



# Microsoft Cloud Checklist for Financial Institutions in Europe



# Introduction

1. This checklist is aimed at financial institutions in the EU who want to use Microsoft Online Services. We use the term “financial institutions” broadly, to include any entity that is regulated and supervised by an EU regulator. These entities include banks, payment institutions, insure and investment firms.

This checklist focuses on EU-wide guidelines, specifically:

- 1.1 [The EBA guidelines on outsourcing arrangements](#) (dated 25 February 2019),
- 1.2 [The EIOPA cloud outsourcing guidelines](#) (published 31 January 2020),
- 1.3 [The ESMA draft guidelines on outsourcing to cloud service providers](#) (published 3 June 2020),

and not all country-specific regulations.

2. The documents that comprise the Microsoft contract suite for Online Services (the “**Microsoft Agreement**”) will depend on your financial institution and its proposed use of Online Services. However, key Microsoft contractual documents that are relevant to the use of Microsoft Online Services for financial institutions and are therefore referenced in the checklist below include:

- 2.1 The Online Service Terms (“OST”) and Online Services Data Protection Addendum (“DPA”), incorporating data processing terms including the EU Model Clauses<sup>1</sup>;
- 2.2 The Online Services Service Level Agreement (“SLA”)<sup>2</sup>; and
- 2.3 The Financial Services Amendment (“**FS Amendment**”).<sup>3</sup>

3. We also refer in the checklist to supporting documents and information that do not form part of your Microsoft Agreement. These materials can be accessed via the relevant [Trust Center](#) or the [Service Trust Portal](#).
4. Microsoft has created the checklist below to assist you to understand how Microsoft enables your compliance in meeting the key EBA, EIOPA and ESMA requirements applicable to financial institutions for cloud outsourcings. This will also help you to assess Microsoft as an outsourced service provider. The checklist not only focuses on the terms that are required to be included in the written agreement, but also highlights a number of non-contractual requirements and demonstrates how our documentation addresses these. Please note that there are operational and organisational requirements in the EBA, EIOPA and ESMA guidelines that we have not included in the checklist below as these fall entirely within the responsibility scope of financial institutions’ arrangements internally and are not specifically related to outsourcing. Please note that at the time of publication of this paper, the ESMA guidelines were not yet final. Therefore, this checklist is based upon the [ESMA draft guidelines](#) on outsourcing to cloud service providers.
5. While Microsoft provides a range of tools and information for customers and potential customers on its [Trust Center](#), [Service Trust Portal](#) and [CELA Europe page for financial services](#) to support firms through their regulatory due diligence and risk assessments, this checklist is a further tool intended to assist financial institutions interested in using Microsoft Online Services.


---

<sup>1</sup> Available at [www.microsoft.com/contracts](http://www.microsoft.com/contracts). Please note that for the purposes of this paper, we reference the October 2020 version of the OST and the July 2020 version of the DPA.

<sup>2</sup> Available at [www.microsoft.com/contracts](http://www.microsoft.com/contracts). Please note that for the purposes of this paper, we reference the October 2020 version of the SLA.

<sup>3</sup> Please note that for the purposes of this paper, we reference the March 2020 version of the FS Amendment.

# Checklist

Item	Reference	Requirement	MS commentary / How and where is this dealt with in the Microsoft Agreement?	MS Agreement reference
 <b>General</b>				
1.	EBA 74 EIOPA 36 ESMA 39	<p><b>Rights and obligations</b> to be clearly allocated in a written agreement.</p> <p>The agreement for critical or important functions must set out:</p>	The rights and obligations of the parties are set out in the Microsoft Agreement.	N/A
2.	EBA 75(a) EIOPA 37(a) ESMA 41(a)	<p><b>Services:</b> A clear description of the outsourced cloud services and type of support services;</p>	<p>The Online Services are described in the Microsoft Agreement. An online description is also available here:</p> <ul style="list-style-type: none"> <li>• <a href="#">Microsoft 365 Service Description</a></li> <li>• <a href="#">Dynamics 365 Service Description</a></li> <li>• <a href="#">Directory of Azure Cloud Services</a></li> </ul> <p>The support services, including Professional Services, are described in the DPA and in the Master Business Services Agreement.</p>	N/A
3.	EBA 75(b) EIOPA 37(b) ESMA 41(b)	<p><b>Term:</b> Start and end date and notice periods;</p>	<p>Refer to the Microsoft Agreement.</p> <p>In general, standard EA Enrollments have a three-year term and may be renewed for a further three-year term.</p>	N/A

Item	Reference	Requirement	MS commentary / How and where is this dealt with in the Microsoft Agreement?	MS Agreement reference
4.	EBA 75(c) EIOPA 37(c) ESMA 41(c)	<b>Governing Law:</b> Governing law and court jurisdiction;	Refer to the Microsoft Agreement.	N/A
5.	EBA 75(d) EIOPA 37(d) ESMA 41(d)	<b>Fees and Liabilities:</b> The parties' financial obligations;	Refer to the Microsoft Agreement.  In general, the customer is required by the EA to commit to an order for the quantities of services to be used.	N/A
6.	EBA 75(k) EIOPA 37(k) ESMA 41(l)	<b>Insurance:</b> Whether the service provider must take mandatory insurance against certain risks and the level of insurance cover requested.	Microsoft maintains self-insurance arrangements for most of the areas where third party insurance is typically obtained. Copies of certificates of insurance are available upon request.	N/A

## Sub-contracting

7.	EBA 75(e) & 76 EIOPA 37(e) ESMA 41(e)	If the sub-outsourcing of a critical or important function, or material parts thereof, is permitted, the agreement must:	Microsoft's enterprise cloud services processes various categories of data, including customer data and personal data. Where Microsoft hires a subcontractor to perform work that may require access to such data, they are considered a subprocessor.  Subprocessors may access data only to deliver the functions in support of Online Services that Microsoft has hired them to provide and are prohibited from using data for any other purpose.	N/A
8.	EBA 78(a) EIOPA 50(a) ESMA 55(a)	Specify any types of activities that are excluded from sub- outsourcing;	The Microsoft Online Services Subprocessor List identifies subprocessors authorized to subprocess customer data or personal data in Microsoft Online Services. This list is applicable for the Microsoft Online Services referred to in the OST for which Microsoft is a data processor.	


Item	Reference	Requirement	MS commentary / How and where is this dealt with in the Microsoft Agreement?	MS Agreement reference
			<p>For further information, refer to the <a href="#">Trust Center</a> and the <a href="#">Subprocessor and Data Privacy White Paper</a>.</p>	
9.	EBA 78(b) EIOPA 50(b) ESMA 55(b)	Specify the conditions to be complied with in the case of sub-outsourcing;	<p>To enable customers to retain oversight of subprocessors that have access to data, Microsoft will:</p> <ol style="list-style-type: none"> <li>1. Provide information about its subprocessors;</li> <li>2. Provide advance notice of changes to its subprocessors;</li> <li>3. Where necessary to perform an audit, give customers access to the processing systems, facilities and supporting documentation relevant to the processing of data by subprocessors; and</li> <li>4. Give customers the ability to terminate if they have concerns about a new subprocessor.</li> </ol>	<p>OST, page 11</p> <p>DPA, “Notice and Controls on use of Subprocessors”</p> <p>DPA, “Auditing Compliance”</p>
10.	EBA 78(c) & 80 EIOPA 50(c) ESMA 55(c)	<p>Specify that the service provider retains full accountability and oversight for the services sub- outsourced;</p> <p><i>Non-contractual requirement</i></p> <p>Financial institutions must ensure that the service provider appropriately oversees the subcontractor in line with the policy defined by the financial institution.</p>	<p>Microsoft will enter into a written agreement with any subprocessor to which Microsoft transfers data that is no less protective than the data processing terms in the Microsoft Agreement and will oversee the performance of all subcontracted obligations and ensure its subprocessors comply with their contractual obligations.</p> <p>To ensure subprocessor accountability, Microsoft requires all of its vendors that handle customer personal information to join the <a href="#">Microsoft Supplier Security and Privacy Assurance Program</a>, which is an initiative designed to standardise and strengthen the handling of customer information, and to bring vendor business processes and systems into compliance with those of Microsoft.</p>	<p>OST, page 11</p> <p>DPA, “Notice and Controls on use of Subprocessors”</p>
11.	EBA 78(d)	Require the service provider to obtain prior specific or general written authorisation from	Customers consent to the subcontracting by Microsoft of the processing of data by entering into the Microsoft Agreement. If customers have concerns about new	OST, page 11

Item	Reference	Requirement	MS commentary / How and where is this dealt with in the Microsoft Agreement?	MS Agreement reference
		the financial institution before sub-outsourcing data;	subprocessors authorised to access data, they have the ability to terminate the affected Online Service (see rows 13 and 14).	DPA, "Notice and Controls on use of Subprocessors"
<b>12.</b>	EBA 78(e) EIOPA 50(d) ESMA 55(d)	Oblige the service provider to inform the financial institution of any planned sub-outsourcing, or material changes thereof (with sufficient time for the financial institution to carry out a risk assessment and to object);	Microsoft gives customers notice of new subprocessors (by updating the Microsoft Online Services Subprocessor List and providing customers with a mechanism to obtain notice of that update) at least six months in advance of the subprocessor's authorization to perform services that may involve secure access to <a href="#">customer data</a> and at least thirty days in advance of potential access to <a href="#">personal data</a> within Microsoft Online Services. This advance notice enables customers to investigate the subprocessor, perform a risk assessment, and ask questions of Microsoft about the subprocessor engagement.	OST, page 11 DPA, "Notice and Controls on use of Subprocessors"
<b>13.</b>	EBA 78(f) EIOPA 50(e) ESMA 55(e)	Include the right to object to intended sub-outsourcing, or material changes thereof, or that explicit approval is required; and	If a customer does not approve of a new subprocessor notified in advance, then the customer may terminate any subscription for the affected Online Service without penalty by providing, before the end of the relevant notice period, written notice of termination that includes an explanation of the grounds for non-approval.	OST, page 11 DPA, "Notice and Controls on use of Subprocessors"
<b>14.</b>	EBA 78(g) EIOPA 50(e) ESMA 55(f)	Include a contractual right to terminate the agreement in the case of undue sub-outsourcing.		
<b>15.</b>	EBA 79(a)	<i>Non-contractual requirement</i> The subcontractor must agree to comply with all applicable laws, regulatory requirements and contractual obligations.	Subprocessors are required to maintain the confidentiality of data and are contractually obligated to meet strict privacy requirements that are equivalent to or stronger than the contractual commitments Microsoft makes to its customers in the OST. Subprocessors are also required to meet EU General Data Protection Regulation (GDPR) requirements, including those related to implementing appropriate technical and organisational measures to protect personal data.	DPA, "Notice and Controls on use of Subprocessors" DPA, Attachment 2, clause 11(1)

Item	Reference	Requirement	MS commentary / How and where is this dealt with in the Microsoft Agreement?	MS Agreement reference
				DPA, Attachment 3, clause 3
16.	EBA 79(b)	<p><i>Non-contractual requirement</i></p> <p>The subcontractor must agree to grant the financial institution and competent authorities the same contractual rights of access and audit as those granted by the service provider.</p>	<p>Microsoft provides unrestricted audit rights for customers and regulators in its FS Amendment.</p> <p>This includes, as necessary, audit rights of subprocessors that perform and process operations of the Online Service.</p>	<p>FS Amendment, section 3 (Unrestricted Rights of Examination or Audit by Regulator)</p> <p>FS Amendment, section 4 (Unrestricted Rights of Audit by Customer)</p> <p>DPA, "Auditing Compliance" DPA, Attachment 2, clause 8(2)</p>

## Location of performance

17.	EBA 75(f) EIOPA 37(f) ESMA 41(f)	Location(s) where the critical or important function will be provided and/or where relevant data will be kept & processed, and the conditions, including that the service provider will notify the financial institution if it proposes to change the location(s).	Information about the locations of customer data at rest for Core Online Services is available in the OST. Additional information pertaining to the data residency and transfer policies specific to the Online Service is available at the <a href="#">Trust Center</a> . This website lets you validate for each Online Service individually how data is stored and processed by Microsoft.	<p>OST, page 28</p> <p>DPA, "Data Transfers and Location"</p> <p>FS Amendment, section 2(d) (Data Residency and Transfer Policies)</p>
-----	--	--	---	--

Item	Reference	Requirement	MS commentary / How and where is this dealt with in the Microsoft Agreement?	MS Agreement reference
 <b>Security of data and systems</b>				
18.	EBA 75(g) IOPA 37(g) SMA 41(g)	Provisions regarding the accessibility, availability, integrity, privacy and safety of relevant data.  In particular, financial institutions must:	<p>The Microsoft Agreement includes various confidentiality, privacy and security protections.</p> <p>For information about how Microsoft cloud services protect your data, and how you can manage cloud data security and compliance for your organisation, refer to the <a href="#">Service Trust Portal</a> (Data Protection Resources).</p> <p>The customer owns, and retains the ability to access, its data that is stored on Microsoft cloud services at all times. Refer to the <a href="#">Trust Center</a> for further information.</p>	N/A
19.	EBA 81 & 72 EIOPA 47 ESMA 43(h)	Ensure that service providers comply with European and national regulations and appropriate IT security standards;	<p><b>European and national regulations</b></p> <p>Microsoft will comply with all laws and regulations applicable to it in the provision of the Online Services, including security breach notification law and data protection requirements.</p> <p><b>Appropriate IT security standards</b></p> <p>Microsoft has implemented and will maintain appropriate technical and organisational measures, internal controls and information security routines designed to protect data against accidental, unauthorised or unlawful access, disclosure, alteration, loss or destruction.</p> <p>Those measures, which will as a minimum comply with the requirements set forth in ISO 27001, 27002 and 27018, are set out in a Microsoft Security Policy which is provided to customers, along with descriptions of the security controls in place for the Online Services and other information reasonably requested by the customer regarding Microsoft's security practices and policies.</p>	OST, pages 5 & 28 DPA, "Compliance with Laws" & "Data Security" DPA, Appendix A



Item	Reference	Requirement	MS commentary / How and where is this dealt with in the Microsoft Agreement?	MS Agreement reference
			<p>Refer to the information provided via the <a href="#">Service Trust Portal</a> (Data Protection Resources).</p> <p>In addition, each Core Online Service also complies with the control standards and frameworks as set out in the OST and implements and maintains the security measures set out in Appendix A of the DPA for the protection of customer data.</p> <p>Many of our services also meet additional certifications and security standards. This information is available via our <a href="#">Trust Centre</a> and our <a href="#">Service Trust Portal</a>.</p>	
20.	EBA 82 & 94 EIOPA 48 & 49 ESMA 41(k) & 43	<p>Define data and system security requirements and monitor compliance with these requirements on an ongoing basis.</p> <p>There should be clear allocation of information security roles and responsibilities between the financial institution and the service provider and a well- documented incident management process.</p> <p>Where relevant, financial institutions should ensure that they are able to carry out security penetration testing.</p>	<p><b>Data and system security requirements</b></p> <p>Microsoft provides detailed information to customers about its security practices so that customers can carry out their risk assessment. Refer to:</p> <ul style="list-style-type: none"> <li>the <a href="#">Service Trust Portal</a> (Data Protection Resources);</li> <li>Microsoft’s <a href="#">Security Documentation</a>;</li> <li>Microsoft’s <a href="#">Penetration Testing Rules of Engagement</a>;</li> <li>the <a href="#">Microsoft Online Services Bounty Program</a>; and</li> <li>downloadable audit reports available on the <a href="#">Service Trust Portal</a>, for the latest privacy, security, and compliance- related information for Microsoft’s cloud services.</li> </ul> <p><b>Roles and responsibilities</b></p> <p>Refer to the Microsoft Agreement which sets out the roles and responsibilities of the parties with regards to ensuring the effectiveness of security policies. Microsoft’s incident management process is described in the DPA and the FS Amendment.</p>	<p>DPA, “Data Security” &amp; “Security Incident Notification”</p> <p>FS Amendment, section 6 (Security Incident: Limited Reimbursement for Certain Costs)</p>

Item	Reference	Requirement	MS commentary / How and where is this dealt with in the Microsoft Agreement?	MS Agreement reference
21.	EBA 40(d), 40(g), 72 & 84 ESMA 42	Ensure that the service provider protects confidential, personal or otherwise sensitive information and complies with all legal requirements regarding the protection of data that apply to the financial institution.	<p>Microsoft will comply with all privacy and data protection laws applicable to it in the provision of the Online Services. For information on how Microsoft handles your data in the cloud, refer to the <a href="#">Subprocessor and Data Privacy White Paper</a>.</p> <p>Microsoft will not disclose confidential information (which includes customer data) to third parties (unless required by law) and will only use confidential information for the purposes of Microsoft’s business relationship with the customer.</p> <p>In addition, Microsoft will ensure that its personnel engaged in the processing of customer and personal data will be obliged to maintain the confidentiality and security of such data even after their engagement ends.</p>	OST, page 5  DPA, “Compliance with Laws” & “Processor Confidentiality Commitment”

## Monitoring and oversight

22.	EBA 75(h), 100 & 104  EIOPA 37(h) ESMA 41(h)	<p>The right of the financial institution to monitor the service provider’s performance on a regular basis.</p> <p><i>Non-contractual requirement</i></p> <p>Financial institutions should receive appropriate reports from service providers and evaluate performance using tools such as key performance indicators, key control indicators, service delivery reports, self-certification and independent reviews.</p>	<p>Customers can monitor Microsoft’s performance of the Online Services (including the SLA commitments) on a regular basis using the functionality of the Online Services.</p> <p>For example, Microsoft’s “service health” dashboards (<a href="#">Office 365 Service Health Dashboard</a> and <a href="#">Azure Status Dashboard</a>) provide 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. Refer to the <a href="#">Service Health and Continuity</a> section of the Microsoft 365 and Office 365 platform service description.</p> <p>Customers may also sign up for <a href="#">Premier Support</a>, in which a designated Technical Account Manager serves as a point of contact for day-to-day management of the Online Services and the customer’s overall relationship with Microsoft.</p>	DPA, “Auditing Compliance”  FS Amendment, section 2(b) (Audits of Online Services by Microsoft)
-----	--	--	---	---

Item	Reference	Requirement	MS commentary / How and where is this dealt with in the Microsoft Agreement?	MS Agreement reference
			<p>Customers have various rights to receive information and reports, examine, monitor and audit Microsoft Online Services. See rows 24 and 29-33.</p> <p>In addition, as part of its certification requirements, Microsoft is required to undergo independent third party auditing and customers have access to those reports. These are available via the <a href="#">Service Trust Portal</a>.</p>	



## Service levels and corrective action

23.	EBA 75(i) EIOPA 37(i) ESMA 41(i)	Agreed service levels, including precise quantitative and qualitative performance targets to allow for timely monitoring so that appropriate corrective action can be taken without undue delay if the agreed service levels are not met.	<p>The SLA sets out 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.</p> <p><b>Refer to:</b></p> <ul style="list-style-type: none"> <li>• <a href="#">Microsoft 365 Service Level Agreement</a></li> <li>• <a href="#">Dynamics 365 Service Level Agreement</a></li> <li>• <a href="#">Azure Service Level Agreements</a></li> </ul>	SLA
-----	--	---	---	-----



## Reporting



24.	EBA 40(e), 59 & 75(j) EIOPA 37(j) ESMA 41(j)	Reporting obligations, including the communication of developments that may materially impact the service provider's ability to effectively carry out the critical or important function in line with the agreed service levels and in compliance with	<p><b>Notification of significant events</b></p> <p>Microsoft will notify the customer of the nature, common causes and resolution of security incidents and other circumstances that can reasonably be expected to have a material service impact on the customer's use of the Online Services, and will provide communications regarding Microsoft's risk-threat evaluations and other circumstances that may have a serious impact.</p>	<p>DPA, "Auditing Compliance"</p> <p>FS Amendment, section 2(e) (Significant Events)</p>
-----	--	--	--	--


Item	Reference	Requirement	MS commentary / How and where is this dealt with in the Microsoft Agreement?	MS Agreement reference
		<p>applicable laws and, as appropriate, obligations to submit reports of the service provider's internal audit function.</p> <p><i>Non-contractual requirement</i></p> <p>Financial institutions must ensure an appropriate flow of information with service providers is maintained.</p>	<p>This is in addition to the various monitoring and reporting features already provided (see rows 22 and 25).</p> <p><b>Internal reports</b></p> <p>Microsoft commissions independent audits of the security of the computers, computing environment and physical data centres that it uses in processing customer/ personal data for each Online Service, the reports of which are available to customers on request.</p> <p>Customers also have access to the results of Microsoft's penetration testing.</p>	<p>FS Amendment, section 2(b) (Audits of Online Services by Microsoft)</p>




## Business continuity

25.	<p>EBA 48, 49 75(l) &amp; 104(c) EIOPA 37(l) ESMA 41(m)</p>	<p>Requirements to implement and test business contingency plans.</p> <p>The financial institution must be able to factor in relevant steps to its own business continuity planning and continuous operation of its business.</p> <p><i>Non-contractual requirement:</i></p> <p>Financial institutions must review the reports that they receive on business continuity measures and testing.</p>	<p>Microsoft has and will maintain adequate business continuity and disaster recovery plans intended to restore normal operations and proper provision of the Online Services in the event of an emergency. Such plans are documented, reviewed and tested at least annually. Microsoft will communicate with customers regarding significant changes to Microsoft's business resumption and contingency plans.</p> <p>For further information about Microsoft's approach to business continuity and disaster recovery, refer to our <a href="#">Enterprise Business Continuity Management (EBCM) Program description</a>. We continually publish validation reports on our EBCM on a quarterly basis on our <a href="#">website</a>.</p>	<p>DPA, Appendix A</p> <p>FS Amendment, sections 2(e) (Significant Events) &amp; 8(e) (Microsoft's Business Continuity and Disaster Recovery Plans)</p>
-----	---	---	---	---

Item	Reference	Requirement	MS commentary / How and where is this dealt with in the Microsoft Agreement?	MS Agreement reference
 <b>Data access</b>				
26.	EBA 75(m) EIOPA 37(n) ESMA 41(o)	The financial institution's data must be accessible in the case of the insolvency, resolution or discontinuation of business operations of the service provider.	See row 41. Customers will at all times have access to customer data using the standard features of the Online Services, including in the case of the insolvency, resolution or discontinuation of business operations of Microsoft where the Data Retention and Deletion provisions in the OST will apply.	OST  DPA, "Data retention and deletion"
 <b>Regulator cooperation</b>				
27.	EBA 75(n) & 86	The service provider must cooperate with the competent authorities and resolution authorities of the financial institution, including other persons appointed by them.	The FS Amendment details the parties' acknowledgment of the relevant regulators' and resolution authorities' information gathering and investigatory powers under applicable laws and that nothing in the FS Amendment will limit or restrict such powers. See also rows 29 and 32.	FS Amendment, section 3 (Unrestricted Rights of Examination or Audit by Regulator)  FS Amendment, section 8 (Business Continuity of Online Services)
28.	EBA 75(o)	For banks and certain investment firms, clear reference to the national resolution authority's powers (BoE in the UK) under BRRD.	Upon intervention by a national resolution authority, Microsoft will comply with the requirements of such national resolution authority. Further detail is set out in the FS Amendment.	FS Amendment, section 8 (Business Continuity of Online Services)


Item	Reference	Requirement	MS commentary / How and where is this dealt with in the Microsoft Agreement?	MS Agreement reference
 <h2 style="display: inline;">Access and Audit</h2>				
29.	EBA 75(p) EIOPA 37(m) ESMA 41(n)	The unrestricted right of financial institutions and competent authorities (including resolution authorities), and any person appointed by them, to inspect and audit the service provider with regard to the critical or important outsourced function, including:	Microsoft provides customers with the ability to access and extract customer data, as well audit and monitoring mechanisms, to enable customers to comply with their regulatory obligations. These rights of access and audit extend to regulators of customers.	DPA, "Auditing Compliance" provision  FS Amendment, section 2(b) (Audits of Online Services by Microsoft)  FS Amendment, section 3 (Unrestricted Rights of Examination or Audit by Regulator)  FS Amendment, section 4 (Unrestricted Rights of Audit by Customer)
30.	EBA 85	Right of the financial institution's internal audit function to review the outsourced function;	Microsoft provides customers with the ability to access and extract customer data, as well audit and monitoring mechanisms, to enable customers to comply with their regulatory obligations.  Additional monitoring, supervisory and audit rights are set out in the FS Amendment.	FS Amendment, section 4 (Unrestricted Rights of Audit by Customer)
31.	EBA 87	Full access to the service provider's relevant business premises (including devices, systems, networks, information and data, related financial information, personnel and the service provider's external auditor) and	<b>Full access to business premises</b>  Microsoft permits any necessary examination or monitoring required to occur at Microsoft's offices or at other locations where	FS Amendment, section 3 (Unrestricted Rights of Examination or Audit by Regulator)

Item	Reference	Requirement	MS commentary / How and where is this dealt with in the Microsoft Agreement?	MS Agreement reference
		unrestricted rights of inspection and auditing;	<p>activities relating to the Online Services are performed. The customer will also have the right to elect its auditor to undertake any such visit if necessary under these provisions. However, Microsoft will only ever allow access to those premises which are relevant to the services provided to the customer.</p> <p><b>Right to inspect and audit</b></p> <p>Customers may conduct their own virtual audits of the Online Services via tools available through the <a href="#">Service Trust Portal</a>. In particular, refer to:</p> <ul style="list-style-type: none"> <li>• <a href="#">Downloadable audit reports</a>;</li> <li>• <a href="#">Security FAQs and white papers</a>;</li> <li>• <a href="#">Audit Videos</a>;</li> <li>• <a href="#">Compliance Manager</a>;</li> <li>• <a href="#">Self-paced Learning Path</a>;</li> <li>• <a href="#">TruSight Independent Assessment Reports</a>.</li> </ul> <p>Microsoft provides customers with information to reconstruct financial transactions and develop audit trail information through two primary sources: <a href="#">Azure Active Directory</a> 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 <a href="#">Azure Monitor</a>, 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.</p> <p>Customers also have access to third party audit reports commissioned by Microsoft (see row 24).</p>	<p>FS Amendment, section 4 (Unrestricted Rights of Audit by Customer)</p> <p>FS Amendment, section 5 (Customer Compliance Program)</p>

Item	Reference	Requirement	MS commentary / How and where is this dealt with in the Microsoft Agreement?	MS Agreement reference
32.	EBA 89 EIOPA 38 ESMA 47	The agreement or any other contractual arrangement must not impede or limit the effective exercise of the access and audit rights by financial institutions, competent authorities or third parties appointed by them to exercise these rights;	<p>Microsoft will provide unrestricted audit and access rights to customers and regulators.</p> <p>To the extent the customer’s audit requirements cannot be satisfied through audit reports, documentation or compliance information Microsoft makes generally available to its customers, or the audit and access rights generally available to customers, Microsoft offers additional monitoring, supervisory and audit rights over Microsoft cloud services through the FS Amendment.</p>	<p>FS Amendment, sections 3 (Unrestricted Rights of Examination or Audit by Regulator)</p> <p>FS Amendment, section 4 (Unrestricted Rights of Audit by Customer)</p> <p>FS Amendment, section 5 (Customer Compliance Program)</p>
33.	EBA 94	The ability of the financial institution, where relevant, to carry out security penetration testing to assess the effectiveness of implemented cyber and internal ICT security measures and processes.	<p>Customers may carry out vulnerability and penetration testing of the services in certain circumstances (for example, where the customer notifies Microsoft in advance of such tests).</p> <p><b>For more information, refer to:</b></p> <ul style="list-style-type: none"> <li>• <a href="#">Microsoft Cyber Defense Operations Center</a>;</li> <li>• <a href="#">Microsoft Rules of Engagement</a> for customers wishing to perform penetration tests against their Microsoft Cloud components;</li> <li>• <a href="#">Microsoft Online Services Bounty Program</a>.</li> </ul>	FS Amendment, section 2(a) (Penetration Testing by Customer and Microsoft)
<div style="background-color: #0070C0; color: white; padding: 5px;">  <span style="font-size: 1.2em; font-weight: bold; vertical-align: middle;">Termination rights</span> </div>				
34.	EBA 75(q) EIOPA 55	Termination rights, including:	The Microsoft Agreement includes rights to terminate early for cause and without cause. Refer to your Microsoft Agreement.	N/A



Item	Reference	Requirement	MS commentary / How and where is this dealt with in the Microsoft Agreement?	MS Agreement reference
	ESMA 40			
35.	EBA 98(a)	Where the service provider is in a breach of applicable law, regulations or contractual provisions;	The customer may with reasonable notice terminate an Online Service upon Microsoft's breach of applicable law, regulations or its contractual obligations.	FS Amendment, section 7 (Additional customer termination rights)
36.	EBA 98(b)	Where impediments capable of altering the performance of the outsourced function are identified;	The customer may with reasonable notice terminate an Online Service where impediments capable of altering the performance of the outsourced function are identified.	FS Amendment, section 7 (Additional Customer Termination Rights)
37.	EBA 78(g) & 98(c) EIOPA 50(e) ESMA 55(f)	Where there are material changes affecting the outsourcing arrangement or the service provider (e.g. sub- outsourcing or changes of sub- contractors);	The customer may with reasonable notice terminate an Online Service where the customer can reasonably demonstrate that there are material changes affecting the provisioning of the Online Service by Microsoft, or if the customer does not approve of a new subprocessor that has access to customer/ personal data.	FS Amendment, section 7 (Additional Customer Termination Rights)
38.	EBA 98(d)	Where there are weaknesses regarding the management and security of confidential, personal or otherwise sensitive data or information; and	The customer may with reasonable notice terminate an Online Service where the customer can reasonably demonstrate that there are weaknesses regarding the management and security of customer data or information.	FS Amendment, section 7 (Additional Customer Termination Rights)
39.	EBA 98(e)	Where instructions are given by the financial institution's competent authority.	The customer may terminate an Online Service at the express direction of a regulator with reasonable notice.	FS Amendment, section 7 (Additional Customer Termination Rights)

Item	Reference	Requirement	MS commentary / How and where is this dealt with in the Microsoft Agreement?	MS Agreement reference
 <b>Exit management</b>				
40.	EBA 40(f), 99 & 106-108	The outsourcing arrangement must facilitate the transfer of the outsourced function to another service provider or its re-incorporation into the financial institution. To this end, the agreement must include:	See rows below and white papers on exit management available via the <a href="#">Service Trust Portal</a> .	N/A
41.	EBA 99(a) ESMA 44(c)	The obligations of the service provider, in the case of a transfer of the outsourced function to another service provider or back to the financial institution, including the treatment of data.	<p><b>Treatment of data on termination</b></p> <p>Customers are able to access, extract and delete customer data stored in each Online Service at all times during the term of the subscription and for a limited period after expiration or termination of the subscription (see row 18).</p> <p>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.</p>	<p>DPA, “Data retention and deletion”</p> <p>FS Amendment, section 3 (Unrestricted Rights of Examination or Audit by regulator)</p> <p>FS Amendment, section 8 (Business Continuity of Online Services)</p>
42.	EBA 99(b)	The transition period (which must be appropriate), during which the service provider, after the termination of the outsourcing arrangement, will continue to provide the outsourced function to reduce the risk of disruptions;	The FS 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.	FS Amendment, section 8 (Business Continuity of Online Services)

Item	Reference	Requirement	MS commentary / How and where is this dealt with in the Microsoft Agreement?	MS Agreement reference
43.	EBA 99(c)	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.		

## Conflicts of interests

44.	EBA 45, 46 & 61(e)	<i>Non-contractual requirement</i> Financial institutions must identify, assess and manage conflicts of interests with regard to their outsourcing arrangements.	This is a customer consideration.	N/A
-----	--------------------	---	-----------------------------------	-----

## Capacity

45.	EBA 69 & 70	<i>Non-contractual requirement</i> Financial institutions must ensure that the service provider is suitable. In particular, with regard to outsourcing critical or important functions, the service provider must have the business reputation, appropriate and sufficient abilities, the expertise, the capacity, the resources, the organisational structure and (if applicable) the required regulatory authorisations or registrations to perform the critical or important function reliably and	<p><b>Business reputation</b></p> <p>Many of the world's top companies use Microsoft cloud services, including financial institution customers in leading markets. Please refer to <a href="https://customers.microsoft.com">customers.microsoft.com</a> for access to case studies relating to the use of Microsoft cloud services.</p> <p><b>Ability, expertise and capacity</b></p> <p>Microsoft is an industry leader in cloud computing and has the ability, expertise and capacity to deliver cloud services to customers across the globe. 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.</p>	N/A
-----	-------------	--	---	-----

Item	Reference	Requirement	MS commentary / How and where is this dealt with in the Microsoft Agreement?	MS Agreement reference
		professionally and to meet its contractual obligations.	<p>A list of its current certifications is available at <a href="https://microsoft.com/en-us/trustcenter/compliance/complianceofferings">microsoft.com/en-us/trustcenter/compliance/complianceofferings</a>.</p> <p><b>Resources and organisational structure</b></p> <p>Microsoft considers that it has the resources and an appropriate organisational structure to deliver cloud services to clients across the globe. Customers may access information on Microsoft’s company profile via <a href="https://microsoft.com/en-us/investor/">microsoft.com/en-us/investor/</a> and Microsoft’s annual reports via <a href="https://microsoft.com/en-us/Investor/annual-reports.aspx">microsoft.com/en-us/Investor/annual-reports.aspx</a>.</p>	

© 2020 Microsoft Corporation. All rights reserved. Please note this document is provided “as-is.” Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it. Neither the information in the checklist nor any of the information available via the links provided is 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. This document does not provide you with any legal rights to any intellectual property in any Microsoft Product. You may copy and use this document for your internal reference purposes only.