assessment of Microsoft's ability to facilitate compliance against the customer's policy, procedural, security control and regulatory requirements. The Microsoft Financial Services Amendment further gives the customer the opportunity to participate in the optional financial institution Financial Services Compliance Program at any time, which enables the customer to have additional monitoring, supervisory and audit rights and additional controls over Microsoft cloud services, such as (a) access to Microsoft personnel for raising questions and escalations relating to Microsoft cloud services, (b) invitation to participate in a webcast hosted by Microsoft to discuss audit results that leads to subsequent access to detailed information regarding planned remediation of any deficiencies identified by the audit, (c) receipt of communication from Microsoft on (1) the nature, common causes, and resolutions of security incidents and other circumstances that can reasonably be expected to have a material service impact on the customer's use of Microsoft cloud services, (2) Microsoft's risk-threat evaluations, and (3) significant changes to Microsoft's business resumption and contingency plans or other circumstances that might have a serious impact on the customer's use of Microsoft cloud services, (d) access to a summary report of the results of Microsoft's third party penetration testing against Microsoft cloud services (e.g. evidence of data isolation among tenants in the multi-tenanted services); and (e) access to Microsoft's subject matter experts through group events.

REF.	QUESTION / REQUIREMENT	GUIDANCE
37	Does the financial institution have access to adequate, independent information in order to appropriately monitor the cloud service provider and the effectiveness of its controls?	Part I, point 7 of the Circular. All customers and potential customers have access to information for monitoring the effectiveness of Microsoft's controls, including through the following online sources: • the information on the Service Trust Portal, and in particular, use of the Compliance Manager provides extensive information enabling self-service audit and due diligence; • a publicly available Trust Center for Microsoft Online Services that includes non-confidential compliance information; • the Service Trust Platform, which provides confidential materials, such as third-party audit reports, to current customers and potential customers testing Microsoft Online Services; • a Financial Services Compliance Program, which provides access to a team of specialists in banking, insurance, asset management, and financial services treasury and remediation services; • the Azure Security Center and Office 365 Advanced Threat Analytics, which enable customers to seamlessly obtain cybersecurity-related information about Online Services deployments; • Office 365 Secure Score, which provides insight into the strength of customers' Office 365 deployment based on the customer's configuration settings compared with recommendations from Microsoft, and Azure Advisor, which enables customers to optimise their Azure resources for high availability, security, performance, and cost; • the Office 365 Service Health Dashboard and Azure Status Dashboard, which broadcast real- time information regarding the status of Microsoft Online Services; and • Office 365 Advanced Threat Protection and the Azure Web Application Firewall, which protect customer email in real-time from cyberattacks and provide customers with information security protections and analytics information.

REF.	QUESTION / REQUIREMENT	GUIDANCE
38	How does the financial institution verify that whoever is performing audits or reviewing third-party certifications or audits carried out by service providers - whether it is its internal auditors, the pool of auditors or external auditors acting on its behalf - has appropriate and relevant skills and knowledge to perform relevant audits and/or assessments effectively?	Part I, point 100 of the Circular.
39	How does the financial institution ensure that it maintains ultimate responsibility for any outsourcing?	Part I, point 7 of the Circular. The contract with Microsoft provides the customer with legal mechanisms to manage the relationship including appropriate allocation of responsibilities, oversight and remedies and the minimum terms required by CSSF.

REF.	QUESTION / REQUIREMENT	GUIDANCE
40	Has the financial institution proceeded to an assessment of whether or not third parties concerned by the outsourcing (i.e. financial sector consumers) should be informed or their consent be obtained in light of data protection regulations and professional secrecy provisions?	Part I, point 8 and 9 of the Circular.
41	Does the financial institution know at any time where their data and systems are located globally, be it production environment or replications or backups?	Part II, Chapter 2, point 142(g) of the Circular. Please see Question 9.

REF.	QUESTION / REQUIREMENT	GUIDANCE

D. THE NEED FOR AN APPROPRIATE OUTSOURCING AGREEMENT

Note: See also Part 2 of this Compliance Checklist for a list of the standard contractual terms that the regulator expects to be included in the outsourcing agreement and how these are addressed by the Microsoft contractual documents. This section D also includes reference to certain issues that the regulator suggests are considered as part of the contractual negotiation but which are not necessarily mandatory contractual terms that should be included in all cases.

42	Are the outsourcing arrangements contained in a documented legally binding agreement that is signed by all parties and addresses the required matters set out in the relevant regulations?	Microsoft enters into agreements with each of its financial institution customers for Online Services, which includes a Financial Services Amendment, the Online Services Terms, and the Service Level Agreement. The agreements clearly define the Online Services to be provided. The contractual documents are further outlined in Part 2, below.
43	Will the outsourcing agreement be subject to the law of one of the EEA countries? If not, in case of critical or important outsourcing, has a derogation been granted by the CSSF?	Part II, Chapter 2, point 143(a) of the Circular. In the event of a group contract aiming at allowing the financial institution as well as other entities of the group to benefit from the cloud services, the contract may also be subject to the country of the signing group entity, including when this country is outside the European Economic Area. Part 2 of this checklist maps this requirement against the contractual documents with each of Microsoft's financial institution customers.

REF.	QUESTION / REQUIREMENT	GUIDANCE
44	Does the outsourcing agreement set out the location(s) (i.e. regions or countries) where the function will be provided and/or where relevant data will be kept and processed, including the possible storage location, and the conditions to be met, including a requirement to notify the financial institution if the service provider proposes to change the location(s)?	Part I, point 77(f) of the Circular. If using Office 365 and/or Dynamics 365: Customers can configure the service such that core categories of data are stored at rest within the European Union. These categories of data are described in the interactive datacenters map at microsoft.com/en-us/TrustCenter/Privacy/where-your-data-is-located If using Azure: Customers can configure the service such that core categories of data are stored at rest within the European Union. These categories of data are described in the interactive datacenters map at: microsoft.com/en-us/TrustCenter/Privacy/where-your-data-is-located Part 2 of this checklist maps this requirement against the contractual documents with each of Microsoft's financial institution customers.

REF.	QUESTION / REQUIREMENT	GUIDANCE
45	Will the outsourcing agreement provide for a resiliency of the cloud computing services provided in the EEA so that in case of spread of processing, data, systems over different datacenters worldwide, at least one of the data centers shall be located within the EEA and allow taking over the shared processing in order to operate autonomously the services provided? If not, in case of critical or important outsourcing, has a derogation been granted by the CSSF?	Part II, Chapter 2, point 143(b) of the Circular. Part 2 of this checklist maps this requirement against the contractual documents with each of Microsoft's financial institution customers.
46	In case the financial institution will not act as "resource operator" (and thus the "resource operator" is a third party), is there a relevant service contract governing the outsourcing arrangement?	Microsoft does not act as the "resource operator".

REF.	QUESTION / REQUIREMENT	GUIDANCE
47	Does the outsourcing agreement contain a clear description of the rights and obligations of the financial institution and the service provider as well as the outsourced function to be provided and the financial obligations of the parties?	Part I, point 76 and 77(a) and (d) of the Circular. Part 2 of this checklist maps this requirement against the contractual documents with each of Microsoft's financial institution customers.
48	Does the outsourcing agreement set out the commencement date and, where applicable, end date as well as the notice periods for both the service provider as the financial institution?	Part I, point 77(b) of the Circular. Part 2 of this checklist maps this requirement against the contractual documents with each of Microsoft's financial institution customers.

REF.	QUESTION / REQUIREMENT	GUIDANCE
49	Does the outsourcing agreement set out provisions regarding the accessibility, availability, integrity, confidentiality, privacy and safety of the relevant data and does it define data and system security requirements? Does the outsourcing agreement include the service provider's obligation to protect confidential, personal or otherwise sensitive information and to comply with all legal requirements regarding the protection of data that apply to the financial institution (e.g. personal data protection, bank secrecy)?	Part I, point 8, 9, 77(g) and 87 of the Circular. See Sections E and F of this Checklist. Part 2 of this checklist maps this requirement against the contractual documents with each of Microsoft's financial institution customers.

REF.	QUESTION / REQUIREMENT	GUIDANCE
50	Is it ensured that access to data and systems fulfil the principles of "need to know" and "least privilege", i.e. access is only granted to persons whose functions so require, with a specific purpose, and their privileges shall be limited to the strict necessary minimum to exercise their functions? Is access to data subject to professional secrecy granted in compliance with Article 41(2a) LFS or Article 30(2a) LPS[2]?	Part II, point 119 of the Circular. Operational processes underlying to our cloud services have been maximally automated with the objective of minimizing the need for accessing customer data by humans. Microsoft business cloud services take strong measures to help protect your customer data from inappropriate access or use by unauthorized persons. This includes restricting access by Microsoft personnel and subcontractors, and carefully defining requirements for responding to government requests for customer data. Microsoft engineers do not have default standing access to cloud customer data. Instead, they are granted access, under management oversight, only when necessary. A monitoring mechanism is available to the customer or its resource operator to control the accesses. This is contractually ensured. Microsoft personnel will use customer data only for purposes compatible with providing you the contracted services, such as troubleshooting and improving features, such as protection from malware. For more info see "Who can access your data and on what terms?".

[2] Article 41(2a) of the Law of 5 April 1993 on the Financial Sector, as amended, as well as Article 30(2a) of the Law of 10 November 2009 on Payment Services, as amended require that persons who have access to such information shall be subject by the law to a professional secrecy obligation or be bound by a confidentiality agreement.

REF.	QUESTION / REQUIREMENT	GUIDANCE
51	Does the outsourcing agreement ensure that the data that is owned by the financial institution can be accessed in the case of the insolvency, resolution or discontinuation of business operations of the service provider?	Part I, point 77(m) of the Circular. Ownership of documents, records and other data remain with the customer and at no point transfer to Microsoft or anyone else. Microsoft has adequate business continuity and disaster recovery plans in place intended to restore normal operations and the proper provision of the online services in the event of an emergency and in accordance with applicable laws and regulations. Part 2 of this checklist maps this requirement against the contractual documents with each of Microsoft's financial institution customers.
52	Does the outsourcing agreement clearly define the expected levels of services to be provided by the service provider both qualitatively and quantitatively?	Part I, point 77(i) of the Circular. Part 2 of this checklist maps this requirement against the contractual documents with each of Microsoft's financial institution customers.

REF.	QUESTION / REQUIREMENT	GUIDANCE
53	Does the outsourcing agreement set out whether the service provider shall take mandatory insurance against certain risks, and, if applicable, the level of insurance cover requested?	Part I, point 77(k) of the Circular. Microsoft maintains self-insurance arrangements for most of the areas where third party insurance is typically obtained and can make certificates of insurance available upon request. Microsoft has taken the commercial decision to take this approach and considers that this does not detrimentally affect its customers, given Microsoft's financial position set out in Microsoft's Annual Reports.
54	Does the outsourcing agreement contain the requirements to implement and test business continuity plans?	Part I, point 77 (l) of the Circular. See Question 86 and 90. Part 2 of this checklist maps this requirement against the contractual documents with each of Microsoft's financial institution customers.

REF.	QUESTION / REQUIREMENT	GUIDANCE
55	Does the outsourcing agreement set out whether sub-outsourcing, in particular, of a critical or important function, or material parts thereof, is permitted and, if so, the conditions that the sub-outsourcing is subject to? If sub-outsourcing of critical or important functions is permitted, does the agreement include: • the type of activities that is excluded from sub-outsourcing; • the conditions to be complied with; • the obligation for the service provider to ensure compliance with contractual obligations in respect of the financial institution; • the prior specific or general written authorisation from the financial institution before sub-outsourcing data; (continued)	Part I, point 77(e) and 78 to 82 of the Circular. In the event of sub-outsourcing of critical or important functions, the financial institution must ensure that the sub-contractor undertakes to (i) comply with applicable laws, regulatory requirements and contractual obligations and (ii) grant the financial institution and the regulator the same rights of access and audit as those granted by the service provider. Part 2 of this checklist maps this requirement against the contractual documents with each of Microsoft's financial institution customers.

Continued Next Page »

REF.	QUESTION / REQUIREMENT	GUIDANCE
55	• the service provider's obligation to inform the financial institution of any planned sub-outsourcing, or material changes thereof (changes of sub-contractors and notification period); • the financial institution's explicit approval of or, right to object to intended sub-outsourcing or material changes thereof; • the financial institution's right to terminate the agreement in case of undue sub-outsourcing, e.g. in case of sub-outsourcing without notification of material risk increase.	

REF.	QUESTION / REQUIREMENT	GUIDANCE
56	Does the outsourcing agreement provide for an appropriate means of contact at the cloud computing service provider in case of an incident?	Part I, point 54(e) of the Circular. Part 2 of this checklist maps this requirement against the contractual documents with each of Microsoft's financial institution customers.
57	Does the outsourcing agreement provide a guarantee of access to the minimum IT assets required to operate under a disaster scenario? Are the measures for redundancy and backup of the systems and data specified in the agreement?	Part I, point 47, 50 and 77(m) of the Circular. Yes. The uptime guarantee given by Microsoft applies to all IT assets, not just a minimum number required to operate in a disaster situation. Microsoft guarantees 99.9% of uptime for most of its Online Services. Uptime guarantees are set forth in Microsoft's contracts with its customers, and if service levels are not maintained, customers may be eligible for a credit towards a portion of their monthly service fees. For information regarding uptime for each Online Service, refer to the Service Level Agreement for Microsoft Online Services. See also question 8 and 90 below. Part 2 of this checklist maps this requirement against the contractual documents with each of Microsoft's financial institution customers.

REF.	QUESTION / REQUIREMENT	GUIDANCE
58	Does the outsourcing agreement also include reporting mechanisms that ensure adequate oversight of IT security risk management by the service provider? Do the reporting obligations of the service provider include the communication by the service provider of any development that may have a material impact on the service provider's ability to effectively carry out the function in line with the agreed service levels and in compliance with applicable laws and regulatory requirements (and including the obligation to report any significant problem having an impact on the outsourced functions as well as any emergency situation? Do the reporting obligations include, where appropriate, the obligation to submit reports of the internal audit function of the service provider?	Part I, point 77(j) of the Circular. Yes, as referenced in Questions 36 and 37 above. Part 2 of this checklist maps this requirement against the contractual documents with each of Microsoft's financial institution customers.

REF.	QUESTION / REQUIREMENT	GUIDANCE
59	Is the outsourcing agreement sufficiently flexible to accommodate changes to existing processes and to accommodate new processes in the future to meet changing circumstances?	Yes. The customer can always order additional services if required. The customer may terminate an Online Service at the express direction of a regulator with reasonable notice. Additionally, to ensure regulatory compliance, Microsoft and the customer may contemplate adding additional products or services, or if these are unable to satisfy the customer's new regulatory requirements, the customer may terminate the applicable Online Service without cause by giving 60 days' prior written notice.
60	Will the financial institution (or its resource operator, if applicable) be notified by the service provider with regard to any change in the application functionality other than changes relating to corrective measures prior to its implementation?	Part II, Chapter 2, point 142(c) and (d) of the Circular. Part 2 of this checklist maps this requirement against the contractual documents with each of Microsoft's financial institution customers. Please note that where only non-critical/important functions are outsourced to a cloud computing infrastructure and in accordance with their risk analysis, financial institutions may justify not applying the requirement of the Circular relating to the notification by the service provider in case of change of functionalities.

REF.	QUESTION / REQUIREMENT	GUIDANCE
61	Does the outsourcing agreement allow the financial institution to terminate the agreement in accordance with applicable law, including in the following situations: a. where the provider is in breach of applicable law, regulations or contractual provisions; b. where impediments capable of altering the performance of the outsourced function are identified; c. where there are material changes affecting the outsourcing arrangement or the service provider (e.g. sub-outsourcing or changes of sub-contractors); d. where there are weaknesses regarding the management and security of confidential, personal or otherwise sensitive data or information; and e. where instructions are given by the regulator, e.g. in the case that the regulator is, caused by the outsourcing arrangement, no longer in a position to effectively supervise the financial institution?	Part I, point 77(q) and 101, 103 and 118(a) of the Circular. Part 2 of this checklist maps this requirement against the contractual documents with each of Microsoft's financial institution customers. The financial institution must ensure that the outsourcing agreement does not include any termination or service termination clause in case of bankruptcy, controlled management, suspension of payments, compositions and arrangements with creditors aimed at preventing bankruptcy or other similar proceedings. Please note that where only non-critical/important functions are outsourced to a cloud computing infrastructure and in accordance with their risk analysis, financial institutions may justify not applying the requirement of the Circular relating to continuity in case of resolution or reorganisation or another procedure.

REF.	QUESTION / REQUIREMENT	GUIDANCE
62	Does the outsourcing agreement facilitate the transfer of the outsourced function to another service provider or its re-incorporation into the financial institution whenever the continuity or quality of the service provision are likely to be affected? Does the outsourcing agreement therefore: • clearly set out the obligations of the existing service provider in those cases; • set an appropriate transition period, during which the service provider, after the termination of the outsourcing agreement, would continue to provide the outsourced function to reduce the risk of disruptions; • include an obligation of the service provider to support the financial institution in the orderly transfer of the function in the event of the termination of the outsourcing agreement; and • include an obligation of the service provider to erase the data and systems of the financial institution within a reasonable timeframe when the contract is terminated?	Part I, point 77(a) and 102 of the Circular. Part 2 of this checklist maps this requirement against the contractual documents with each of Microsoft's financial institution customers. Upon expiration or termination, the customer can extract its data. As set out in the OST, Microsoft will retain customer data stored in the Online Service in a limited function account for 90 days after expiration or termination of the customer's subscription so that the customer may extract the data. After the 90-day retention period ends, Microsoft will disable the customer's account and delete the customer data. Microsoft will disable the account and delete customer data from the account no more than 180 days after expiration or termination of customer's use of an Online Service. Ownership of documents, records and other data remain with the customer and at no point transfer to Microsoft or anyone else, so this does not need to be addressed through transition. Being a cloud services solution, ownership of software and hardware used to provide the service remains with Microsoft.

REF.	QUESTION / REQUIREMENT	GUIDANCE
63	Does the outsourcing agreement provide for the right of the financial institution to monitor the service provider's performance on an ongoing basis?	Part I, point 77(h) of the Circular. See Questions 36 and 37. Part 2 of this checklist maps this requirement against the contractual documents with each of Microsoft's financial institution customers.
64	Does the outsourcing agreement provide for the unrestricted right of the financial institution and competent authorities to audit and inspect the service provider, including in case of sub-outsourcing, with regard to, at least, the critical or important outsourced function, including (continued)	Part I, point 77(p), 88 to 91 of the Circular. Yes. There are terms in the contract that enable the regulator to carry out inspection or examination of Microsoft's facilities, systems, processes and data relating to the services. Pursuant to the Financial Services Amendment, Microsoft provides the regulator with a direct right to examine the Online Services, including the ability to conduct an on-premise examination, to meet with Microsoft personnel and Microsoft's external auditors, and to access any related information, records, reports and documents, in the event that the regulator requests to examine the Online Services operations in order to meet their supervisory obligations. Microsoft will cause the performance of audits of the security of the computers, computing environment and physical datacenters that it uses in processing customer data for each Online Service. Customers may also participate in the optional Financial Services Compliance Program to have additional monitoring, supervisory and audit rights and additional controls over the Online Services. Under the outsourcing agreement, Microsoft commits that it will not disclose customer data to the regulator except as required by law or at the direction or consent of the customer.

Continued Next Page »

REF.	QUESTION / REQUIREMENT	GUIDANCE
64		
	• guaranteed access by the internal audit function, statutory auditor and the CSSF to the information relating to the outsourced functions including relevant data kept by the service provider, (in the cases provided for in the applicable national law) the power to perform on-site inspection of the service provider; • the right of the internal control functions to have access to any documentation relating to the outsourced function, at any time and without difficulty, to maintain these function's continued ability to exercise their controls; and • a reference to the information gathering and investigatory powers of competent authorities under Articles 49, 53 and 59 LFS[3], Articles 31, 38 and 58-5 LPS[4] and, where applicable, resolution authorities under Article 61(1) BRRD Law[5]?	Microsoft's cloud services are subject to regular independent third party audits, including SSAE16 SOC1 Type II, SSAE SOC2 Type II, ISO/IEC 27001, ISO/IEC 27002 and ISO/IEC 27018. Rigorous third-party audits, including by Deloitte, validate the adherence of the Online Services to the strict requirements of these standards

[3] Law of 5 April 1993 on the Financial Sector, as amended.
[4] Law of 10 November 2009 on Payment Services, as amended.
[5] Law of 18 December 2015 on the resolution, reorganisation and winding up measures of credit institutions and certain investment firms and on deposit guarantee and investor compensation schemes, as amended.

REF.	QUESTION / REQUIREMENT	GUIDANCE
65	Does the outsourcing agreement contain the obligation for the service provider to cooperate with the CSSF and, where applicable, the resolution authorities, including the persons appointed by them?	Part I, point 77(n) of the Circular. See Question 64 above. Part 2 of this checklist maps this requirement against the contractual documents with each of Microsoft's financial institution customers.

REF.	QUESTION / REQUIREMENT	GUIDANCE
66	Do the inspection and audit rights with regard to the outsourcing of critical or important functions grant the financial institution, its statutory auditor, the CSSF, where applicable the resolution authority and any other person appointed by the financial institution, CSSF or resolution authority: • full access to all relevant business premises, including the full range of relevant devices, systems, networks, information and data used for providing the outsourced function, including related financial information, personnel and the service provider's external auditors ('access and information rights'); and (continued)	Part I, point 77(p) and 90 of the Circular. See Question 64. Part 2 of this checklist maps this requirement against the contractual documents with each of Microsoft's financial institution customers

Continued Next Page »

REF.	QUESTION / REQUIREMENT	GUIDANCE
66	• unrestricted rights of inspection and auditing related to the outsourcing arrangement ('audit rights'), including the possibility for the CSSF to communicate any observations made in this context to the financial institution, to enable them to monitor the outsourcing arrangement and ensure compliance with the applicable regulatory and contractual requirements?	

REF.	QUESTION / REQUIREMENT	GUIDANCE
67	Where the financial institution uses third-party certifications and third-party or internal audit reports made available by the service provider, does the financial institution have the contractual right to (i) request the expansion of scope of further certifications or audit reports to some systems and/or controls, provided that the number and frequency of such requests for scope modification should be reasonable and legitimate from a risk management perspective and (ii) to perform individual audits at their discretion with regard to the outsourcing of critical or important functions?	Part I, point 96(g) and (h) of the Circular. Microsoft makes available certain tools through the Service Trust Platform to enable customers to conduct their own virtual audits of the Online Services. Part 2 of this checklist maps this requirement against the contractual documents with each of Microsoft's financial institution customers.

REF.	QUESTION / REQUIREMENT	GUIDANCE
68	For BRRD institutions, does the outsourcing agreement contain a clear reference to the national resolution authority's powers, especially to Articles 59-47, 66 and 69 of the BRRD Law[6], and in particular, a description of the 'substantive obligations'[7] of the contract in the sense of the Articles 59-47 and 66 of the BRRD Law?	Part I, point 77(o) of the Circular. Part 2 of this checklist maps this requirement against the contractual documents with each of Microsoft's financial institution customers.

[6] Law of 18 December 2015 on the resolution, reorganisation and winding up measures of credit institutions and certain investment firms and on deposit guarantee and investor compensation schemes, as amended.
[7] At least any payment or delivery obligation and the provision of collateral are deemed to be 'substantive obligations'.

REF.	QUESTION / REQUIREMENT	GUIDANCE
	E. TECHNICAL AND OPERATIONAL RISK Q&A Under various regulatory requirements, including its business continuity management and IT security risk requirements (which are not specific to outsourcing but should be considered nonetheless in the context of the outsourcing) financial institutions need to have in place appropriate measures to address IT risk, security risk, IT security risk and operational risk. This section provides some more detailed technical and operational information about Microsoft cloud services which should address many of the technical and operational questions that may arise. If other questions arise, please do not hesitate to get in touch with your Microsoft contact.	
69	Does the financial institution maintain an information security policy covering all IT activities spread among the financial institution and all the actors in the outsourcing chain to be implemented accordingly?	Section 3.4.1 of the EBA ICT Guidelines as endorsed by CSSF Circular 20/750.

REF.	QUESTION / REQUIREMENT	GUIDANCE
70	Does the financial institution maintain an information security policy covering all IT activities spread among the financial institution and all the actors in the outsourcing chain to be implemented accordingly?	Section 3.6.1, point 65 of the EBA ICT Guidelines as endorsed by CSSF Circular 20/750.

REF.	QUESTION / REQUIREMENT	GUIDANCE
71	What security controls are in place to protect the transmission and storage of confidential information such as customer data within the infrastructure of the service provider? (continued)	Part I, point 83 to 87 of the Circular. Microsoft as an outsourcing partner is an industry leader in cloud security and implements policies and controls on par with or better than on-premises datacenters of even the most sophisticated organisations. Microsoft cloud services were built based on ISO/IEC 27001 and ISO/IEC 27018 standards, a rigorous set of global standards covering physical, logical, process and management controls. The Microsoft cloud services security features consist of three parts: (a) built-in security features; (b) security controls; and (c) scalable security. These include 24-hour monitored physical hardware, isolated customer data, automated operations and lock-box processes, secure networks and encrypted data. Microsoft implements the Microsoft Security Development Lifecycle (SDL) which is a comprehensive security process that informs every stage of design, development and deployment of Microsoft cloud services. Through design requirements, analysis of attack surface and threat modelling, the SDL helps Microsoft predict, identify and mitigate vulnerabilities and threats from before a service is launched through its entire production lifecycle. Networks within Microsoft's data centers are segmented to provide physical separation of critical back- end servers and storage devices from the public-facing interfaces. Edge router security allows the ability to detect intrusions and signs of vulnerability. Customer access to services provided over the Internet originates from users' Internet-enabled locations and ends at a Microsoft datacenter. These connections are encrypted using industry-standard transport layer security TLS. The use of TLS establishes a highly secure client-to-server connection to help provide data confidentiality and integrity between the desktop and the datacenter. Customers can configure TLS between Microsoft cloud services and external servers for both inbound and outbound email. This feature is enabled by default. Microsoft also implements traffic throttling to prevent denial-of-service attacks. It uses the "prevent, detect and mitigate breach" process as a defensive strategy to predict and prevent security breaches before they happen. This involves continuous improvements to built-in security features, including port- scanning and remediation, perimeter vulnerability scanning, OS patching to the latest updated security software, network-level DDOS detection and prevention and multi-factor authentication for service access. Use of a strong password is enforced as mandatory, and the password must be changed on a regular basis. From a people and process standpoint, preventing breach involves auditing all operator/administrator access and actions, zero standing permission for administrators in the service, "Just-In-Time (JIT) access and elevation" (that is, elevation is granted on an as-needed and only-at-the time-of-need basis) of engineer privileges to troubleshoot the service, and isolation of the employee email environment from the production access environment. Employees who have not passed

Continued Next Page »

REF.	QUESTION / REQUIREMENT	GUIDANCE
71	What security controls are in place to protect the transmission and storage of confidential information such as customer data within the infrastructure of the service provider?	background checks are automatically rejected from high privilege access, and checking employee backgrounds is a highly scrutinized, manual-approval process. Preventing breach also involves automatically deleting unnecessary accounts when an employee leaves, changes groups, or does not use the account prior to its expiration. Data is also encrypted. Customer data in Microsoft cloud services exists in two states: • at rest on storage media; and • in transit from a data center over a network to a customer device. Microsoft offers a range of built-in encryption capabilities to help protect data at rest. • For Office 365, Microsoft follows industry cryptographic standards such as TLS/SSL and AES to protect the confidentiality and integrity of customer data. For data in transit, all customer- facing servers negotiate a secure session by using TLS/SSL with client machines to secure the customer data. For data at rest, Office 365 deploys BitLocker with AES 256-bit encryption on servers that hold all messaging data, including email and IM conversations, as well as content stored in SharePoint Online and OneDrive for Business. Additionally, in some scenarios, Microsoft uses file-level encryption. For Azure, technological safeguards such as encrypted communications and operational processes help keep customers' data secure. Microsoft also provides customers the flexibility to implement additional encryption and manage their own keys. For data in transit, Azure uses industry-standard secure transport protocols, such as TLS/SSL, between user devices and Microsoft datacenters. For data at rest, Azure offers many encryption options, such as support for AES-256, giving customers the flexibility to choose the data storage scenario that best meets the customer's needs. • Such policies and procedures are available through Microsoft's online resources, including the Trust Center and the Service Trust Platform.

REF.	QUESTION / REQUIREMENT	GUIDANCE
72	How is the financial institution's data isolated from other data held by the service provider?	For all of its Online Services, Microsoft logically isolates customer data from the other data Microsoft holds. For example, Microsoft Office 365 is a multi-tenant service designed to host multiple tenants in a highly secure way through data isolation. Data storage and processing for each tenant is segregated through an "Active Directory" structure, which isolates customers using security boundaries ("silos"). The silos safeguard the customer's data such that the data cannot be accessed or compromised by co-tenants.
73	How are the service provider's access logs monitored?	Part II, Chapter 2, point 135(a) of the Circular. Microsoft provides monitoring and logging technologies to give its customers maximum visibility into the activity on their cloud-based network, applications, and devices, so they can identify potential security gaps. The Online Services contain features that enable customers to restrict and monitor their employees' access to the services, including the Azure AD Privileged Identify Management system and Multi-Factor Authentication. In addition, the Online Services include built-in approved Windows PowerShell Scripts, which minimise the access rights needed and the surface area available for misconfiguration. Microsoft logs, or enables customers to log, access and use of information systems containing customer data, registering the access ID, time, authorisation granted or denied, and relevant activity. An internal, independent Microsoft team audits the log at least once per quarter, and customers have access to such audit logs. In addition, Microsoft periodically reviews access levels to ensure that only users with appropriate business justification have access to appropriate systems.

REF.	QUESTION / REQUIREMENT	GUIDANCE
74	What policies does the service provider have in place to monitor employees with access to confidential information?	For certain core services of Office 365 and Azure, personnel (including employees and subcontractors) with access to customer data content are subject to background screening, security training, and access approvals as allowed by applicable law. Background screening takes place before Microsoft authorises the employee to access customer data. To the extent permitted by law, any criminal history involving dishonesty, breach of trust, money laundering, or job-related material misrepresentation, falsification, or omission of fact may disqualify a candidate from employment, or, if the individual has commenced employment, may result in termination of employment at a later day.
75	How are customers authenticated?	Microsoft cloud services use two-factor authentication to enhance security. Typical authentication practices that require only a password to access resources may not provide the appropriate level of protection for information that is sensitive or vulnerable. Two-factor authentication is an authentication method that applies a stronger means of identifying the user. The Microsoft phone-based two-factor authentication solution allows users to receive their PINs sent as messages to their phones, and then they enter their PINs as a second password to log on to their services.
76	What are the procedures for identifying, reporting and responding to suspected security incidents and violations? (continued)	First, there are robust procedures offered by Microsoft that enable the prevention of security incidents and violations arising in the first place and detection if they do occur. Specifically: • Microsoft implements 24 hour monitored physical hardware. Datacenter access is restricted 24 hours per day by job function so that only essential personnel have access to customer applications and services. Physical access control uses multiple authentication and security processes, including badges and smart cards, biometric scanners, on-premises security officers, continuous video surveillance, and two-factor authentication. • Microsoft implements "prevent, detect, and mitigate breach", which is a defensive strategy aimed at predicting and preventing a security breach before it happens. This involves continuous improvements to built-in security features, including port scanning and remediation, perimeter vulnerability scanning, OS patching to the latest updated security software, network-level DDOS(distributed denial-of-service) detection and prevention, and

Continued Next Page »

REF.	QUESTION / REQUIREMENT	GUIDANCE
76	What are the procedures for identifying, reporting and responding to suspected security incidents and violations? (continued)	multi-factor authentication for service access. In addition, Microsoft has anti-malware controls to help avoid malicious software from gaining unauthorised access to customer data. Microsoft implements traffic throttling to prevent denial-of-service attacks, and maintains a set of Security Rules for managed code to help ensure that application cybersecurity threats are detected and mitigated before the code is deployed. • Microsoft employs some of the world's top experts in cybersecurity, cloud compliance, and financial services regulation. Its Digital Crimes Unit, for example, employs cyber experts, many of whom previously worked for law enforcement, to use the most advanced tools to detect, protect, and respond to cybercriminals. Its Cyber Defense Operations Center brings together security response experts from across Microsoft to help protect, detect, and respond 24/7 to security threats against Microsoft's infrastructure and Online Services in real-time. General information on cybersecurity can be found here. • Microsoft conducts a risk assessment for Azure at least annually to identify internal and external threats and associated vulnerabilities in the Azure environment. Information is gathered from numerous data sources within Microsoft through interviews, workshops, documentation review, and analysis of empirical data. The assessment follows a documented process to produce consistent, valid, and comparable results year over year. • Wherever possible, human intervention is replaced by an automated, tool-based process, including routine functions such as deployment, debugging, diagnostic collection, and restarting services. Microsoft continues to invest in systems automation that helps identify abnormal and suspicious behaviour and respond quickly to mitigate security risk. Microsoft is continuously developing a highly effective system of automated patch deployment that generates and deploys solutions to problems identified by the monitoring systems—all without human intervention. This greatly enhances the security and agility of the service. • Microsoft allows customers to monitor security threats on their server by providing access to the Azure Security Center, Office 365 Advanced Threat Analytics, Azure Status Dashboard, and the Office 365 Service Health Dashboard, among other online resources. • Microsoft maintains 24-hour monitoring of its Online Services and records all security breaches. For security breaches resulting in unlawful or unauthorised access to Microsoft's equipment, facilities, or customer data, Microsoft notifies affected parties without unreasonable delay. Microsoft conducts a thorough review of all information security incidents.

Continued Next Page »

REF.	QUESTION / REQUIREMENT	GUIDANCE
76	What are the procedures for identifying, reporting and responding to suspected security incidents and violations? (continued)	Microsoft conducts penetration tests to enable continuous improvement of incident response procedures. These internal tests help Microsoft cloud services security experts create a methodical, repeatable, and optimised stepwise response process and automation. In addition, Microsoft provides customers with the ability to conduct their own penetration testing of the services. This is done in accordance with Microsoft's rules of engagement, which do not require Microsoft's permission in advance of such testing. Second, if a security incident or violation is detected, Microsoft Customer Service and Support notifies customers by updating the Service Health Dashboard. Customers would have access to Microsoft's dedicated support staff, who have a deep knowledge of the service. Microsoft provides Recovery Time Objective (RTO) commitments. These differ depending on the applicable Microsoft service and are outlined further below. Finally, after the incident, Microsoft provides a thorough post-incident review report (PIR). The PIR includes: o An incident summary and event timeline. o Broad customer impact and root cause analysis. o Actions being taken for continuous improvement. If the customer is affected by a service incident, Microsoft shares the post-incident review with them. Microsoft's commitment to cybersecurity and data privacy, including restrictions on access to customer data, are set forth in Microsoft's contracts with customers. In summary: • Logical Isolation. Microsoft logically isolates customer data from the other data Microsoft holds. This isolation safeguards customers' data such that the data cannot be accessed or compromised by co-tenants. • 24-Hour Monitoring & Review of Information Security Incidents. Microsoft maintains 24-hour monitoring of its Online Services and records all security breaches. Microsoft conducts a thorough review of all information security incidents. For security breaches resulting in unlawful or unauthorised access to Microsoft's equipment, facilities, or customer data, Microsoft notifies affected parties without unreasonable delay. For more information regarding Microsoft's security incident management, refer to http://aka.ms/SecurityResponsepaper.

Continued Next Page »

REF.	QUESTION / REQUIREMENT	GUIDANCE
76	What are the procedures for identifying, reporting and responding to suspected security incidents and violations?	• Minimising Service Disruptions - Redundancy. Microsoft makes every effort to minimise service disruptions, including by implementing physical redundancies at the disk, Network Interface Card ("NIC"), power supply, and server levels; constant content replication; robust backup, restoration, and failover capabilities; and real-time issue detection and automated response such that workloads can be moved off any failing infrastructure components with no perceptible impact on the service. • Resiliency. Microsoft Online Services offer active load balancing, automated failover and human backup, and recovery testing across failure domains. • Distributed Services. Microsoft offers distributed component services to limit the scope and impact of any failures of a single component, and directory data is replicated across component services to insulate one service from another in the event of a failure. • Simplification. Microsoft uses standardised hardware to reduce issue isolation complexities. Microsoft also uses fully automated deployment models and a standard built-in management mechanism. • Human Backup. Microsoft Online Services include automated recovery actions with 24/7 on- call support; a team with diverse skills on call to provide rapid response and resolution; and continuous improvement through learning from the on-call teams. • Disaster Recovery Tests. Microsoft conducts disaster recovery tests at least once per year. Customers also have access to the Azure Security Center, Office 365 Advanced Threat Analytics, Azure Status Dashboard, and the Office 365 Service Health Dashboard, among other online resources, which allow customers to monitor security threats on the cloud service provider's server.

REF.	QUESTION / REQUIREMENT	GUIDANCE
77	How is end-to-end application encryption security implemented to protect PINs and other sensitive data transmitted between terminals and hosts? (continued)	Microsoft cloud services use industry-standard secure transport protocols for data as it moves through a network—whether between user devices and Microsoft datacenters or within datacenters themselves. To help protect data at rest, Microsoft offers a range of built-in encryption capabilities. There are three key aspects to Microsoft's encryption: • Secure identity: Identity (of a user, computer, or both) is a key element in many encryption technologies. For example, in public key (asymmetric) cryptography, a key pair—consisting of a public and a private key—is issued to each user. Because only the owner of the key pair has access to the private key, the use of that key identifies the associated owner as a party to the encryption/decryption process. Microsoft Public Key Infrastructure is based on certificates that verify the identity of users and computers. • Secure infrastructure: Microsoft uses multiple encryption methods, protocols, and algorithms across its products and services to help provide a secure path for data to travel through the infrastructure, and to help protect the confidentiality of data that is stored within the infrastructure. Microsoft uses some of the strongest, most secure encryption protocols in the industry to provide a barrier against unauthorised access to our data. Proper key management is an essential element in encryption best practices, and Microsoft helps ensure that encryption keys are properly secured. Protocols and technologies examples include: a) Transport Layer Security (TLS), which uses symmetric cryptography based on a shared secret to encrypt communications as they travel over the network. b) Internet Protocol Security (IPsec), an industry-standard set of protocols used to provide authentication, integrity, and confidentiality of data at the IP packet level as it's transferred across the network. c) Office 365 servers using BitLocker to encrypt the disk drives containing log files and customer data at rest at the volume-level. BitLocker encryption is a data protection feature built into Windows to safeguard against threats caused by lapses in controls (e.g., access control or recycling of hardware) that could lead to someone gaining physical access to disks containing customer data. d) BitLocker deployed with Advanced Encryption Standard (AES) 256-bit encryption on disks containing customer data in Exchange Online, SharePoint Online, and Skype for Business. Advanced Encryption Standard (AES)-256 is the National Institute of Standards and Technology (NIST) specification for a symmetric key data encryption that was adopted by the US government to replace Data Encryption Standard (DES) and RSA 2048 public key encryption technology.

Continued Next Page »

REF.	QUESTION / REQUIREMENT	GUIDANCE
77	How is end-to-end application encryption security implemented to protect PINs and other sensitive data transmitted between terminals and hosts?	BitLocker encryption that uses AES to encrypt entire volumes on Windows server and client machines, which can be used to encrypt Hyper-V virtual machines when a virtual Trusted Platform Module (TPM) is added. BitLocker also encrypts Shielded VMs in Windows Server 2016, to ensure that fabric administrators cannot access the information inside the virtual machine. The Shielded VMs solution includes the Host Guardian Service feature, which is used for virtualization host attestation and encryption key release. e) Office 365 offers service-level encryption in Exchange Online, Skype for Business, SharePoint Online, and OneDrive for Business with two key management options — Microsoft managed and Customer Key. Customer Key is built on service encryption and enables customers to provide and control keys that are used to encrypt their data at rest in Office 365. f) Microsoft Azure Storage Service Encryption encrypts data at rest when it is stored in Azure Blob storage. Azure Disk Encryption encrypts Windows and Linux infrastructure as a service (IaaS) virtual machine disks by using the BitLocker feature of Windows and the DM-Crypt feature of Linux to provide volume encryption for the operating system and the data disk. g) Transparent Data Encryption (TDE) encrypts data at rest when it is stored in an Azure SQL database. h) Azure Key Vault helps easily and cost-effectively manage and maintain control of the encryption keys used by cloud apps and services via a FIPS 140-2 certified cloud based hardware security module (HSM). i) Microsoft Online Services also transport and store secure/multipurpose Internet mail extensions (S/MIME) messages and transport and store messages that are encrypted using client-side, third-party encryption solutions such as Pretty Good Privacy (PGP). • Secure apps and data: The specific controls for each Microsoft cloud service are described in more detail at microsoft.com/en-us/trustcenter/security/encryption.

REF.	QUESTION / REQUIREMENT	GUIDANCE
78	Are there procedures established to securely destroy or remove the data when the need arises (for example, when the contract terminates)?	Part I, point 102(d) of the Circular. Yes. Microsoft uses best practice procedures and a wiping solution that is NIST 800-88, ISO/IEC 27001, ISO/IEC 27018, SOC 1 and SOC 2 compliant. For hard drives that cannot be wiped it uses a destruction process that destroys it (i.e. shredding) and renders the recovery of information impossible (e.g., disintegrate, shred, pulverize, or incinerate). The appropriate means of disposal is determined by the asset type. Records of the destruction are retained. All Microsoft online services utilise approved media storage and disposal management services. Paper documents are destroyed by approved means at the pre-determined end-of-life cycle. In its contracts with customers, Microsoft commits to disabling a customer's account and deleting customer data from the account no more than 180 days after the expiration or termination of the Online Service. "Secure disposal or re-use of equipment and disposal of media" is covered under the ISO/IEC 27001 standards against which Microsoft is certified.
79	Are there documented security procedures for safeguarding premises and restricted areas? If yes, provide descriptions of these procedures.	Part I, point 87of the Circular. Yes. Physical access control uses multiple authentication and security processes, including badges and smart cards, biometric scanners, on-premises security officers, continuous video surveillance and two-factor authentication. The datacenters are monitored using motion sensors, video surveillance and security breach alarms.

REF.	QUESTION / REQUIREMENT	GUIDANCE
80	Are there documented security procedures for safeguarding hardware, software and data in the data center? Do such security measures comply with the financial institution's security policy?	Part I, points 84 to 87 of the Circular. Yes. These are described at length in the Microsoft Trust Center at microsoft.com/trust. For information on: • design and operational security see microsoft.com/en-us/trustcenter/security/designopsecurity • network security see microsoft.com/en-us/trustcenter/security/networksecurity • encryption see microsoft.com/en-us/trustcenter/security/encryption • threat management see microsoft.com/en-us/trustcenter/security/threatmanagement • identify and access management see microsoft.com/en-us/trustcenter/security/identity
81	How are privileged system administration accounts managed? (continued)	Microsoft applies strict controls over access to customer data. Access to the IT systems that store customer data is strictly controlled via role-based access control (RBAC) and lock box processes. Access control is an automated process that follows the separation of duties principle and the principle of granting least privilege. This process ensures that the engineer requesting access to these IT systems has met the eligibility requirements, such as a background screen, required security training, and access approvals. In addition, the access levels are reviewed on a periodic basis to ensure that only users who have appropriate business justification have access to the systems. This process ensures that the engineer requesting access to these IT systems has met the eligibility requirements. In addition, the Online Services include built-in approved Windows PowerShell Scripts, which minimise the access rights needed and the surface area available for misconfiguration. For more information regarding Microsoft identity and access management, see microsoft.com/en-us/trustcenter/security/identity.

Continued Next Page »

REF.	QUESTION / REQUIREMENT	GUIDANCE
81	Describe the procedures governing the issuance (including emergency usage), protection, maintenance and destruction of these accounts. Please describe how the privileged accounts are subjected to dual control (e.g. password is split into 2 halves and each given to a different staff for custody).	Microsoft provides monitoring and logging technologies to give customers maximum visibility into the activity on their cloud-based network, applications, and devices, so they can identify potential security gaps. The Online Services contain features that enable customers to restrict and monitor their employees' access to the services, including the Azure AD Privileged Identify Management system and Multi-Factor Authentication. Microsoft logs, or enables customers to log, access and use of information systems containing customer data, registering the access ID, time, authorisation granted or denied, and relevant activity (see Online Services Terms, page 13). An internal, independent Microsoft team audits the log at least once per quarter, and customers have access to such audit logs. In addition, Microsoft periodically reviews access levels to ensure that only users with appropriate business justification have access to appropriate systems. Microsoft provides customers with information to reconstruct financial transactions and develop audit trail information through two primary sources: Azure Active Directory reporting, which is a repository of audit logs and other information that can be retrieved to determine who has accessed customer transaction information and the actions they have taken with respect to such information, and Azure Monitor, which provides activity logs and diagnostic logs that customers can use to determine the "what, who, and when" with respect to changes to customer cloud information and to obtain information about the operation of the Online Services, respectively. In emergency situations, a "JIT (as defined above) access and elevation system" is used (that is, elevation is granted on an as-needed and only-at-the-time-of-need basis) of engineer privileges to troubleshoot the service.

REF.	QUESTION / REQUIREMENT	GUIDANCE
82	Are the activities of privileged accounts captured (e.g. system audit logs) and reviewed regularly? Indicate the party reviewing the logs and the review frequency.	Yes. An internal, independent Microsoft team will audit the log at least once per quarter. More information is available at microsoft.com/en-us/trustcenter/security/auditingandlogging.
83	Are the audit/activity logs protected against tampering by users with privileged accounts? Describe the safeguards implemented.	Yes. Microsoft logs, or enables customers to log, access and use of information systems containing customer data, registering the access ID, time, authorization granted or denied, and relevant activity (see Online Services Terms, page 13). An internal, independent Microsoft team audits the log at least once per quarter, and customers have access to such audit logs. In addition, Microsoft periodically reviews access levels to ensure that only users with appropriate business justification have access to appropriate systems. All logs are saved to the log management system which a different team of administrators manages. All logs are automatically transferred from the production systems to the log management system in a secure manner and stored in a tamper-protected way.

REF.	QUESTION / REQUIREMENT	GUIDANCE
84	Does the financial institution fulfil the appropriate safeguards in relation to outsourcing? More particularly: • will access to data and systems that the financial institution owns on a cloud computing infrastructure be restricted for the service provider and subject to preventive and detective measures as well as prior and explicit agreement of the institution (unless in the event of extreme urgency in which case the institution should be informed *a posteriori*); and (continued)	Part II, Chapter 2, point 136 of the Circular. Yes. System level data such as configuration data/file and commands are managed as part of the configuration management system. Any changes or updates to or deletion of those data/files/commands will be automatically deleted by the configuration management system as anomalies. Further, Microsoft applies strict controls over access to customer data. Access to the IT systems that store customer data is strictly controlled via role-based access control (RBAC) and lock box processes. Access control is an automated process that follows the separation of duties principle and the principle of granting least privilege. This process ensures that the engineer requesting access to these IT systems has met the eligibility requirements, such as a background screen, required security training, and access approvals. In addition, the access levels are reviewed on a periodic basis to ensure that only users who have appropriate business justification have access to the systems. This process ensures that the engineer requesting access to these IT systems has met the eligibility requirements. In addition, the Online Services include built-in approved Windows PowerShell Scripts, which minimise the access rights needed and the surface area available for misconfiguration. For more information regarding Microsoft identity and access management, see microsoft.com/en-us/trustcenter/security/identity. See Question 7.

Continued Next Page »

REF.	QUESTION / REQUIREMENT	GUIDANCE
	• will the financial institution safeguard that the cloud service provision does not entail any manual interaction by the cloud computing service provider as regards the day-to-day management of the cloud computing resources used by the financial institution except (i) in cases of global management of IT systems supporting the cloud computing infrastructure or (ii) within the context of a specific request by the financial institution?	
85	What remote access controls are implemented?	Administrators who have rights to applications have no physical access to the production systems. So administrators have to securely access the applications remotely via a controlled, and monitored remote process called lockbox. All operations through this remote access facility are logged. Further, Microsoft applies strict controls over access to customer data. Access to the IT systems that store customer data is strictly controlled via role-based access control (RBAC) and lock box processes. Access control is an automated process that follows the separation of duties principle and the principle of granting least privilege. This process ensures that the engineer requesting access to these IT systems has met the eligibility requirements, such as a background screen, required security training, and access approvals. In addition, the access levels are reviewed on a periodic basis to ensure that only users who have appropriate business justification have access to the systems. This process ensures that the engineer requesting access to these IT systems has met the eligibility requirements. In addition, the Online Services include built-in approved Windows PowerShell Scripts, which minimise the access rights needed and the surface area available for misconfiguration. For more information regarding Microsoft identity and access management, see microsoft.com/en-us/trustcenter/security/identity.

REF.	QUESTION / REQUIREMENT	GUIDANCE
86	Does the service provider have a disaster recovery or business continuity plan? Have you considered any dependencies between the plan(s) and those of your financial institution? Has the financial institution taken appropriate measures to secure business continuity?	Part I, Section 4.2.5. and 4.3.4. and point 49 of the Circular. Yes. Microsoft makes every effort to minimize service disruptions by implementing a highly resilient online service design with both physically and logically redundant systems that replicate data across multiple systems and data centers. The service also benefits from real-time monitoring, issue detection and automated recovery systems (=automated response so that workloads hindered by problems can be moved away from any failing infrastructure components to healthy systems). Disaster recovery planning and testing is part of our Enterprise Business Continuity Management process for which we report results on a quarterly basis. The financial institution still needs to examine any critical business or technical processes that rely on cloud services and establish their own internal end-to-end disaster recovery or business continuity plan (DRP/BCP) to deal with any outages that affect access those services. This includes power issues/failures within the organization, network failures and 3rd-party supplier outages such as cloud services, ISP, or DNS. Microsoft recommends reviewing the M365 Resiliency & Customer Guidance white paper for further guidance on incorporating these considerations into your BCP. More info is available on the Service Trust Portal: Data Resiliency in Office 365, M365 Resiliency & Customer Guidance, Azure Resiliency, the Microsoft Enterprise Business Continuity Program (EBCM) and the latest published EBCM report. Also see the Financial Services Compliance Program; Premier Support; Office 365 Support; Premier Support for Enterprise; and Azure Support Plans.

REF.	QUESTION / REQUIREMENT	GUIDANCE
87	What are the recovery time objectives (RTO) of systems or applications outsourced to the service provider?	Customers can review Microsoft's SLAs and details on its business continuity and failover testing in appropriate whitepapers and policy documents (available at https://servicetrust.microsoft.com/ViewPage/TrustDocuments).
88	What are the recovery point objectives (RPO) of systems or applications outsourced to the service provider?	• Office 365: Peer replication between datacenters ensures that there are always multiple live copies of any data. Standard images and scripts are used to recover lost servers, and replicated data is used to restore customer data. Because of the built-in data resiliency checks and processes, Microsoft maintains backups only of Office 365 information system documentation (including security-related documentation), using built-in replication in SharePoint Online and our internal code repository tool, Source Depot. System documentation is stored in SharePoint Online, and Source Depot contains system and application images. Both SharePoint Online and Source Depot use versioning and are replicated in near real-time. • Azure: Backup and resiliency RPO is provided on a service-by-service basis, with information on each Azure service available from the Azure Trust Center: microsoft.com/en-us/trustcenter/cloudservices/azure • 1 minute of less for Virtual Storage

REF.	QUESTION / REQUIREMENT	GUIDANCE
89	What are the data backup and recovery arrangements for your organisation's data that resides with the service provider? (continued)	Redundancy • Physical redundancy at server, datacenter, and service levels. • Data redundancy with robust failover capabilities. • Functional redundancy with offline functionality. Microsoft's redundant storage and its procedures for recovering data are designed to attempt to reconstruct customer data in its original or last-replicated state from before the time it was lost or destroyed. Additionally, Microsoft maintains multiple live copies of data at all times. Live data is separated into "fault zones", which ensure continuous access to data. For Office 365, Microsoft maintains multiple copies of customer data across for redundancy. For Azure, Microsoft may copy customer data between regions within a given geography for data redundancy or other operational purposes. For example, Azure Globally-Redundant Storage replicates certain data between two regions within the same geography for enhanced data durability in case of a major data center disaster. Resiliency • Active/active load balancing. • Automated failover with human backup. • Recovery testing across failure domains. For example, Azure Traffic Manager provides load balancing between different regions, and the customer can use network virtual appliances in its Azure Virtual Networks for application delivery controllers (ADC/load balancing) functionality. Load balancing is also provided by Power BI Services, the Gateway, and Azure API Management roles. Office 365 services have been designed around specific resiliency principles that are designed to protect data from corruption, to separate data into different fault zones, to monitor data for failing any part of the ACID test, and to allow customers to recover on their own.

Continued Next Page »

REF.	QUESTION / REQUIREMENT	GUIDANCE
89	What are the data backup and recovery arrangements for your organisation's data that resides with the service provider?	**Distributed Services** • Distributed component services like Exchange Online, SharePoint Online, and Skype for Business Online limit scope and impact of any failures in a component. • Directory data replicated across component services insulates one service from another in any failure events. • Simplified operations and deployment. **Monitoring** • Internal monitoring built to drive automatic recovery. • Outside-in monitoring raises alerts about incidents. • Extensive diagnostics provide logging, auditing, and granular tracing. **Simplification** • Standardised hardware reduces issue isolation complexities. • Fully automated deployment models. • Standard built-in management mechanism. **Human Backup** • Automated recovery actions with 24/7 on-call support. • Team with diverse skills on the call provides rapid response and resolution. • Continuous improvement by learning from the on-call teams. **Continuous learning** • If an incident occurs, Microsoft does a thorough post-incident review every time. • Microsoft's post-incident review consists of analysis of what happened, Microsoft's response, and Microsoft's plan to prevent it in the future. • If the organisation was affected by a service incident, Microsoft shares the post-incident review with the organisation. **Disaster recovery tests** • Microsoft conducts disaster recovery tests at least once per year.

REF.	QUESTION / REQUIREMENT	GUIDANCE
90	How frequently does the service provider conduct disaster recovery tests?	Microsoft conducts disaster recovery tests at least once per year. By way of background, Microsoft maintains physical redundancy at the server, datacenter, and service levels; data redundancy with robust failover capabilities; and functional redundancy with offline functionality. Microsoft's redundant storage and its procedures for recovering data are designed to attempt to reconstruct customer data in its original or last-replicated state from before the time it was lost or destroyed. Microsoft maintains multiple live copies of data at all times. Live data is separated into "fault zones," which ensure continuous access to data. For Office 365, Microsoft maintains multiple copies of customer data across datacenters for redundancy. For Azure, Microsoft may copy customer data between regions within a given geography for data redundancy or other operational purposes. For example, Azure Globally-Redundant Storage ("GRS") replicates certain data between two regions within the same geography for enhanced data durability in case of a major datacenter disaster. To promote data resiliency, Microsoft Online Services offer active load balancing, automated failover and human backup, and recovery testing across failure domains. For example, Azure Traffic Manager provides load balancing between different regions, and the customer can use network virtual appliances in its Azure Virtual Networks for application delivery controllers (ADC/load balancing) functionality. Load balancing is also provided by Power BI Services, the Gateway, and Azure API Management roles. Office 365 services have been designed around specific resiliency principles that are designed to protect data from corruption, to separate data into different fault zones, to monitor data for failing any part of the ACID test, and to allow customers to recover on their own. For more information, refer to Microsoft's white paper "Data Resiliency in Microsoft Office 365," available at https://aka.ms/Office365DR.

REF.	QUESTION / REQUIREMENT	GUIDANCE
	F. PRIVACY	
	In addition to the sector-specific requirements imposed by the regulator, the financial institution also needs to comply with the General Data Protection Regulation (2016/679), GDPR, and the national implementing laws in respect of any personal information that Microsoft hosts for the financial institution in the course of providing the Microsoft cloud services.	
91	Will the use of the cloud service enable the institution to continue complying with local privacy law?	Microsoft is committed to protect the privacy of its customers and is constantly working to help strengthen privacy and compliance protections for its customers. Not only does Microsoft have robust and industry leading security practices in place to protect its customers' data and robust data protection clauses included, as standard, in its online service terms, Microsoft has gone further. Notably, Microsoft has taken two important and industry first steps to prove its commitment to privacy. First, in April 2014, the EU's data protection authorities acted through their "Article 29 Working Party" to approve that Microsoft's contractual commitments meet the requirements of the EU's "model clauses". Europe's privacy regulators have said, in effect, that personal data stored in Microsoft's enterprise cloud is subject to Europe's rigorous privacy standards no matter where that data is located. Second, in February 2015, Microsoft became the first major cloud provider to adopt the world's first international standard for cloud privacy, ISO/IEC 27018. The standard was developed by the International Organization for Standardization (ISO) to establish a uniform, international approach to protecting privacy for personal data stored in the cloud. Finally, Microsoft is committed to GDPR compliance across its cloud services and provides GDPR related assurances in its contractual commitments. Following the European Data Protection Board's (EDPB) recommendations on measures that companies should implement as a result of the Schrems II decision, Microsoft announced its Defending Your Data initiative, which extends beyond the EDPB's recommendations. We have also launched the Tech Fit for Europe initiative to develop digital solutions based on European values and rules.

Part 2: Contract Checklist

WHAT ARE OUR CONTRACT DOCUMENTS?

The following table sets out the relevant Microsoft documents:

CORE MICROSOFT CONTRACT DOCUMENTS	DOCUMENTS INCORPORATED IN MICROSOFT CONTRACTS[1]
Microsoft Business and Services Agreement (MBSA); Enterprise Agreement (EA); and the enabling Enrollment, which is likely to be either an Enterprise Enrollment or a Server and Cloud Enrollment.	The Data Protection (DPA); Product Terms; Online Services Service Level Agreement (SLA).
AMENDMENT PROVIDED BY MICROSOFT TO ADD TO CORE CONTRACT DOCUMENTS FOR FINANCIAL SERVICES CUSTOMERS	**SUPPORTING DOCUMENTS AND INFORMATION THAT DO NOT FORM PART OF THE CONTRACT[2]**
Financial Services Amendment	Materials available from the relevant Trust Center.

WHAT DOES THIS PART 2 COVER?

The Circular provides that, at a minimum, your agreement with the cloud services provider must address specified matters. This Part 2 sets out those specific items that must be addressed in your agreement as well as other provisions that customers and regulators in other jurisdictions generally expect to be addressed. The third column indicates how and where in the Microsoft contractual documents the requirement is covered. All regulatory references are to the Circular unless indicated otherwise.

[1] Available at www.microsoft.com/contracts.

[2] Available at www.microsoft.com/trustcenter.

REFERENCE	REQUIREMENT	HOW AND WHERE IS THIS DEALT WITH IN MICROSOFT'S CONTRACT?
Point 77(a) and (i)	(a) The scope of the arrangement and the expected level of services to be supplied qualitatively and quantitatively	The contract pack comprehensively sets out the scope of the arrangement and the respective commitments of the parties. The online services are ordered under the EA Enrollment, and the order will set out the online services and relevant prices. Microsoft enters into agreements with each of its financial institution customers for Online Services, which includes a Financial Services Amendment, the Online Services Terms, and the Service Level Agreement. The agreements clearly define the Online Services to be provided. The services are broadly described, along with the applicable usage rights, in the Product Terms and the Product Terms, particularly in the Product Terms "Core Features" commitments.
Point 76 and 77(a)	(b) Clear description of • the outsourced function; • the roles and responsibilities, rights and obligations of all the parties in the outsourcing chain	Microsoft enters into agreements with each of its financial institution customers for Online Services, which includes a Financial Services Amendment, the Online Services Terms, and the Service Level Agreement. The agreements clearly define the Online Services to be provided. The contract pack comprehensively sets out the scope of the arrangement and the respective commitments of the parties.
Point 77(h)	(c) Right to monitor the service provider's Performance on an ongoing basis	The customer may monitor the performance of the Online Services via the administrative dashboard at any time, which includes information as to Microsoft's compliance with its SLA commitments.

REFERENCE	REQUIREMENT	HOW AND WHERE IS THIS DEALT WITH IN MICROSOFT'S CONTRACT?
Point 77(p) and 88 to 89 (continued)	(d) Inspection and audit rights including: • guaranteed access by the internal audit function, statutory auditor and CSSF to the information relating to the outsourced functions including relevant data kept by the service provider, (in the cases provided for in the applicable national law) the power to perform on-site inspection of the service provider; • the right of the internal control functions to have access to any documentation relating to the outsourced function, at any time and without difficulty, to maintain these function's continued ability to exercise their controls; and • a reference to the information gathering and investigatory powers of competent authorities under Articles 49, 53 and 59 LFS[1], Articles 31, 38 and 58-5 LPS[1] and, where applicable, resolution authorities under Article 61(1) BRRD Law[1].	The DPA specifies the audit and monitoring mechanisms that Microsoft puts in place to verify that the Online Services meet appropriate security and compliance standards. Rigorous third-party audits validate the adherence of Microsoft Online Services to these strict requirements. Upon request, Microsoft will provide each Microsoft audit report to a customer to verify Microsoft's compliance with the security obligations under the DPA. Microsoft also conducts regular penetration testing to increase the level of detection and protection throughout the Microsoft cloud. Microsoft makes available to customers penetration testing and other audits of its cybersecurity practices, and customers also may conduct their own penetration testing of the services. This is done in accordance with Microsoft's rules of engagement, which do not require Microsoft's permission in advance of such testing. For more information regarding penetration testing, see https://technet.microsoft.com/en-us/mt784683.aspx. Microsoft makes available certain tools through the Service Trust Platform to enable customers to conduct their own virtual audits of the Online Services. Microsoft also provides customers with information to reconstruct financial transactions and develop audit trail information through two primary sources: Azure Active Directory reporting, which is a repository of audit logs and other information that can be retrieved to determine who has accessed customer transaction information and the actions they have taken with respect to such information, and Azure Monitor, which provides activity logs and diagnostic logs that can be used to determine the "what, who, and when" with respect to changes to customer cloud information and to obtain information about the operation of the Online Services, respectively. In addition, the Financial Services Amendment details the examination and audit rights that are granted to the customer and the regulator. The "Regulator Right to Examine" sets out a process which can culminate in the regulator's examination of Microsoft's premises. To enable the customer to meet its examination, oversight and control, and audit requirements, Microsoft has developed specific rights and processes that provide the customer with access to information, Microsoft personnel and Microsoft's external auditors. Microsoft will provide the customer with the following rights:

Continued Next Page »

REFERENCE	REQUIREMENT	HOW AND WHERE IS THIS DEALT WITH IN MICROSOFT'S CONTRACT?
Point 77(p) and 88 to 89		1. Online Services Information Policy Microsoft makes each Information Security Policy available to the customer, along with descriptions of the security controls in place for the applicable Online Service and other information reasonably requested by the customer regarding Microsoft security practices and policies. 2. Audits of Online Services On behalf of the customer, Microsoft will cause the performance of audits of the security of the computers, computing environment and physical datacenters that it uses in processing customer data for each Online Service. Pursuant to the terms in the OST, Microsoft will provide Customer with each Microsoft Audit Report. 3. Financial Services Compliance Program The customer also has the opportunity to participate in the Financial Services Compliance Program, which is a for-fee program that facilitates the customer's ability to audit Microsoft, including: (a) assess the services' controls and effectiveness, (b) access data related to service operations, (c) maintain insight into operational risks of the services, (d) be provided with notification of changes that may materially impact Microsoft's ability to provide the services, and (e) provide feedback on areas for improvement in the services.
Point 96(g) and (h)	(e) Where the financial institution use third-party certifications and third-party or internal audit reports made available by the service provider, the right for the financial institution to • to request the expansion of scope of the certifications or audit reports to other relevant systems and controls, the number and frequency of such requests for scope modification should be reasonable and legitimate from a risk management perspective; • to perform individual audits at its discretion with regard to the outsourcing of critical or important functions.	Microsoft makes available certain tools through the Service Trust Platform to enable customers to conduct their own virtual audits of the Online Services. See as well the Financial Services Amendment which details the examination and audit rights that are granted to the customer and the regulator.

REFERENCE	REQUIREMENT	HOW AND WHERE IS THIS DEALT WITH IN MICROSOFT'S CONTRACT?
Point 77(p) and 90	(f) Inspection and audit rights with regard to the outsourcing of critical or important functions, granting the financial institution, its statutory auditor, the CSSF, where applicable the resolution authority and any other person appointed by the financial institution, CSSF or resolution authority: • full access to all relevant business premises, including the full range of relevant devices, systems, networks, information and data used for providing the outsourced function, including related financial information, personnel and the service provider's external auditors ('access and information rights'); and • unrestricted rights of inspection and auditing related to the outsourcing arrangement ('audit rights'), including the possibility for the CSSF to communicate any observations made in this context to the financial institution, to enable them to monitor the outsourcing arrangement and ensure compliance with the applicable regulatory and contractual requirements.	The Financial Services Amendment details the examination and audit rights that are granted to the customer and the regulator. The "Regulator Right to Examine" sets out a process which can culminate in the regulator's examination of Microsoft's premises. To enable the customer to meet its examination, oversight and control, and audit requirements, Microsoft has developed specific rights and processes that provide the customer with access to information, Microsoft personnel and Microsoft's external auditors. Microsoft will provide the customer with the following rights: 1. Online Services Information Policy Microsoft makes each Information Security Policy available to the customer, along with descriptions of the security controls in place for the applicable Online Service and other information reasonably requested by the customer regarding Microsoft security practices and policies. 2. Audits of Online Services On behalf of the customer, Microsoft will cause the performance of audits of the security of the computers, computing environment and physical datacenters that it uses in processing customer data for each Online Service. Pursuant to the terms in the OST, Microsoft will provide Customer with each Microsoft Audit Report. 3. Financial Services Compliance Program The customer also has the opportunity to participate in the Financial Services Compliance Program, which is a for-fee program that facilitates the customer's ability to audit Microsoft, including: (a) assess the services' controls and effectiveness, (b) access data related to service operations, (c) maintain insight into operational risks of the services, (d) be provided with notification of changes that may materially impact Microsoft's ability to provide the services, and (e) provide feedback on areas for improvement in the services. Pursuant to the Financial Services Amendment, Microsoft provides the regulator with a direct right to examine the Online Services, including the ability to conduct an on-premise examination, to meet with Microsoft personnel and Microsoft's external auditors, and to access any related information, records, reports and documents, in the event that the regulator requests to examine the Online Services operations in order to meet their supervisory obligations.

REFERENCE	REQUIREMENT	HOW AND WHERE IS THIS DEALT WITH IN MICROSOFT'S CONTRACT?
Point 77(n)	(g) Cooperation obligation with the competent authorities and, where applicable, resolution authorities, including other persons appointed by them.	Pursuant to the Financial Services Amendment, Microsoft provides the regulator with a direct right to examine the Online Services, including the ability to conduct an on-premise examination, to meet with Microsoft personnel and Microsoft's external auditors, and to access any related information, records, reports and documents, in the event that the regulator requests to examine the Online Services operations in order to meet their supervisory obligations.
Point 77(o)	(h) For BRRD institutions, the national resolution authority's powers, especially to Articles 59-47, 66 and 69 of the BRRD Law[11], and the 'substantive obligations'[12] of the contract in the sense of the Articles 59-47 and 66 of the BRRD Law?	See section 6 and 7 of the Financial Services Amendment containing rights and commitments related to termination and continuity after termination.
Point 77(f)	(i) To the extent applicable, offshoring arrangements (including through subcontracting), including the location(s) (i.e. regions or countries) where the function will be provided and/or where relevant data will be kept and processed and, a requirement to notify the financial institution if the service provider proposes to change the location(s).	The DPA provides commitments on the location at which Microsoft will store customer data at rest (see OST, page 11). Microsoft also makes GDPR specific commitments (Attachment 4, OST) to all customers effective May 25, 2018.

[11]Law of 18 December 2015 on the resolution, reorganisation and winding up measures of credit institutions and certain investment firms and on deposit guarantee and investor compensation schemes, as amended.
[12] At least any payment or delivery obligation and the provision of collateral are deemed to be 'substantive obligations'.

REFERENCE	REQUIREMENT	HOW AND WHERE IS THIS DEALT WITH IN MICROSOFT'S CONTRACT?
Point 143(b)	(j) Resiliency requirement: in case of spread of processing, data, systems over different datacenters worldwide, at least one of the datacenters shall be located within the EEA.	The DPA provides commitments on the location(s) at which Microsoft will store customer data at rest, including those for back-up purposes (see OST) and can be restricted to the EU. Please note that where only non-critical/important functions are outsourced to a cloud computing infrastructure and in accordance with their risk analysis, financial institutions may justify not applying the requirements of the Circular relating to resiliency and may request a specific derogation in this respect, as part of its notification, from the CSSF.
	(k) Appropriate clauses in case the service provider is the resource operator so that the financial institution may control the outsourcing chain.	Microsoft does not act as the "resource operator".
	(l) Provision for appropriate means of contact, at the service provider.	The DPA provides a section on how to contact Microsoft (see OST).
Point 77(c) and 143(a)	(m) Applicable law, i.e. the law of one of the EEA countries unless a derogation has been granted by the CSSF or the outsourcing agreement is signed as a group contract.	The agreements are governed by Irish law. Please note that where only non-critical/important functions are outsourced to a cloud computing infrastructure and in accordance with their risk analysis, financial institutions may justify not applying the requirements of the Circular relating to the applicable law and may request a specific derogation in this respect, as part of its notification, from the CSSF.

REFERENCE	REQUIREMENT	HOW AND WHERE IS THIS DEALT WITH IN MICROSOFT'S CONTRACT?
Point 77(b)	(n) Commencement and end date and the notice periods.	Standard EA Enrollments have a three-year term and may be renewed for a further three-year term.
	(o) Review provisions enabling changes to existing processes and to accommodate new processes in the future to meet changing circumstances.	The customer may monitor the performance of the Online Services via the administrative dashboard, which includes information as to Microsoft compliance with its SLA commitments. The DPA (at OST pages 10-14) specifies the control standards and frameworks that Microsoft will comply with for each Online Service. The DPA also provides for independent audits of compliance of those Online Services, Microsoft remediation of issues raised by the audits and availability to customers of the audit reports and Microsoft information security policies. The customer can always order additional services if required. The customer may terminate an Online Service at the express direction of a regulator with reasonable notice. Additionally, to ensure regulatory compliance, Microsoft and the customer may contemplate adding additional products or services, or if these are unable to satisfy the customer's new regulatory requirements, the customer may terminate the applicable Online Service without cause by giving 60 days' prior written notice.
Point 77(d)	(p) The parties' financial obligations (pricing and fee structure).	The pricing for the online services is specified in the Customer Price Sheet and each customer's order. In general, the customer is required by the EA to commit to annual payments (payable in advance) based upon the customer's number of users.
Point 77(i)	(q) Service levels and performance requirements	The SLA sets outs Microsoft's service level commitments for online services, as well as the service credit remedies for the customer if Microsoft does not meet the commitment. The SLA is fixed for the initial term of the Enrollment: *"We will not modify the terms of your SLA during the initial term of your subscription; however, if you renew your subscription, then the version of this SLA that is current at the time of renewal will apply for your renewal term."* For information regarding uptime for each Online Service, refer to the Service Level Agreement for Microsoft Online Services.

REFERENCE	REQUIREMENT	HOW AND WHERE IS THIS DEALT WITH IN MICROSOFT'S CONTRACT?
	(r) The form in which data is to be kept and clear provisions identifying ownership and control of data. In the event of termination, transitional arrangements should address access to, and ownership of, documents, records, software and hardware, and the role of the service provider in transitioning the service. (continued)	The customer will have the ability to access and extract its Customer Data stored in each Online Service at all times during the subscription and for a retention period of at least 90 days after it ends (see OST, page 5). Microsoft also makes specific commitments with respect to customer data in the OST. In summary, Microsoft commits that: 1. Ownership of customer data remains at all times with the customer (see OST, page 7). 2. Customer data will only be used to provide the online services to the customer. Customer data will not be used for any other purposes, including for advertising or other commercial purposes (see OST, page 7). 3. Microsoft will not disclose customer data to law enforcement unless it is legally obliged to do so, and only after not being able to redirect the request to the customer (see OST, page 7). 4. Microsoft will implement and maintain appropriate technical and organisational measures, internal controls, and information security routines intended to protect customer data against accidental, unauthorised or unlawful access, disclosure, alteration, loss, or destruction (see OST, page 8 and pages 10-14 for more details). 5. Microsoft will notify the customer if it becomes aware of any security incident, and will take reasonable steps to mitigate the effects and minimise the damage resulting from the security incident (see OST, pages 8 and 12-13). MBSA section 3 deals with confidentiality. Under this section Microsoft commits not to disclose confidential information (which includes customer data) to third parties (unless required by law) and to only use confidential information for the purposes of Microsoft's business relationship with the customer. If there is a breach of the contractual confidentiality obligations by Microsoft, the customer would be able to bring a claim for breach of contract against Microsoft. Continued Next Page »

REFERENCE	REQUIREMENT	HOW AND WHERE IS THIS DEALT WITH IN MICROSOFT'S CONTRACT?
	(r) The form in which data is to be kept and clear provisions identifying ownership and control of data. In the event of termination, transitional arrangements should address access to, and ownership of, documents, records, software and hardware, and the role of the service provider in transitioning the service.	Upon expiration or termination, the customer can extract its data. As set out in the OST, Microsoft will retain customer data stored in the Online Service in a limited function account for 90 days after expiration or termination of the customer's subscription so that the customer may extract the data. After the 90-day retention period ends, Microsoft will disable the customer's account and delete the customer data. Microsoft will disable the account and delete customer data from the account no more than 180 days after expiration or termination of customer's use of an Online Service. Ownership of documents, records and other data remains with the customer and at no point transfer to Microsoft or anyone else, so this does not need to be addressed through transition. Being a cloud services solution, ownership of software and hardware used to provide the service remains with Microsoft.
Point 77(m)	(s) Access of data owned by the financial institution in the case of the insolvency, resolution or discontinuation of business operations of the service provider	(see the Financial Services Amendment page 5-7).
Point 77(j)	(t) Reporting requirements, including (i) the communication by the service provider of any development that may have a material impact on the service provider's ability to effectively carry out the function in line with the agreed service levels and in compliance with applicable laws and regulatory requirements, (ii) the obligation to report any significant problem having an impact on the outsourced functions as well as any emergency situation and, where appropriate, (iii) the obligation to submit reports of the internal audit function of the service provider	The customer may monitor the performance of the Online Services via the administrative dashboard at any time, which includes information as to Microsoft's compliance with its SLA commitments. Microsoft also commits to providing the customer with Microsoft's audit reports, resulting from audits performed by a qualified, independent, third-party security auditor that measures compliance against Microsoft's standards certifications (see DPA, pages 9 and the Financial Services Amendment page 2-3). See the DPA page 9.

REFERENCE	REQUIREMENT	HOW AND WHERE IS THIS DEALT WITH IN MICROSOFT'S CONTRACT?
Point 142(c)	(u) Notification of change in the application functionality prior to implementation.	Yes, Microsoft informs customers through a portal about upcoming changes in its products. For example, see for O365: https://www.microsoft.com/fr-be/microsoft-365/roadmap?rtc=2&filters= Or for Azure see: https://azure.microsoft.com/en-us/updates/ where customers can subscribe to notifications to stay informed.
Point 50 and 77(l)	(v) Business continuity management, including specifying measures for redundancy and backup of the systems and data	Business Continuity Management forms part of the scope of the accreditation that Microsoft maintains in relation to the online services, and Microsoft commits to maintain specified business continuity management practices (see the Financial Services Amendment page 5-7). Business continuity management also forms part of the scope of Microsoft's industry standards compliance commitments and regular third-party compliance audits.
Point 77(g), 85 and 87	(w) Accessibility, availability, integrity, confidentiality, privacy and security of information and, the service provider's obligation to protect confidential, personal or otherwise sensitive information and to comply with all legal requirement regarding the protection of data that apply to the financial institution (e.g. personal data protection and bank secrecy) (continued)	The contractual documents include various confidentiality, privacy and security protections: • Microsoft will deal with customer data in accordance with the OST and makes various commitments in this respect. • Microsoft commits to reimburse customer mitigation costs incurred as a consequence of a security incident involving customer data (see Financial Services Amendment, page 5 and OST, page 8 for the details of this commitment). The OST states that Microsoft and the customer each commit to comply with all applicable privacy and data protection laws and regulations. The customer owns its data that is stored on Microsoft cloud services at all times. The customer also retains the ability to access its customer data at all times, and Microsoft will deal with customer data in accordance with the terms and conditions of the Enrollment and the OST. Microsoft will retain customer data stored in the Online Service in a limited function account for 90 days after expiration or termination of customer's subscription so that the customer

Continued Next Page »

REFERENCE	REQUIREMENT	HOW AND WHERE IS THIS DEALT WITH IN MICROSOFT'S CONTRACT?
Point 77(g), 85 and 87	(w) Accessibility, availability, integrity, confidentiality, privacy and security of information and, the service provider's obligation to protect confidential, personal or otherwise sensitive information and to comply with all legal requirement regarding the protection of data that apply to the financial institution (e.g. personal data protection and bank secrecy)	customer may extract the data. No more than 180 days after expiration or termination of the customer's use of an Online Service, Microsoft will disable the account and delete customer data from the account. Microsoft makes specific commitments with respect to safeguarding your data in the OST. In summary, Microsoft commits that: 6. Your data will only be used to provide the online services to you and your data will not be used for any other purposes, including for advertising or similar commercial purposes. (OST, page 7) 7. Microsoft will not disclose your data to law enforcement unless required by law. If law enforcement contacts Microsoft with a demand for your data, Microsoft will attempt to redirect the law enforcement agency to request that data directly from you. (OST, page 7) 8. Microsoft has implemented and will maintain appropriate technical and organizational measures, internal controls, and information security routines intended to protect your data against accidental, unauthorised or unlawful access, disclosure, alteration, loss, or destruction. (OST, page 36) Technical support personnel are only permitted to have access to customer information when needed. (OST, page 13) The OST states the responsibilities of the contracting parties that ensure the effectiveness of security policies. To the extent that a security incident results from Microsoft's failure to comply with its contractual obligations, and subject to the applicable limitations of liability, Microsoft reimburses you for reasonable and third-party validated, out-of-pocket remediation costs you incurred in connection with the security incident, including actual costs of court- or governmental body-imposed payments, fines or penalties for a Microsoft-caused security incident and additional, commercially-reasonable, out-of-pocket expenses you incurred to manage or remedy the Microsoft-caused security incident (FSA, Section 3). Applicable limitation of liability provisions can be found in the MBSA. Microsoft further agrees to notify you if it becomes aware of any security incident, and to take reasonable steps to mitigate the effects and minimise the damage resulting from the security incident (OST).

REFERENCE	REQUIREMENT	HOW AND WHERE IS THIS DEALT WITH IN MICROSOFT'S CONTRACT?
Point 77(e) and 78 to 82	(x) whether sub-outsourcing, in particular of critical or important functions or parts thereof, is permitted? If sub-outsourcing of critical or important functions is permitted: excluded activities; • conditions to be complied with; • obligation for the service provider to ensure compliance with contractual obligations in respect of the financial institution; • prior specific or general written authorisation from the financial institution before sub-outsourcing data; • service provider's obligation to inform the financial institution of any planned sub-outsourcing, or material changes thereof (changes of sub-contractors and notification period); • financial institution's explicit approval of or, right to object to intended sub-outsourcing or material changes thereof; and (y) financial institution's right to terminate the agreement in case of undue sub-outsourcing, e.g. in case of sub-outsourcing without notification of material risk increase.	Microsoft commits that its subcontractors will be permitted to obtain customer data only to deliver the services Microsoft has retained them to provide and will be prohibited from using customer data for any other purpose. Microsoft remains responsible for its subcontractors' compliance with these restrictions. To ensure subcontractor accountability, Microsoft requires all of its vendors that handle customer personal information to join the Microsoft Supplier Security and Privacy Assurance Program, which is an initiative designed to standardise and strengthen the handling of customer personal information, and to bring vendor business processes and systems into compliance with those of Microsoft. For more information regarding Microsoft's Supplier Security and Privacy Program, see microsoft.com/en-us/procurement/msp-requirements.aspx. Microsoft will enter into a written agreement with any subcontractor to which Microsoft transfers customer data that is no less protective than the data processing terms in the customer's contracts with Microsoft (DPA, see OST, page 11). In addition, Microsoft's ISO/IEC 27018 certification requires Microsoft to ensure that its subcontractors are subject to the same security controls as Microsoft. Microsoft's ISO 27001 certification provides a layer of additional controls that impose stringent requirements on Microsoft's subcontractors to comply fully with Microsoft's privacy, security, and other commitments to its customers, including requirements for handling sensitive data, background checks, and non-disclosure agreements. Microsoft provides a website that lists subcontractors authorised to access customer data in the Online Services as well as the limited or ancillary services they provide. At least 6 months before authorising any new subcontractor to access Customer Data, Microsoft will update the website and provide the customer with a mechanism to obtain notice of that update. If the customer does not approve of a new subcontractor, then the customer may terminate the affected Online Service without penalty by providing, before the end of the notice period, written notice of termination that includes an explanation of the grounds for non-approval. If the affected cloud computing service is part of a suite (or similar single purchase of services), then any termination will apply to the entire suite. After termination, Microsoft will remove payment obligations for the terminated Online Services from subsequent customer invoices. (DPA, see OST, page 11).

REFERENCE	REQUIREMENT	HOW AND WHERE IS THIS DEALT WITH IN MICROSOFT'S CONTRACT?
	(z) Liability and indemnity	MBSA clause 7 deals with liability. MBSA clause 6 sets out Microsoft's obligation to defend the regulated entity against third party infringement claims.
Point 77(k)	(aa) Insurance	Microsoft maintains self-insurance arrangements for most of the areas where third party insurance is typically obtained and can make certificates of insurance available upon request. Microsoft has taken the commercial decision to take this approach, and considers that this does not detrimentally affect its customers, given Microsoft's financial position set out in Microsoft's Annual Reports (see Part 1, Question 1 above).
Point 77(q)	(bb) Default arrangements and termination provisions, including termination rights?	Microsoft agreements are usually subject to terms of 12-36 months, which may be extended at the customer's election. They also include rights to terminate early for cause and without cause.
Point 77(q) and 101	(cc) Termination right for the financial institution in the following situations: • where the provider is in breach of applicable law, regulations or contractual provisions; • where impediments capable of altering the performance of the outsourced function are identified; • where there are material changes affecting the outsourcing arrangement or the service provider (e.g. sub-outsourcing or changes of sub-contractors); (continued)	See the Financial Services Amendment page 4 combined with the termination rights as set out in the Volume Licencing Agreement.

Continued Next Page »

REFERENCE	REQUIREMENT	HOW AND WHERE IS THIS DEALT WITH IN MICROSOFT'S CONTRACT?
Point 77(q) and 101	• where there are weaknesses regarding the management and security of confidential, personal or otherwise sensitive data or information; and • where instructions are given by the regulator, e.g. I the case that the regulator is, caused by the outsourcing arrangement, no longer in a position to effectively supervise the financial institution?	
Point 77(q) and 102	(dd) Transfer facilitation whenever the continuity or quality of the service are likely to be affected, including: • the obligations of the existing service provider in those cases; • appropriate transition period, during which the service provider, after the termination of the outsourcing agreement, would continue to provide the outsourced function to reduce the risk of disruptions; • the obligation of the service provider to support the financial institution in the orderly transfer of the function in the event of the termination of the outsourcing agreement; and (continued)	Microsoft's Financial Services Amendment provides for business continuity and exit provisions, including rights for the customer to obtain exit assistance at market rates from Microsoft Consulting Services. Customers should work with Microsoft to build such business continuity and exit plans. Microsoft's flexibility in offering hybrid solutions further facilitate transition from cloud to on-premise solutions more seamlessly. Upon expiration or termination, the customer can extract its data. As set out in the OST, Microsoft will retain customer data stored in the Online Service in a limited function account for 90 days after expiration or termination of the customer's subscription so that the customer may extract the data. After the 90-day retention period ends, Microsoft will disable the customer's account and delete the customer data. Microsoft will disable the account and delete customer data from the account no more than 180 days after expiration or termination of customer's use of an Online Service. Ownership of documents, records and other data remains with the customer and at no point transfer to Microsoft or anyone else, so this does not need to be addressed through transition. Being a cloud services solution, ownership of software and hardware used to provide the service remains with Microsoft. See DPA page 10. Continued Next Page »

Back to Contents

REFERENCE	REQUIREMENT	HOW AND WHERE IS THIS DEALT WITH IN MICROSOFT'S CONTRACT?
Point 77(q) and 102	• erasure of the data and systems of the financial institution within a reasonable timeframe (when the contract is terminated).	
	(ee) Dispute resolution arrangements	In the event that a financial institution and Microsoft have a dispute, the choice-of-law and dispute resolution provisions would be clearly described in the agreement between Microsoft and the financial institution. MBSA clauses 10(g) and 10(h) contains terms that describe how a dispute under the contract is to be conducted.

Further Information

- Navigating Your Way to the Cloud: microsoft.com/en-sg/apac/trustedcloud
- Trust Center: microsoft.com/trust
- Service Trust Portal: aka.ms/trustportal
- Customer Stories: customers.microsoft.com
- Product Terms: microsoft.com/contracts
- Service Level Agreements: microsoft.com/contracts
- SAFE Handbook: aka.ms/safehandbook
- A Cloud for Global Good | Microsoft: news.microsoft.com/cloudforgood/