Microsoft Cloud Services

A compliance checklist for financial institutions in Australia

Version: 12 April 2019

Contents

Introduction: A compliance checklist for financial institutions in Australia	**Page 3**
Overview of the Regulatory Landscape	**Page 6**
Compliance Checklist	**Page 10**
Part 1: Key Considerations	***Page 11***
Part 2: Contract Checklist	***Page 54***
Further Information	**Back**

Introduction: A compliance checklist for financial institutions in Australia

Overview

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

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. In its 2018 Information Paper, "Outsourcing Involving Cloud Computing Services", the Australian Prudential Regulatory Authority (**APRA**) noted a continuous evolution, since 2015, of both cloud computing service offerings and financial institutions' risk management. Service providers have strengthened their control environments and improved their customers' ability to monitor their environments, and financial institutions have also improved their management capability and processes for assessing and overseeing the services provided.

Microsoft is committed to providing a trusted set of cloud services to financial institutions in Australia. 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 Australia. We developed it to help financial institutions in Australia adopt Microsoft cloud services with the confidence that they can meet 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 Australia;

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 Australia who want to use Microsoft cloud services. We use the term "financial institutions" broadly, to include any entity that is regulated by APRA. These entities include banks, credit unions, general insurers, life insurers and superannuation entities.

What Microsoft cloud services does this checklist apply to?

This checklist applies to Microsoft Office 365, Microsoft Dynamics 365 Core Services and Microsoft Azure Core Services, as referenced in Microsoft's Online Services Terms (**OST**). 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?

No. In Australia, there is no mandatory requirement for financial institutions to complete a checklist to adopt Microsoft cloud services. However, through conversations with our many cloud customers in Australia, we understand that a checklist approach like this is helpful – first, as a way of understanding the regulatory requirements; second, as a way of learning more about how Microsoft cloud services can help financial institutions meet those regulatory requirements; third, as an internal framework for documenting compliance; and fourth, as a tool to streamline consultations with APRA, if they are required. By reviewing and completing the checklist, financial institutions can adopt Microsoft cloud services with confidence that they are complying with the requirements in Australia.

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 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 to assisting in any required consultation with APRA. 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's 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 Protection Terms (**DPT**) of Microsoft's OST.

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 Australian Prudential Regulatory Authority (**APRA**). Banks, credit unions, general insurers, life insurers, superannuation trustees and other financial institutions are regulated by APRA. The APRA website at apra.gov.au provides links to underlying regulations and guidance.
What regulations and guidance are relevant?	There are several requirements and guidelines that financial institutions should be aware of when moving to the cloud: 1. APRA Prudential Standard: Information Security (CPS 234) July 2019 (**Information Security Standards**)* 2. APRA Information Paper, "Outsourcing involving cloud computing services", September 2018 (**APRA Cloud Information Paper**) 3. APRA Prudential Standard: Outsourcing (CPS 231) July 2017 (**Outsourcing Standards**)* 4. APRA Prudential Standard: Outsourcing (SPS 231) July 2013 (applying to registrable superannuation entities only, these standards are materially similar to the Outsourcing Standards)* 5. APRA Prudential Practice Guide: Outsourcing (PPG 231 — Outsourcing) 6. APRA Prudential Practice Guide: Management of Security Risk in Information and Information Technology (CPG 234) 7. APRA Prudential Standard: Business Continuity Management (CPS 232) July 2017* 8. APRA Prudential Standard: Risk Management (CPS 220) July 2017* 9. APRA Prudential Standard: Fit and Proper (CPS 520) July 2017* 10. APRA Prudential Practice Guide: Managing Data Risk (CPG 235) The latest version of each document can be found on the APRA website at https://www.apra.gov.au/adi-standards-and-guidance. The APRA Cloud Information Paper is the best starting point for a financial institution transitioning a workload to the cloud. Microsoft

	has published a response to the APRA Cloud Information Paper. In it, Microsoft responds to each issue raised and demonstrates how Australian financial services organisations can move to Microsoft cloud services in a manner consistent with the APRA Cloud Information Paper. Microsoft's response is available at: aka.ms/apraresponse. *Please be advised that these marked standards are legally binding on financial institutions, and the other documents provide guidance only.
Is regulatory approval required?	**No.** However, financial institutions must: • **notify** APRA after entering into agreements involving material outsourcing arrangements within Australia; or • **consult** with APRA before outsourcing material business activities outside of Australia. In practice, financial institutions need to be satisfied that APRA has no objections to the offshore outsourcing before entering into the agreement. See below for details of what constitutes a "material business activity". In addition, when the proposed use of cloud computing services involves "heightened" or "extreme inherent risks" (see below), the financial institution is encouraged (but not required) to consult with APRA, regardless of whether the service is provided within or outside of Australia. Formal consultation for initiatives with "heightened inherent risk" should take place after the financial institution has completed its internal governance processes and the initiative has been fully risk-assessed and approved by the appropriate governance authority. For uses involving "extreme inherent risk", APRA encourages early engagement so that it has the ability to provide feedback on any areas of potential concern.
What is a "material business activity"?	**At the outset, it is important to note that APRA is concerned with cloud scenarios that involve outsourcing a "material business activity". If that threshold is not met, no consultation or notification is required and the Outsourcing Standards do not apply.** A "material business activity" is an activity that has the potential, if disrupted, to have a significant impact on the financial institution's business operations or its ability to manage risks effectively. Applying APRA's material business activity definition involves a very context-specific inquiry. Your organisation will need to look closely at the business processes and IT assets impacted by the proposed cloud service, as well as the service's projected uptake within your organisation. APRA also recommends scenario analysis of plausible security events as a useful technique for understanding the materiality of the arrangement. Microsoft is available to help you throughout this assessment. We are experienced in helping customers conduct risk assessments and engage with regulators, including APRA. We can assist by providing

	resources to inform your business case and risk assessments, including the most recent audit reports for our cloud services. We are also happy to facilitate discussions with Microsoft subject matter experts to answer questions that arise during your organisation's own due diligence or APRA engagement. Please contact your Account Manager to let us know how we can help.

What is "heightened inherent risk" and "extreme inherent risk"?	According to the APRA Cloud Information Paper:
	• arrangements with a **"heightened inherent risk"** are arrangements involving critical and/or sensitive IT assets that result in either:
	  ○ an increased likelihood of a disruption; or
	  ○ where a disruption would result in a significant impact; and
	• arrangements with an **"extreme inherent risk"** are heightened inherent risk arrangements which could, if disrupted, result in an extreme impact (including financial and reputational impacts, potentially threatening the ongoing ability of the financial institution to meet its obligations).

Are transfers of data outside of Australia permitted?	**Yes.** Australian privacy legislation (which applies across all sectors, not just to financial institutions) permits transfers outside of Australia where: (a) the individual gives informed consent; (b) the financial institution reasonably believes that the cloud services provider is subject to laws, binding schemes or contracts that protect personal information in a substantially similar way to those in Australia; or (c) the cloud services provider agrees to contractual terms in line with the Australian Privacy Principles. Even though Microsoft agrees to contractual terms in line with the Australian Privacy Principles and transfers of data outside of Australia are permitted, many of our Australian financial services customers take advantage of the cloud services available from our Australian data centres, including Azure, Office 365 and Dynamics 365. Since April 2018, our Australian financial services customers have been able to access two new Microsoft Azure cloud regions that are specifically designed to support the regulated financial services community. Known as Azure Australia Central Regions, they are located within the highly secure, resilient Australian-owned facilities of Canberra Data Centres (CDC). We make specific contractual commitments to store categories of data at rest in the Australian geography. These are outlined further in the Compliance Checklist, below.
Are public cloud services sufficiently secure?	**Yes.** Many financial institutions in Australia 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. The use of cloud services has evolved significantly in recent years. APRA has observed the growing usage of cloud computing services by financial institutions in Australia. In addition, the APRA Cloud Information Paper mentions that cloud service providers have strengthened their control environments, increased transparency regarding the nature of the controls in place, and improved their customers' ability to monitor their environments.
Are there any mandatory terms that must be included in the contract with the services provider?	**Yes.** APRA does stipulate some specific points that financial institutions must ensure are incorporated in their cloud services contracts. These are primarily set out in the Outsourcing Standards. 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 Australian privacy laws apply to the use of cloud services by financial institutions?	The **Australian Privacy Principles** set out in the Privacy Act 1988 (Cth) will apply to personal information collected by financial institutions. When it comes to outsourcing arrangements, the financial institution is likely to be accountable for downstream use of the personal information by its service providers. In Microsoft's experience, privacy compliance is an increasingly important issue for financial institutions and we address the requirements, and provide details of how they apply to use of Microsoft cloud services, in the Compliance Checklist below. Additionally, a European privacy law, the General Data Protection Regulation (**GDPR**), came into effect on 25 May 2018. Of note, 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 monitor personal behaviour taking place in the EU. In this regard, the GDPR applies on an extraterritorial basis, and not only to entities that are established in the EU. Microsoft is committed to GDPR compliance across its cloud services and provides GDPR related assurances in its contractual commitments. You can learn more about how Microsoft's products help you comply with the GDPR here.

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.

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 Australia.

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?	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
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.

Ref.	Question / requirement	Guidance
		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?	*APRA believes that the nature of the type of cloud services consumed presents different risk profiles, and an understanding of the type of cloud solution may be relevant when determining the risk associated with the solution (see APRA Cloud Information Paper and Microsoft's response at aka.ms/apraresponse). 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	*Various APRA guidelines focus on the risks associated with data processing – for example, the "Prudential Practice Guide: CPG 235 – Managing Data Risk". It is therefore 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*

Ref.	Question / requirement	Guidance
	behalf of the financial institution?	*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, account information, payment card data, security credentials 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). • Transaction data (data relating to transactions in which the organisation is involved). • Indices (for example, market feeds). • Other personal and non-personal data relating to the organisation's business operations as a financial institution. 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?	*Various APRA documents recommend that financial institutions do their due diligence on the service provider to address risks associated with a service provider failing to meet the terms of any agreement or otherwise to perform as agreed (for example, the APRA Prudential Practice Guide: Outsourcing). 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 financial institutions globally. Microsoft also makes specific commitments across its Online Services in its Online Services Terms available at https://www.microsoft.com/en-sg/Licensing/product-licensing/products.aspx.

Ref.	Question / requirement	Guidance
		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. Office 365 has grown to have over 100 million users, including some of the world's largest organisations and financial institutions. Azure continues to experience more than 90% growth, and over 80% of the largest financial institutions use or have committed to use Azure services. **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 $800 billion (as of October 2018), 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.
B. OFFSHORING ***Microsoft gives customers the opportunity to choose that certain core categories of data will be stored at-rest within Australia. This section only applies to the extent that data and services will be hosted outside of Australia. This will depend on the configuration of Microsoft cloud services that you select. Your responses will need to be tailored accordingly.***		
7.	Will the proposed outsourcing require offshoring? If so, from which territory(ies) will the	*The Outsourcing Standards state that a regulated institution must consult with APRA before entering any offshoring agreement involving a material business activity so that APRA can satisfy itself that the impact of the offshoring arrangement has been*

Ref.	Question / requirement	Guidance
	outsourced cloud services be provided?	*adequately addressed as part of the risk management framework. Microsoft provides data location transparency and allows customers to choose that certain categories of data will be stored at-rest within Australia.* *If using Office 365 and/or Dynamics 365:* Customers can configure the service such that core categories of data are stored at rest within Australia. These categories of data are described in the interactive data centres map at o365datacentermap.azurewebsites.net. Certain other categories of data may be stored outside of Australia and the relevant locations are also described in the interactive data centres map. *If using Azure:* Customers can configure the service such that core categories of data are stored at rest within Australia. These categories of data are described in the interactive data centres map at: azure.microsoft.com/en-us/regions. Certain other categories of data may be stored outside of Australia and the relevant locations are also described in the interactive data centres map. Since April 2018, our Australian financial services customers have been able to access two new Microsoft Azure cloud regions that are specifically designed to support the regulated financial services community. Known as Azure Australia Central Regions, they are located within the highly secure, resilient Australian-owned facilities of Canberra Data Centres (CDC).
8.	APRA considers that an offshoring arrangement "can give rise to a number of particular risks". How do arrangements with the cloud services	*The APRA Prudential Practice Guide: Outsourcing lists the following potential risk areas:* *(a) Country risk — the risk that overseas economic, political and/or social events will have an impact upon the ability of an overseas service provider to continue to provide an outsourced service to the regulated institution.* *(b) Compliance (legal) risk — the risk that offshoring arrangements will have an impact upon the regulated institution's ability to comply with relevant Australian and foreign laws and regulations (including accounting practices).* *(c) Contractual risk — the risk that the regulated institution's ability to enforce the offshoring agreement may be limited or completely negated.*

Ref.	Question / requirement	Guidance
	provider manage these risks?	*(d) Access risk — the risk that the ability of the regulated institution to obtain information and to retain records is partly or completely hindered. This risk also refers to the potential difficulties or inability of APRA to gain access to the service provider and the material business activity being conducted for prudential review purposes.* *(e) Counterparty risk – see Section A (Overview), Question 6 above.* First, and most importantly, the customer can configure the service such that core categories of data are stored at rest within Australia. In relation to the limited categories of data that are stored or processed outside of Australia, customers may become satisfied that any offshoring risk is addressed for the following reasons: i. Customers know where their data is stored. For the limited categories of data stored or processed outside of Australia, the relevant locations are listed at o365datacentermap.azurewebsites.net *(for Office 365 and Dynamics 365)* and at azure.microsoft.com/en-us/regions *(for Azure)*. ii. The relevant data centres are strategically located, taking into account a long list of country and socioeconomic factors. Microsoft's data centres are located in jurisdictions that are recognised as stable, safe, and reliable with respect to their legal systems, regulatory regime, technology, and infrastructure. The circumstances under which authorities in these countries may have rights to access information are not considered to be unwarranted. iii. The customer's ability to enforce the agreement against Microsoft is not affected by any use of Microsoft's data centres outside of Australia. Microsoft is a large international organisation with significant resources. It has a presence in many countries (including Australia) and has a long-track record in financial services. iv. APRA's regulatory oversight and access is not impacted by use of Microsoft's data centres outside of Australia. There are terms in the contract that enable APRA to examine Microsoft's facilities, systems, processes and data relating to the services. v. The customer's ability to access data is not affected by use of Microsoft's data centres outside of Australia. When customers stores data in Microsoft cloud services, they retain ownership of that data. They can download a copy of that data at any time and for any reason, without assistance from Microsoft.

Ref.	Question / requirement	Guidance
9.	What other risks have been considered in relation to the proposed offshoring arrangement?	*APRA Prudential Practice Guide: Outsourcing, states that "Typically, these and other risks would be specifically addressed during the preparation of a business case, when conducting due diligence and during contract negotiations". 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 environments. **b. Country/socioeconomic** Microsoft's data centres 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 data centres 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. Since April 2018, our Australian financial services customers have been able to access two new Microsoft Azure cloud regions that are specifically designed to support the regulated financial services community. Known as Azure Australia Central Regions, they are located within the highly secure, resilient Australian-owned facilities of Canberra Data Centres (CDC). Azure Australia Central Regions deliver high availability and performance, low latency, disaster resilience and the opportunity for real-time data streaming and analysis. Highly secure and with the leading security certifications, these regions were built with the challenging demands and specific risk profiles of mission-critical computing in mind. In addition, Microsoft's data centres in Australia have been formally assessed against the Security Construction and Equipment Committee (SCEC) standards for the construction of secure zones and facilities and have met the requirements for SCEC Zone 3 in accordance with aka.ms/ausdcphysical. **d. Environmental (i.e. earthquakes, typhoons, floods)** Microsoft data centres are built in seismically safe zones. Environmental controls have been implemented to protect the data centres including temperature control, heating, ventilation and air-conditioning, fire detection and suppression systems and

<table>
<tr><th>Ref.</th><th>Question / requirement</th><th>Guidance</th></tr>
<tr><td></td><td></td><td>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 APRA's regulatory oversight. The terms are summarised in Part 2.</td></tr>
<tr><td colspan="3">C. COMPLIANCE WITHIN YOUR ORGANISATION

APRA requires that financial institutions 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.</td></tr>
<tr><td>10.</td><td>The financial institution must be able to demonstrate to APRA that, in assessing the options for outsourcing a material business activity to a third party, it has undertaken certain steps by way of due diligence (as set out in the next column). How does the</td><td>This section sets out each of the steps required by APRA under section 26 of the Outsourcing Standards. The APRA Cloud Information Paper emphasises that cloud services are based on a shared responsibility model – a recognition that the allocation of responsibility for the implementation of controls is a shared responsibility between the service provider and the customer.

Has your organisation:

<table>
<tr><td>(a) prepared a business case for outsourcing the material business activity;</td><td>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</td></tr>
</table>
</td></tr>
</table>

Ref.	Question / requirement	Guidance		
	financial institution comply?		• 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 data centres 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's Online Services in terms of managing updates, addressing security threats, and providing real-time improvements to the service are	

Ref.	Question / requirement	Guidance		
			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.	
		(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).	
		(c) undertaken a due diligence review of the chosen service provider, including the ability of the service provider to conduct the	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.	

Ref.	Question / requirement	Guidance	
		business activity on an ongoing basis;	
		(d) involved the Board of the APRA-regulated institution, Board committee of the APRA-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.
		(e) considered all of the minimum contractual requirements required by APRA;	See Part 2 of this Compliance Checklist.
		(f) established procedures for monitoring	See Question 13 for relevant information about the measures offered by Microsoft to enable customers to monitor performance.

Ref.	Question / requirement	Guidance		
		performance under the outsourcing agreement on a continuing basis;		
		(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 that have executed the Financial Services Amendment 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.	
		(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 stored in each Online Service at all times 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
11.	Does the financial institution have a policy, approved by the Board, relating to the outsourcing?	*APRA requires that financial institutions have a Board-approved policy in relation to the outsourcing, which must "set out the approach to outsourcing of material business activities, including a detailed framework for managing all such outsourcing arrangements" (Outsourcing Standards section 23).* 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 materiality 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 10 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.
12.	What procedures does the financial	*Outsourcing Standards section 21.*

Ref.	Question / requirement	Guidance
	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.
13.	What monitoring processes does the financial institution have in place to manage the outsourcing?	*APRA requires that financial institutions have sufficient monitoring processes in place to manage the outsourcing, so you should consider what internal processes you have or will put in place. 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's 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 data centres 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

Ref.	Question / requirement	Guidance
		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 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) ad hoc access to Microsoft subject matter experts for raising questions and escalations relating to Microsoft cloud services, (b) an invitation to participate in an annual 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 detailed reports 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) an opportunity to attend an annual compliance summit which includes technical presentations from Microsoft's senior engineering managers.
14.	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?	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's Online Services that includes non-confidential compliance information; • the Service Trust Portal, which provides confidential materials, such as third-party audit reports, to current customers and potential customers testing Microsoft's Online Services;

Ref.	Question / requirement	Guidance
		• a Financial Services Compliance Program, which provides regulated financial services customers with the opportunity to examine the control framework of the cloud service, review their risk management framework, hold one-to-one discussions with Microsoft's auditors and obtain in-depth views directly from Microsoft subject matter experts; • 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's 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.
15.	How does the financial institution ensure that it maintains ultimate responsibility for any outsourcing?	*The Outsourcing Standards section 22 provides that although outsourcing may result in the service provider having day-to-day managerial responsibility for a business activity, the APRA-regulated institution is responsible for complying with all prudential requirements that relate to the outsourced business activity.* The contract with Microsoft provides the customer with legal mechanisms to manage the relationship including appropriate allocation of responsibilities, oversight and remedies and the mandatory terms required by APRA.
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 APRA 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 APRA***		

Ref.	Question / requirement	Guidance
suggests are considered as part of the contractual negotiation but which are not necessarily mandatory contractual terms that should be included in all cases.		
16.	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 Outsourcing Standards?	*Outsourcing Standards section 28.* 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.
17.	Does the outsourcing agreement include a clause that allows APRA to access documentation and information relating to the outsourcing arrangement?	*Outsourcing Standards section 34.* Yes. There are terms in the contract that enable APRA to carry out inspection or examination of Microsoft's facilities, systems, processes and data relating to the services. As part of the Financial Services Amendment that Microsoft offers to regulated financial services institutions, Microsoft will, upon a regulator's request, provide the regulator a direct right to examine the relevant service, including the ability to conduct an on-premises examination; to meet with Microsoft personnel and Microsoft's external auditors; and to access related information, records, reports and documents. 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.
18.	Does the outsourcing agreement provide a guarantee of access to the minimum IT assets required to	*APRA Prudential Practice Guide: Management of Security Risk in Information and Information Technology.* 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

Ref.	Question / requirement	Guidance
	operate under a disaster scenario?	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.
19.	Does the outsourcing agreement also include reporting mechanisms that ensure adequate oversight of IT security risk management by the service provider?	*APRA Prudential Practice Guide: Management of Security Risk in Information and Information Technology.* Yes as referenced in Question 14 above.
20.	Is the outsourcing agreement sufficiently flexible to accommodate changes to existing processes and to accommodate new processes in the future to meet changing circumstances?	*APRA Prudential Practice Guide: Outsourcing.* 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.
21.	In the event of termination, do transitional arrangements	*APRA Prudential Practice Guide: Outsourcing.*

Ref.	Question / requirement	Guidance
	address access to, and ownership of, documents, records, software and hardware, and the role of the service provider in transitioning the service?	Yes. 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.
E. TECHNICAL AND OPERATIONAL RISK Q&A ***Under various APRA 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.***		
22.	Does the service provider permit audit by the financial institution and/or APRA?	*Outsourcing Standards section 34. The APRA Cloud Information Paper also identifies this as a separate consideration for APRA-regulated entities.* Yes. Pursuant to the Financial Services Amendment, Microsoft provides APRA 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 APRA 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 data centres that it uses in processing customer data for

Ref.	Question / requirement	Guidance
		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. See Part 2 below, in relation to Section 29(h), Outsourcing Standards for further detail.
23.	Are the provider's services subject to any third party audit?	*APRA Prudential Practice Guide: Management of Security Risk in Information and Information Technology. APRA envisages that a regulated institution would ensure audit trails exist for IT assets that facilitate independent audit.* Yes. 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. In Australia, our services undertake a biennial Information Security Registered Assessor (IRAP) assessment, are certified by the Australian Signals Directorate (ASD), and are listed on the Certified Cloud Services List (CCSL) (https://asd.gov.au/infosec/cloudsecurity.htm) as being able to store and process Australian Government sensitive information that is classified with Dissemination Limiting Markers (DLMs). Copies of these audit reports are available at microsoft.com/en-us/trustcenter/guidance/risk-assessment. In addition, the Financial Services Amendment further gives customers the opportunity to participate in the optional Financial Services Compliance Program at any time, which enables them to (amongst other things) participate in an annual 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. A recording of this webcast will also be made available for members of the Financial Services Compliance Program.
24.	What security controls are in place to protect the transmission and storage of confidential information such as customer data within	*The APRA guidance focuses on confidentiality in several places, both in terms of general requirements and as something that should be addressed in the outsourcing contract. For example, section 16 of the Information Security Standards states that, where information assets are managed by a service provider, financial institutions must assess the information security capability of that service provider, commensurate with the potential consequences of an information security incident affecting those assets*

Ref.	Question / requirement	Guidance
	the infrastructure of the service provider?	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 data centres 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 centres 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 data centre. 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 data centre. 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

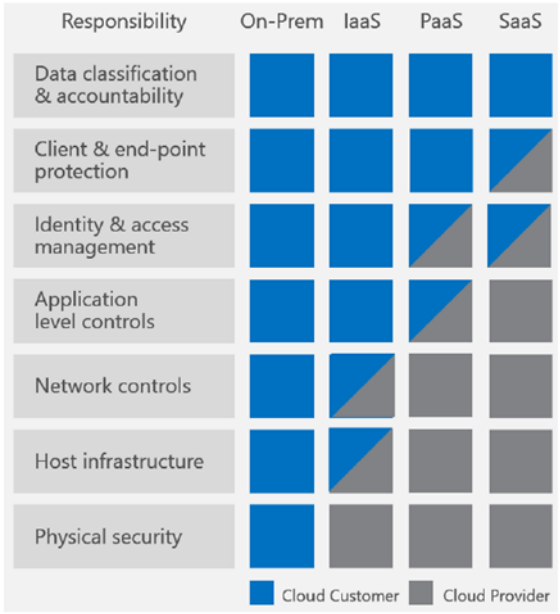
Ref.	Question / requirement	Guidance
		basis. From a people and process standpoint, preventing breach involves auditing all operator/administrator access and actions, zero standing permission for administrators in the service, “Just-In-Time (JIT) access and elevation” (that is, elevation is granted on 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 background checks are automatically rejected from high privilege access, and checking employee backgrounds is a highly scrutinised, 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 centre 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 data centres. For data at rest, Azure offers many encryption options,

Ref.	Question / requirement	Guidance
		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 Portal.
25.	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. 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.
26.	How are the service provider's access logs monitored?	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.
27.	What policies does the service provider have in place to monitor employees	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

Ref.	Question / requirement	Guidance
	with access to confidential information?	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.
28.	How are customers authenticated?	*APRA Prudential Practice Guide: Management of Security Risk in Information and Information Technology: "A regulated institution would normally take appropriate measures to identify and authenticate users or IT assets".* 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.
29.	Does the service provider have sufficient information security capability?	*Information Security Standards sections 15 – 17. Financial institutions must maintain an information security capability that is commensurate with the size and extent of threats to its information assets, and must continue to maintain that information security capability in light of changes in vulnerabilities and threats. In addition, APRA requires that financial institutions assess the information security capability of the service provider to ensure that it is commensurate with the potential consequences of an information security incident affecting those information assets managed by the service provider.* There are several avenues through which financial institutions can assess the information security capability of Microsoft and evaluate the design of the information security controls of Microsoft cloud services. Together they ensure that you can meet your regulatory requirements and supervise the cloud services. First, Microsoft provides many built-in service capabilities to help you examine and verify access, control and service operation as part of your regular assurance processes. These include: • **Service Trust Portal** – for deep technical trust and compliance information, including recent audit reports for our services, as well as the International Standards Organisation (ISO) Statements of Applicability

Ref.	Question / requirement	Guidance
		• **Compliance Manager** – a tool that provides detailed information about our internal controls, including test status and most recent test dates, and allows you to create your own assessments and monitor your own controls • **Office 365 Audited Controls** – for detailed information about our internal control set, including mapping to international standards, and the most recent test dates • **Office 365 Management Activity API** – for visibility of user, admin, system and policy actions and events from your Office 365 and Azure Active Directory activity logs • **Office 365 Health Dashboard** – to immediately check service health, including current known services issues and ongoing resolution plans in progress • **Azure Security Center** – for visibility into the security state of your Azure resources and the ability to respond to threats and vulnerabilities • **Azure Advisor** – for continuous intelligent recommendation for how to further secure your Azure environment • **Microsoft Trust Center** – for information about data protection and security, including the location of our primary and backup data centres, subcontractor lists, and rules for when Microsoft service administrators have access to customer data. Furthermore, our extended contract terms for financial services customers add the ability for your internal compliance officers to examine the service more deeply to meet regulatory requirements. Through the optional Financial Services Compliance Program, customers have the opportunity to examine the control framework of the service, review its risk management framework, hold one-to-one discussions with Microsoft's auditors and obtain in-depth views directly from Microsoft subject matter experts.

Ref.	Question / requirement	Guidance
		The Microsoft Security Policy Governance White Paper provides an overview of Microsoft's Security Policy Framework, with links to the key Microsoft Security Policy documents. Customers can refer to the Azure Response on Security, Privacy and Compliance to assess Microsoft security capability for Azure, and underpinning Office 365 / Microsoft 365 and Dynamics 365 cloud services.
30.	Does the financial institution have an information security policy framework? If so, does it address the responsibilities of the service provider?	*Every financial institution must maintain an information security policy framework under sections 18 and 19 of the Information Security Standards. This policy framework must be commensurate with the financial institution's exposures to vulnerabilities and threats. Because the service provider is also obliged to maintain information security, the policy framework must also provide direction on the responsibilities of the service provider.* Microsoft cloud services comply with several security frameworks, such as ISO 27001, PCI- DSS and FedRAMP etc. These frameworks mandate Microsoft to implement a comprehensive Vulnerability Management Framework for continuous assessment of known and unknown threats. Microsoft cloud security policy framework compliance offerings are committed in the "*Security Practices and Policies*" section of the Online Services Terms and are summarised at the Trust Center Compliance Offerings page. A financial institution's information security policy framework should include roles for Microsoft, as cloud services provider, consistent with the customer-side and service-side controls in the shared responsibility model (see diagram below), and with contractual commitments in the Online Services Terms.

Ref.	Question / requirement	Guidance
		The figure below describes how shared responsibility works across the cloud service models.  For more information, see our White Paper on Shared Responsibilities for Cloud Computing and related Blog Post.
31.	Are all information assets of the financial institution (including those managed by the service provider) classified by	*Information Security Standards section 20. This classification must reflect the degree to which an information security incident affecting an information asset has the potential to affect, financially or non-financially, the financial institution or the interests of depositors, policyholders, beneficiaries or other customers.* Microsoft has implemented and commits to maintain specified security measures for Customer Data in the Core Online Services, including Asset Inventory and Asset Handling practices and other security commitments set out in the OST. Additionally, Microsoft has cloud service offerings that leverage data classification and protection technologies to help financial institutions discover, classify, protect and monitor their sensitive data, across devices, apps, cloud services and on-premises.

Ref.	Question / requirement	Guidance
	criticality and sensitivity?	Examples of Microsoft Information Protection solutions can be found here, including Azure Information Protection, Office 365 Information Protection, Windows Information Protection, and Microsoft Cloud App Security. Office 365 / Microsoft 365 also has further advanced capabilities that helps financial institutions meet higher level of assurance and compliance requirements. Examples include: • Advanced electronic discovery • Data governance and retention • Bring-your-own service encryption key • Control how Microsoft support engineer access your data • Privileged access management For Azure SQL, there are data security capabilities that support data discovery and classification, along with data masking and encryption.
32.	Does the design of the service provider's information security controls protect the financial institution's information assets?	*Financial institutions must have information security controls that are implemented in a timely manner and commensurate with the factors set out in section 21 of the Information Security Standards. These controls must protect all of the financial institution's assets, including those managed by the service provider. In addition, under section 22 of the Information Security Standards, the financial institutions must evaluate the design of the information security controls of the service provider.* To evaluate the design of Microsoft's information security controls, regulated customers should review: • Microsoft Security Policy Governance White Paper, which provides an overview of Microsoft's Security Policy Framework, with links to the key Microsoft Security Policy documents. • Information Security Management System for Microsoft's Cloud Infrastructure • Office 365 Security Incident Management

Ref.	Question / requirement	Guidance
		• Azure Security Response in the Cloud • Assessment of Azure and the Cloud Security Alliance (CSA) Cloud Control Matrix (CCM) security, privacy, compliance, and risk management requirements Microsoft Secure Score helps financial institutions to find, assess and mitigate risks, and proactively manage security controls of Microsoft cloud services. Secure Score analyses an organisation's security based on regular activities and security settings of respective Microsoft cloud service offerings, giving financial institutions security posture visibility, report on areas that require attention, as well as recommendations for actions to further reduce the attack surface in your organization. Microsoft Secure Score covers a number of Microsoft cloud service workloads, devices, identity: see Office 365, Azure Security Center, Windows 10, and Azure Active Directory.
33.	What are the procedures for detecting, responding to and reporting information security incidents?	*Information Security Standards sections 23 to 26 and the APRA Prudential Practice Guide: Management of Security Risk in Information and Information Technology. APRA requires that financial institutions maintain robust mechanisms to respond to actual and potential information security incidents in a timely manner. Such information security response plans must include mechanisms for managing all relevant stages of an incident and escalation and reporting of incidents to the Board, other governing bodies and individuals responsible for information security incident management and oversight, as appropriate. Financial institutions must annually review and test their information security response plans to ensure they remain effective and fit-for-purpose.* The Incident Management Implementation Guidance for Azure and Office 365 is a comprehensive document customers can use to harden the security posture of their Microsoft cloud environment. It outlines the best methods for configuring the tenant for optimal security incident management: prevention, detection, alerts, anomalous activity monitoring, and post-incident investigations, made possible by in-product logging capability. Microsoft's Office 365 Security Incident Management and Azure Security Response program documents also help you assess Microsoft's own incident management capabilities, policies and processes. Microsoft also supports your compliance through its "*Security Incident Notification*" commitments in the Online Services Terms:

Ref.	Question / requirement	Guidance
		"Security Incident Notification If Microsoft becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data or Personal Data while processed by Microsoft (each a "Security Incident"), Microsoft will promptly and without undue delay (1) notify Customer of the Security Incident; (2) investigate the Security Incident and provide Customer with detailed information about the Security Incident; (3) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident … Microsoft shall make reasonable efforts to assist Customer in fulfilling Customer's obligation under GDPR Article 33 or other applicable law or regulation to notify the relevant supervisory authority and data subjects about such Security Incident." "Microsoft has implemented and will maintain for Customer Data in the Core Online Services the following security measures: … **Incident Response Process** • Microsoft maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data. • For each security breach that is a Security Incident, notification by Microsoft (as described in the "Security Incident Notification" section above) will be made without undue delay and, in any event, within 72 hours. • Microsoft tracks, or enables Customer to track, disclosures of Customer Data, including what data has been disclosed, to whom, and at what time. **Service Monitoring**. Microsoft security personnel verify logs at least every six months to propose remediation efforts if necessary." Furthermore, the optional Financial Services Compliance Program provides for deeper information sharing by Microsoft about information security incidents and potential threats, including their nature, common causes and resolutions.

Ref.	Question / requirement	Guidance
		Microsoft Threat Protection (**MTP**), and other Microsoft security products and capabilities, help financial institutions to comply with this obligation. MTP provides protection across Identities, Endpoint, User Data, Cloud Apps and Infrastructure. Microsoft facilitates compliance with the obligation to annually review and test the Microsoft cloud service information security response plans, to ensure they remain effective and fit-for-purpose, through our "Auditing Compliance" contractual commitments in the Online Services Terms, described further in item 34 below.
34.	What procedures are in place to test, and conduct internal audits of, the effectiveness of information security controls, including those maintained by the service provider?	*Under sections 27 to 34 of the Information Security Standards, APRA sets out extensive requirements as to testing control effectiveness and internal audits of information security controls.* Microsoft facilitates compliance with these regulations with respect to tests of the Microsoft cloud services thoughts its "Auditing Compliance" contractual commitments in the Online Services Terms: "**Auditing Compliance** Microsoft will conduct audits of the security of the computers, computing environment and physical data centers that it uses in processing Customer Data and Personal Data, as follows: • Where a standard or framework provides for audits, an audit of such control standard or framework will be initiated at least annually. • Each audit will be performed according to the standards and rules of the regulatory or accreditation body for each applicable control standard or framework. • Each audit will be performed by qualified, independent, third party security auditors at Microsoft's selection and expense. Each audit will result in the generation of an audit report (**Microsoft Audit Report**), which Microsoft will make available at https://servicetrust.microsoft.com/ or another location identified by Microsoft. The Microsoft Audit Report will be Microsoft's

Ref.	Question / requirement	Guidance
		Confidential Information and will clearly disclose any material findings by the auditor. Microsoft will promptly remediate issues raised in any Microsoft Audit Report to the satisfaction of the auditor." Furthermore, our extended contract terms for regulated financial services customers add the ability to examine the service more deeply to meet regulatory requirements. Regulated financial services customers that opt to join the Financial Services Compliance Program (including their internal and external auditors) have the right to conduct audits on Microsoft business premises, examine the control framework of the service, review its risk management framework, hold one-to-one discussions with Microsoft's independent auditors and obtain in-depth views directly from Microsoft subject matter experts.
35.	How will the financial institution ensure that it notifies APRA of information security incidents and control weaknesses?	*The Information Security Standards require financial institutions to notify APRA of:* • *certain information security incidents – as soon as possible and, in any case, no later than 72 hours after becoming aware of such (section 35); and* • *certain information security control weaknesses – as soon as possible and, in any case, no later than 10 business days after becoming aware of such (section 36).* Microsoft supports compliance through its "*Security Incident Notification*" commitments in the Online Services Terms, which are excerpted in item 33 above. When Microsoft notifies the financial institution of an information security incident, the financial institution then "becomes aware" of the incident, and so must notify APRA as soon as possible and, in any case, no later than 72 hours, after receiving notice from Microsoft and evaluating whether the incident requires APRA notification under the criteria in section 35 of the Information Security Standards. Furthermore, the optional Financial Services Compliance Program provides for deeper information sharing by Microsoft about information security incidents and potential threats, including their nature, common causes and resolutions.

Ref.	Question / requirement	Guidance
		It is important to note that security incident monitoring is a shared responsibility. Microsoft cloud customers are responsible to detect some types of security incidents, and are not dependent upon Microsoft to detect those incidents. Microsoft provides the tools and resources outlined in item 33 above to empower our customers to identify security concerns and detect security incidents.
36.	How is end-to-end application encryption security implemented to protect PINs and other sensitive data transmitted between terminals and hosts?	*APRA Prudential Practice Guide: Management of Security Risk in Information and Information Technology: "In APRA's view, cryptographic techniques would normally be used to control access to sensitive data/information, both in storage and in transit".* Microsoft cloud services use industry-standard secure transport protocols for data as it moves through a network—whether between user devices and Microsoft data centres or within data centres 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: 1. **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. 2. **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.

Ref.	Question / requirement	Guidance
		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. e. 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. f. 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. g. 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. h. Transparent Data Encryption (TDE) encrypts data at rest when it is stored in an Azure SQL database. i. 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). j. 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).

Ref.	Question / requirement	Guidance
		3. **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.
37.	Are there procedures established to securely destroy or remove the data when the need arises (for example, when the contract terminates)?	*APRA guidance usually deals with the destruction of data in the context of decommissioning of IT assets. For example, APRA Prudential Practice Guide: Management of Security Risk in Information and Information Technology provides that: "Decommissioning and destruction controls are used to ensure that IT security is not compromised as IT assets reach the end of their useful life". Since this is a cloud-based solution, decommissioning of assets would not work in the same way as with an on-premises solution but it is still useful to consider what would happen to data at the end of the relationship with your service provider.* 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.
38.	Are there documented security procedures for safeguarding	*APRA Prudential Practice Guide: Management of Security Risk in Information and Information Technology states that "The absence of physical security could compromise the effectiveness of other IT security controls".*

Ref.	Question / requirement	Guidance
	premises and restricted areas? If yes, provide descriptions of these procedures.	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 data centres are monitored using motion sensors, video surveillance and security breach alarms.
39.	Are there documented security procedures for safeguarding hardware, software and data in the data centre?	*APRA Prudential Practice Guide: Management of Security Risk in Information and Information Technology states that "The absence of physical security could compromise the effectiveness of other IT security controls".* Yes. These are described at length in the Microsoft Trust Center at microsoft.com/trustcenter. For information on: • design and operational security see https://www.microsoft.com/en-us/trustcenter/security/designopsecurity • network security see https://www.microsoft.com/en-us/trustcenter/security/networksecurity • encryption see https://www.microsoft.com/en-us/trustcenter/security/encryption • threat management see https://www.microsoft.com/en-us/trustcenter/security/threatmanagement • identify and access management see https://www.microsoft.com/en-us/trustcenter/security/identity
40.	How are privileged system administration accounts managed? Describe the procedures governing the issuance (including emergency usage), protection, maintenance and destruction of these	*Various parts of the APRA Prudential Practice Guide: Management of Security Risk in Information and Information Technology deal with privileged system administration accounts. For example, it lists "administration or other privileged access to sensitive or critical IT assets" as one of several "examples where increased authentication strength is typically required, given the risks involved".* 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

Ref.	Question / requirement	Guidance
	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).	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 https://www.microsoft.com/en-us/trustcenter/security/identity. 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
41.	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.	*APRA Prudential Practice Guide: Management of Security Risk in Information and Information Technology states that "a regulated institution would typically deploy… [audit logging and monitoring of access to IT assets by all users] to limit access to IT assets, based on a risk assessment".* 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.
42.	Are the audit/activity logs protected against tampering by users with privileged accounts? Describe the safeguards implemented.	*As above, audit logging and security of privileged accounts are dealt with in the APRA Prudential Practice Guide: Management of Security Risk in Information and Information Technology.* 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.
43.	Is access to sensitive files, commands and services restricted and protected from manipulation? Provide details of	*APRA Prudential Practice Guide: Management of Security Risk in Information and Information Technology: "A key requirement for ensuring IT security is an effective process for providing access to IT assets".* 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.

Ref.	Question / requirement	Guidance
	controls implemented.	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 https://www.microsoft.com/en-us/trustcenter/security/identity.
44.	What remote access controls are implemented?	*APRA Prudential Practice Guide: Management of Security Risk in Information and Information Technology lists "remote access (i.e. via public networks) to sensitive or critical IT assets" as being one of several "examples where increased authentication strength is required".* 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

Ref.	Question / requirement	Guidance
		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 https://www.microsoft.com/en-us/trustcenter/security/identity.
45.	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?	*Various obligations regarding disaster recovery and business continuity management that apply to financial institutions are set out in the APRA Prudential Standard: Business Continuity Management. These requirements apply whether or not activities are outsourced to third party service providers such as Microsoft. Your Microsoft Account Manager can assist with any questions about Microsoft's disaster recovery arrangements and how they would interface with those of your institution.* Yes. Microsoft makes every effort to minimise service disruptions, including by implementing physical redundancies at the disk, 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. Microsoft also maintains 24/7 on-call engineering teams for assistance. See Financial Services Compliance Program and Premier Support; see also Office 365 Support; Premier Support for Enterprise; and Azure Support Plans. • *Redundancy*. Microsoft maintains physical redundancy at the server, data centre, 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. o For Office 365, Microsoft maintains multiple copies of customer data across data centres for redundancy.

Ref.	Question / requirement	Guidance
		○ For Azure, Microsoft may copy customer data between regions within a given geography for data redundancy or other operational purposes. For example, Azure GRS replicates certain data between two regions within the same geography for enhanced data durability in case of a major data centre disaster. • *Resiliency*. To promote data resiliency, Microsoft's 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. • *Distributed Services*. Microsoft also offers distributed component services like Exchange Online, SharePoint Online, and Lync Online to limit the scope and impact of any failures of a single component. Directory data is also replicated across component services to insulate one service from another in the event of a failure. • *Monitoring*. Microsoft's Online Services include internal monitoring to drive automatic recovery; outside-in monitoring to raise alerts about incidents; and extensive diagnostics for logging, auditing, and granular tracing. • *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's 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. • *Continuous Learning*. If an incident occurs, Microsoft conducts a thorough post-incident review. This post-incident review consists of an analysis of the events that occurred, Microsoft's response, and Microsoft's plan to prevent a

Ref.	Question / requirement	Guidance
		similar problem from occurring in the future. Microsoft will share the post-incident review with any organization affected by the service incident. • *Disaster Recovery Tests*. Microsoft conducts disaster recovery tests at least once per year.
46.	What are the recovery time objectives (RTO) of systems or applications outsourced to the service provider?	*APRA Prudential Standard: Business Continuity Management states that a financial institution "must identify and document appropriate recovery objectives and implementation strategies". No maximum RTO is specified.* The RTO for each Microsoft Online Service is specified in the Service Level Agreement (SLA) here: http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=37 For example: • **Microsoft Exchange Online:** 1 hour or less • **SharePoint Online:** 6 hours or less • **Virtual Machines and Storage:** 30 minutes or less • **Virtual Network:** 1 hour or less
47.	What are the recovery point objectives (RPO) of systems or applications outsourced to the service provider?	*APRA Prudential Standard: Business Continuity Management states that a financial institution "must identify and document appropriate recovery objectives and implementation strategies". No maximum RPO is specified.* • **Office 365:** Peer replication between data centres 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

Ref.	Question / requirement	Guidance
		are replicated in near real-time. Information on each Office 365 service available from the Office 365 Trust Center: https://www.microsoft.com/en-us/trustcenter/cloudservices/office365 o 45 minutes or less for Microsoft Exchange Online o 2 hours or less for SharePoint Online • **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 o 1 minute of less for Virtual Storage
48.	What are the data backup and recovery arrangements for your organisation's data that resides with the service provider?	*APRA Prudential Practice Guide: Management of Security Risk in Information and Information Technology: "APRA envisages that a regulated institution would regularly backup critical and sensitive IT assets, regardless of the level of resilience in place".* **Redundancy** • Physical redundancy at server, data centre, 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 centre disaster. **Resiliency**

Ref.	Question / requirement	Guidance
		• 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. **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.

Ref.	Question / requirement	Guidance
		• Standard built-in management mechanism. **<u>Human Backup</u>** • 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. **<u>Continuous Learning</u>** • 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. **<u>Disaster recovery tests</u>** • Microsoft conducts disaster recovery tests at least once per year.
49.	How frequently does the service provider conduct disaster recovery tests?	*APRA Prudential Standard: Business Continuity Management: "A regulated institution must review and test its BCP at least annually, or more frequently if there are material changes to business operations".* Microsoft conducts disaster recovery tests at least once per year. By way of background, Microsoft maintains physical redundancy at the server, data center, 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.

Ref.	Question / requirement	Guidance
		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's 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.
F. PRIVACY ***In addition to the sector-specific requirements imposed by APRA, the financial institution also needs to comply with the Privacy Act 1988 (Cth) in respect of any personal information disclosed to Microsoft by the financial institution in the course of providing the Microsoft cloud services.***		
50.	Will use of the cloud service enable the institution to continue complying with the Australian Privacy Principles?	*The **Australian Privacy Principles** set out in the Privacy Act 1988 (Cth) will generally apply to personal information collected by financial institutions.* Yes. The Australian Privacy Principles Amendment states that Microsoft will comply with the Australian Privacy Principles in respect of any personal information hosted by Microsoft while providing the cloud services. Microsoft has prepared a mapping document which indicates how Microsoft's compliance with ISO/IEC 27018 enables the customer to continue to comply with its

Ref.	Question / requirement	Guidance
		key privacy obligations under the Privacy Act (including, for example, processing personal data in accordance with the customer's instructions only). This is available at: http://aka.ms/australiaisoprivacylaw.
51.	Does the service provider agree to comply with the Australian Privacy Principles?	*The financial institution is likely to be accountable for downstream use of the personal information by its service providers and, for information transferred outside of Australia, the financial institution will need to ensure that it obtains sufficient commitments from its service provider to ensure that it complies with the Australian Privacy Principles.* Yes. The Australian Privacy Principles Amendment states that Microsoft will comply with the Australian Privacy Principles in respect of any personal information hosted by Microsoft while providing the cloud services. More general principles that are expressly stated in the Microsoft online services contract include commitments that: • Microsoft will use customer data only for the purposes of providing the services; • customers retain all rights in, and effective control of, their data; • customers can extract, verify, amend or delete their data at any time; • Microsoft will not provide any third party access to customer data except as directed by a customer or required by law; and • after a customer terminates its use of the service, customer data is held for at least 90 days to allow data to be extracted or migrated to a new service, and after this period it is deleted. The Microsoft online services contract also includes the standard contractual data protection clauses created by the European Union (called the "EU Model Clauses"), and the contract has also expressly been endorsed by the Article 29 Working Group (which comprises representatives from the Data Protection Authorities of the EU member states). Microsoft is also committed to GDPR compliance across their cloud services, and that is why we provide GDPR related assurances in our contractual commitments. More information regarding GDPR compliance can be found here.

Ref.	Question / requirement	Guidance
		Microsoft's contractual commitments, in combination with its independent certification process and the functionality of the Microsoft online services, collectively represent binding commitments which meet the threshold required by the Australian Privacy Principles.
52.	How will the financial institution ensure that it complies with its reporting obligations under the Notifiable Data Breach scheme in respect of personal information managed by the service provider?	*Financial institutions will be required to comply with the Notifiable Data Breach scheme, set out in the Privacy Act 1988 (Cth), in respect of personal information that is managed by its service providers on basis that they retain the right to deal with such personal information. Under the Notifiable Data Breach scheme, if a financial institution experiences an eligible data breach then, unless an exemption applies, it must report the breach (in the prescribed form) to the Office of the Australian Information Commissioner and the individuals affected by the breach.* Similar to the breach notifications to APRA discussed in item 35 above, Microsoft supports compliance through its "*Security Incident Notification*" commitments in the Online Services Terms. These are excerpted in item 33. When Microsoft notifies the financial institution of an information security incident, the financial institution must determine whether it has reasonable grounds to believe that there has been an eligible data breach for the purposes of the Privacy Act 1988 (Cth). If so and no exemption applies to the breach, the financial institution must notify the Office of the Australian Information Commissioner and the individuals affected by the breach as soon as practicable, in accordance with the Privacy Act 1988 (Cth). Furthermore, the optional Financial Services Compliance Program provides for deeper information sharing by Microsoft about information security incidents and potential threats, including their nature, common causes and resolutions. It is important to note that security incident monitoring is a shared responsibility. Microsoft cloud customers are responsible to detect and report eligible data breaches, and are not dependent upon Microsoft to detect or report those incidents. Microsoft provides the tools and resources outlined in item 33 above to empower our customers to identify security concerns and detect security incidents.

Part 2: Contract Checklist

What are our contract documents?

Section 28 of the Outsourcing Standards requires that all outsourcing arrangements must be contained in a documented legally binding agreement, signed by all parties to it before the outsourcing arrangement commences. There are various parts to your signed contract with Microsoft. Your Microsoft Account Manager can walk you through the relevant parts if helpful. 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.	Online Service Terms (**OST**), incorporating the Data Protection Terms (**DPT**) including GDPR terms; **Product Terms** Online Services Service Level Agreement (**SLA**).
Amendment provided by Microsoft to add to core contract documents for financial services customers **Financial Services Amendment**	**Supporting documents and information that do not form part of the contract**[2] Materials available from the **Trust Center**

What does this Part 2 cover?

Section 29 of the Outsourcing Standards 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, and the third column indicates how and where in the Microsoft contractual documents the mandatory requirement is covered.

[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?
Section 29(a), Outsourcing Standards	(a) The scope of the arrangement and services to be supplied	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 OST, particularly in the OST "Core Features" commitments.
Section 29(b), Outsourcing Standards	(b) Commencement and end dates	Standard EA Enrollments have a three-year term and may be renewed for a further three-year term.
Section 29(c), Outsourcing Standards	(c) Review provisions	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 DPT (in the OST) specifies the control standards and frameworks that Microsoft will comply with for each Online Service. The DPT 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.
Section 29(e), Outsourcing Standards	(d) 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.

Reference	Requirement	How and where is this dealt with in Microsoft's contract?
Section 29(f), Outsourcing Standards	(e) 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.
Section 29(f), Outsourcing Standards	(f) The form in which data is to be kept and clear provisions identifying ownership and control of data	Under the OST, 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. 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. 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. 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.

Reference	Requirement	How and where is this dealt with in Microsoft's contract?
		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. 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. The MBSA deals with confidentiality. 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.
Section 29(g), Outsourcing Standards	(g) Reporting requirements, including content and frequency of reporting	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. In the OST, 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 measure compliance against Microsoft's standards certifications.
Section 29(h), Outsourcing Standards	(h) Audit and monitoring procedures	The DPT 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's 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 DPT 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

Reference	Requirement	How and where is this dealt with in Microsoft's contract?
		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 Portal 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 APRA. 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**

Reference	Requirement	How and where is this dealt with in Microsoft's contract?
		On behalf of the customer, Microsoft will cause the performance of audits of the security of the computers, computing environment and physical data centres 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. In relation to the Outsourcing Standards requirement that requires the regulated entity to obtain examination and access rights from the service provider, Microsoft believes that the Financial Services Amendment meets this requirement.
Section 29(i), Outsourcing Standards	(i) Business continuity management	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 DPT in the OST). Business continuity management also forms part of the scope of Microsoft's industry standards compliance commitments and regular third party compliance audits.
Section 29(j), Outsourcing Standards	(j) Confidentiality, privacy and security of information	The contractual documents include various confidentiality, privacy and security protections: • The Australian Privacy Principles Amendment states that Microsoft will comply with the Australian Privacy Principles in respect of any personal information hosted by Microsoft while providing the cloud services. • As set out under Section 29(f), above, Microsoft will deal with customer data in accordance with the OST and makes various commitments in this respect.

Reference	Requirement	How and where is this dealt with in Microsoft's contract?
		• Microsoft commits to reimburse customer mitigation costs incurred as a consequence of a security incident involving customer data (see Financial Services Amendment and OST 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 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: 1. 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. 2. 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. 3. Microsoft has implemented and will maintain appropriate technical and organisational measures, internal controls, and information security routines intended to protect your data against accidental, unauthorised or unlawful access, disclosure, alteration, loss, or destruction. Technical support personnel are only permitted to have access to customer information when needed.

Reference	Requirement	How and where is this dealt with in Microsoft's contract?
		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. 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 (see OST).
Section 29(k), Outsourcing Standards	(k) Default arrangements and termination provisions	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. 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.
Section 29(l), Outsourcing Standards	(l) 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. The MBSA contains terms that describe how a dispute under the contract is to be conducted.

Reference	Requirement	How and where is this dealt with in Microsoft's contract?
Section 29(m), Outsourcing Standards	(m) Liability and indemnity	The MBSA contains clauses which deal with liability. The MBSA sets out Microsoft's obligation to defend the regulated entity against third party infringement claims.
Section 29(n), Outsourcing Standards	(n) Sub-contracting	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 conduct as if it was Microsoft's. Microsoft's obligations in the OST, which Microsoft considers complies with section 30 of the Outsourcing Standards[3]. 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 https://www.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 (see DPT in the OST). 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.

[3] Section 30 of the Outsourcing Standards provides: "*A regulated institution that outsources a material business activity must ensure that its outsourcing agreement includes an indemnity to the effect that any subcontracting by a third-party service provider of the outsourced function will be the responsibility of the third-party service provider, including liability for any failure on the part of the sub-contractor*."

Reference	Requirement	How and where is this dealt with in Microsoft's contract?
		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. (see DPT in the OST)
Section 29(o), Outsourcing Standards	(o) 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, Section 1 above).
Section 29(p), Outsourcing Standards	(p) To the extent applicable, offshoring arrangements (including through subcontracting)	The DPT provides commitments on the location at which Microsoft will store customer data at rest. Microsoft also makes GDPR specific commitments (Attachment 4, OST) to all customers. Microsoft notes that APRA has the power under the Outsourcing Standards to direct the regulated entity to cease using the outsourced service. In the unlikely event that this occurs in relation to Microsoft cloud services, Microsoft has equivalent on-premises products that the customer can use itself or host with a Microsoft partner (there are several partners located in Australia). The customer also has the flexibility to maintain a hybrid solution, which involves part of its business using on-premises and part of its business using online services, with a consistent interface and experience for all users.

Further Information

- **Australian Regulatory Compliance for Financial Services Customers: aka.ms/aufs**
- **Asia Regulatory Compliance for Financial Services Customers: aka.ms/asiafs**
- **Trust Center: microsoft.com/trust**
- **Service Trust Portal: aka.ms/trustportal**
- **Microsoft's response to APRA's 2018 Information Paper on Cloud: aka.ms/apraresponse**
- **ISO 27018 and Australian Privacy Compliance: aka.ms/australiaisoprivacylaw**
- **Customer Stories: customers.microsoft.com**
- **Online Service Terms: microsoft.com/contracts**
- **Service Level Agreements: microsoft.com/contracts**
- **SAFE Handbook: aka.ms/safehandbook**