AUSTRALIA

GUIDANCE ON COMPLYING WITH REGULATORY REQUIREMENTS APPLICABLE TO FINANCIAL SERVICES INSTITUTIONS USING CLOUD COMPUTING (AZURE)

Last updated: November 2014.

1. WHAT DOES THIS GUIDANCE CONTAIN?

This guidance document provides a guide to complying with the regulatory process and requirements applicable to financial services institutions using cloud computing. In this guidance financial services institutions means ADIs, including foreign ADIs, and authorized banking NOHCs, all general insurers, including Category C insurers, and authorized insurance NOHCs, and all life companies, including friendly societies and eligible foreign life insurance companies (EFLICs), and registered life NOHCs ("**FSIs**").

Sections 2 to 6 of this guidance sets out information about the regulatory process and the regulations that apply.

Section 7 sets out questions in relation to outsourcing to a cloud services solution based on the laws, regulations and guidance that are relevant to the use of cloud services. Although there is no requirement to complete a checklist like this one, we have received feedback from FSIs that a checklist approach like this is very helpful. The checklist can be used:

(i) as a checklist for ensuring regulatory compliance with the requirements set out in the laws, regulations and guidelines (listed in Section 2); and

(ii) as a tool to aid discussions with the regulator(s) (listed in Section 3), should they wish to discuss your organization's overall approach to compliance with their requirements.

Appendix Two also contains a list of the mandatory contractual requirements required by relevant regulation.

Note that this document is not intended as legal or regulatory advice and does not constitute any warranty or contractual commitment on the part of Microsoft or its affiliates. Instead, it is intended to streamline the regulatory process for you. You should seek independent legal advice on your technology outsourcing project and your legal and regulatory obligations. If you have any questions, please do not hesitate to get in touch with your Microsoft contact.

2. WHAT LAWS, REGULATIONS AND GUIDANCE ARE RELEVANT?

APRA is not against outsourcing or the use of cloud services. However, although there are no forms that must be completed, there are certain requirements that FSIs should be aware of. In particular:

- APRA Prudential Standard: Outsourcing (**"Outsourcing Guidelines"**);
- APRA Prudential Practice Guide: Outsourcing;
- APRA Prudential Practice Guide: Management of Security Risk in Information and Information Technology; and
- APRA Prudential Standard: Business Continuity Management.

3. WHO IS/ARE THE RELEVANT REGULATOR(S)?

The Australian Prudential Regulatory Authority ("**APRA**")

4. IS REGULATORY APPROVAL REQUIRED IN AUSTRALIA?

No.

APRA does not require approval before FSIs outsource IT functionality to a cloud services solution such as Microsoft Azure. However, FSIs (other than regulated superannuation entities) must notify APRA after entering into agreements to outsource material business activities (within Australia) or consult with APRA before outsourcing a material business activity to a service provider outside of Australia. More information about what types of business activities are considered "material" can be found in the Fact Sheet attached at Appendix One.

5. IS/ARE THERE (A) SPECIFIC FORM(S) OR QUESTIONNAIRE(S) TO BE COMPLETED?

No.

Unlike in certain jurisdictions, such as Singapore, there are no specific forms or questionnaires that an FSI must complete when considering cloud computing solutions.

6. DOES THE REGULATOR MANDATE SPECIFIC CONTRACTUAL REQUIREMENTS THAT MUST BE ADOPTED?

Yes.

APRA does stipulate some specific points that FSIs must ensure are incorporated in their outsourcing contracts. These are set out in section 25 of the Outsourcing Guidelines. We have incorporated responses to these points in the main document, together with some other points raised in APRA guidance regarding the content of the outsourcing contract which are “for consideration” rather than being mandatory requirements. In Appendix Two we have mapped the specific requirements against the sections in the Microsoft document where you will find them addressed.

7. CHECKLIST

Key:

In blue text, Microsoft has included template responses that would demonstrate how your proposed use of Microsoft's services would address the point raised in the checklist. The suggested responses may provide sufficient detail but if you require further information, Microsoft will be happy to provide this if you get in touch with your Microsoft contact. Some points are specific to your own internal operations and processes and you will need to complete these answers as well.

In *red italics*, Microsoft has provided guidance to assist you with the points in the checklist.

Ref.	Question/requirement	Template response and guidance
A. OVERVIEW ***This section provides a general overview of the Microsoft Azure solution.***		
1.	Who is the service provider?	The service provider is Microsoft Operations Pte Ltd, the regional licensing entity for 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: https://www.microsoft.com/en-us/news/inside_ms.aspx.
2.	What activities and operations will be outsourced to the service provider?	• Compute • Data & Storage • Networking • Identity & Access Management

Ref.	Question/requirement	Template response and guidance
		- IT support services
3.	What type of cloud services would your organization be using?	*APRA guidance does not distinguish between different types of cloud solution but an understanding of the type of solution (i.e. multi-tenant or dedicated) is relevant for your organization's own risk management purposes.* Microsoft's "Azure" service, which is described in more detail here: Azure. Azure is a multi-tenant service. It hosts multiple tenants in a secure way through logical data isolation/separation. Data storage and processing for each tenant is segregated through Active Directory structure and capabilities specifically developed to help build, manage, and secure multi-tenant environments. Active Directory isolates customers using security boundaries (also known as silos). This safeguards a customer's data so that the data cannot be accessed or compromised by co-tenants.
4.	Will the proposed outsourcing require offshoring? If so, from which territory(ies) will the outsourced cloud services be provided?	*The Outsourcing Guidelines, sections 35 and 36, state that a regulated institution must consult with APRA before entering into any offshoring agreement involving a material business activity so that APRA can satisfy itself that the impact of the offshoring arrangement has been adequately addressed as part of the risk management framework.The answer to this question will depend on the region you are in. You may discuss this with your Microsoft contact. Microsoft enables customers to select the region that it is provisioned from.* Yes. Microsoft informs us that it takes a regional approach to hosting of Azure data. Microsoft is transparent in relation to the location of our data. Microsoft data center locations are made public on the Microsoft Trust Center. *Microsoft enables customers to select the region that it is provisioned from. Under the OST, Microsoft*

<table>
<tr><th>Ref.</th><th>Question/requirement</th><th>Template response and guidance</th></tr>
<tr><td></td><td></td><td>

commits that if a customer provisions its tenant in the United States or EU, Microsoft will store the customer's data at rest in the United States or EU, as applicable.

The table below will need to be amended depending on the specific solution that you are taking up.

<table>
<tr><th>#</th><th>Locations of Data Centre</th><th>Classification of DC: Tier I, II, III or IV</th><th>Storing your organization's data (Y/N)</th></tr>
<tr><td>1.</td><td></td><td></td><td></td></tr>
<tr><td>2.</td><td></td><td></td><td></td></tr>
</table>

See section B, below, for more information on how the offshoring risk is managed.

</td></tr>
<tr><td>5.</td><td>What data will be processed by the service provider on behalf of the FSI?</td><td>

Various APRA guidelines focus on the risks associated with data processing. For example, the "Prudential Practice Guide: CPG 235 – Managing Data Risk". Clearly, therefore, it is important to understand what data will be processed through the use of Azure. You will need to tailor this section depending on what data you intend to store or process within Azure.

- 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

</td></tr>
</table>

Ref.	Question/requirement	Template response and guidance
		organization). • Transaction data (data relating to transactions in which the organization is involved). • Indices (for example, market feeds). • Other personal and non-personal data relating to the organization's business operations as an FSI. We ensure, pursuant to the terms of the contract in place with the service provider, that all data (but in particular any customer data) is treated with the highest level of security so that we can continue to comply with our legal and regulatory obligations and our commitments to customers. We do of course only collect and process data that is necessary for our business operations in compliance with all applicable laws and regulation and this applies whether we process the data on our own systems or via a cloud solution such as Microsoft Azure.

B. OFFSHORING

Microsoft's data centers are located outside of Australia . APRA must satisfy itself that the impact of the offshoring has been adequately managed by the FSI. This section looks at how Azure helps organizations to manage the impact of an offshoring.

		Risk flagged by APRA	**How Microsoft Azure addresses this**
6.	APRA considers that an offshoring arrangement "can give rise to a number of particular risks" How does the Microsoft Azure solution help organizations to manage these risks?	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	*APRA Prudential Practice Guide: Outsourcing, section 24 The answer to this question will depend on the region you are in. You may discuss this with your Microsoft contact. Microsoft enables customers to select the region that it is provisioned from.*

Ref.	Question/requirement	Template response and guidance	
		continue to provide an outsourced service to the regulated institution.	Azure is hosted out of [.....]. This/These location(s) has/have been vetted for geopolitical/socioeconomic risks as set out in this checklist requirement. As part of our usual processes, we constantly monitor the countries in which we operate. a. **Political (i.e. cross-broader conflict, political unrest etc.).** Azure offers data-location transparency so that the organizations and regulators are informed of the jurisdiction(s) in which data is hosted. We are confident that Microsoft's data center locations offer extremely stable political environments. b. **Country/socioeconomic.** Azure offers data-location transparency so that the organizations and regulators are informed of the jurisdiction(s) in which data is hosted. The centers are strategically located around the world taking into account country and socioeconomic factors. We are confident that Microsoft's data center locations offer extremely stable socioeconomic environments. See also the response to question 7, below.
		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	*APRA Prudential Practice Guide: Outsourcing, section 24. If this is a particular concern, Microsoft recommends that you obtain a legal opinion from an international or other reputable legal firm in your data center location on this matter..* We will have in place a binding negotiated contractual agreement

Ref.	Question/requirement	Template response and guidance	
		(including accounting practices).	with Microsoft in relation to the outsourced service, giving us direct contractual rights. We also took into account the fact that Azure was built based on ISO/IEC 27001 standards, a rigorous set of global standards covering physical, logical, process and management controls. Finally, we took into account the fact that Microsoft offers access and regulator audit rights thereby allowing us to comply with our regulatory obligations in this respect.We also took into account the fact that the European Union's data protection authorities have found that Microsoft's enterprise cloud contracts meet the high standards of EU privacy law. Microsoft is the first – and so far the only – company to receive this approval.
		Contractual risk — the risk that the regulated institution's ability to enforce the offshoring agreement may be limited or completely negated.	*APRA Prudential Practice Guide: Outsourcing, section 24.* The fact that Microsoft, the service provider, is an international organization with a presence in many countries around the world (including Australia) should provide comfort that we could enforce the agreement, should the need arise. See also Appendix Two for details of how the Microsoft contract meets the APRA requirements.
		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	*APRA Prudential Practice Guide: Outsourcing, section 24 and Outsourcing Guidelines, section 30.* **Obtaining information and access:** There are provisions in the contract that enable APRA to carry out inspection or examination of Microsoft's facilities, systems, processes and data relating to the services. This is a key advantage of the Microsoft product over

Ref.	Question/requirement	Template response and guidance	
		gain access to the service provider and the material business activity being conducted for prudential review purposes.	competitor products, which often provide only very limited (or no) audit and inspection rights. **Ability to retain records:** Microsoft offers contractually-guaranteed uptime, hosted out of world class data centers with physical redundancy at disk, NIC, power supply and server levels, constant content replication, robust backup, restoration and failover capabilities, 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, with 24/7 on-call engineering teams.
		Counterparty risk — the risk arising from the obligor's failure to meet the terms of any agreement with the regulated institution or to otherwise perform as agreed.	*APRA Prudential Practice Guide: Outsourcing, section 24.* See response to next question.
7.	How is the issue of counterparty risk in offshoring addressed through your choice of service provider?	*APRA Prudential Practice Guide: Outsourcing, section 24.* **a. Competence and experience.** Microsoft is an industry leader in cloud computing. Azure was built based on ISO/IEC 27001 standards and was the first major business productivity public cloud service to have implemented the rigorous set of global standards covering physical, logical, process and management controls. **b. Past track-record.** 40% of the world's top brands use Azure. We consulted various case studies	

Ref.	Question/requirement	Template response and guidance
		relating to Azure, which are available on the Microsoft website and also considered the fact that Microsoft has amongst its customers some of the world's largest organizations and financial institutions. 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 Azure meets their respective regulatory requirements. This gives us confidence that Microsoft is able to help meet the high burden of financial services regulation and is experienced in meeting these requirements. d. **Microsoft's staff hiring and screening process.** All personnel with access to customer data are subject to background screening, 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. User access to data is also limited by user role. For example, system administrators are not provided with database administrative access. e. **Financial strength of Microsoft.** Microsoft Corporation is publicly-listed in the United States and is amongst the world's largest companies by market capitalization. Microsoft's audited financial statements indicate that it has been profitable for each of the past three years. Its market capitalization is in the region of USD 280 billion. Accordingly, we have no concerns regarding its financial strength. f. **Business resumption and contingency plan.** Microsoft offers contractually-guaranteed uptime, hosted out of world class data centers, with physical redundancy at disk, NIC, power supply and server levels, constant content replication, robust backup, restoration and failover capabilities, real-time issue detection and automated response such that workloads can be moved off any failing

Ref.	Question/requirement	Template response and guidance
		infrastructure components with no perceptible impact on the service, with 24/7 on-call engineering teams. **g. Security and internal controls, audit, reporting and monitoring.** Microsoft is an industry leader in cloud security and implements policies and controls on par with or better than on-premises data centers of even the most sophisticated organizations. We have confidence in the security of the solution and the systems and controls offered by Microsoft. In addition to the ISO/IEC 27001 certification, Azure is designed for security with controls for encryption of data at rest and SSL/TLS encryption of data in transit. The Microsoft service is subject to the SSAE16 SOC1 Type II audit, an independent, third party audit.
8.	What other risks have been considered in relation to the proposed offshoring arrangement?	*APRA Prudential Practice Guide: Outsourcing, section 25: "Typically, these and other risks would be specifically addressed during the preparation of a business case, when conducting due diligence and during contract negotiations".* **a. Infrastructure/security/terrorism** Microsoft's data centers are built to exacting standards, designed to protect customer data from harm and unauthorized access. Data center access is restricted 24 hours per day by job function so that only essential personnel have access. 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 centers are monitored using motion sensors, video surveillance and security breach alarms. **b. Environmental (i.e. earthquakes, typhoons, floods)** Microsoft data centers are built in seismically safe zones. Environmental controls have been

Ref.	Question/requirement	Template response and guidance	
		implemented to protect the data centers including temperature control, heating, ventilation and air-conditioning, fire detection and suppression systems and power management systems, 24-hour monitored physical hardware and seismically-braced racks. These requirements are covered by Microsoft's ISO/IEC 27001 accreditation for Azure.	
C. COMPLIANCE WITHIN YOUR ORGANIZATION ***APRA requires that FSIs have internal mechanisms and controls in place to properly manage the outsourcing. Although this is a matter for each organization, Microsoft provides some suggested approaches in this section, based on its experience of approaches taken by its customers. Ultimately this will of course need to be tailored for the FSI in question.***			
9.	The FSI 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 FSI comply?	*This section sets out each of the steps required by APRA under the Outsourcing Guidelines, section 22. Where possible, Microsoft has suggested a response, although in most cases the appropriate response depends on your organization's internal procedures.* Has your organization:	
		prepared a business case for outsourcing the material business activity;	*Outsourcing Guidelines, section 22(a). You will need to provide your business case for the use of Azure. Where appropriate, this could include reference to some of the key benefits of Azure, which are as follows:* Yes. As part of the business case, we considered some of the key benefits of

Ref.	Question/requirement	Template response and guidance	
			Azure, namely: • **Enterprise-class security and reliability.** One of the best aspects of the cloud is that it makes enterprise-class technologies, as well as their associated benefits, available at a price that smaller companies can afford. For instance, numerous layers of security help protect Azure's data centers; stringent privacy policies help keep our data safe. Additionally, the data centers provide first-rate disaster recovery capabilities, are fully redundant and are geographically dispersed to help ensure our data is available. This means no more worrying about what would happen to our network should natural disasters or other unforeseen complications occur - with Azure, we get a financially backed guaranteed uptime. • **IT control and efficiency.** On any given day, basic IT management tasks like retaining security updates and upgrading back-end systems occupy a great deal of our IT workers' time, preventing them from focusing their energy on business priorities. Azure will handle tasks like these, while still giving our IT staff control over user management and service configuration. • **User familiarity and productivity.** Creating an Azure workspace doesn't necessarily result in a large learning curve for employees. If our business already uses programs like Microsoft Office, Outlook, SharePoint and others, our employees will merely be transitioning to a similar, but cloud-based experience. Moreover,

Ref.	Question/requirement	Template response and guidance	
			since these programs are hosted on the cloud, employees can access information while on the go, from any laptop, PC or Smartphone, depending on Wi-Fi capability or phone network availability.
		undertaken a tender or other selection process for service providers;	*Outsourcing Guidelines, section 22(b). You will need to describe what selection process you had in place.*
		undertaken a due diligence review of the chosen service provider;	*Outsourcing Guidelines, section 22(c). You will need to describe your due diligence process. As part of this, you could mention some of the items listed in question 7, above (e.g. regarding Microsoft's past track record). You could also mention that as part of Microsoft's certification requirements, they are required to undergo regular independent third party auditing and Microsoft shares with its customers the independent third party audit reports. The third party audit carried out in relation to Microsoft's services is SSAE16 SOC1 Type II.*
		Involved the Board, Board committee, or senior manager with delegated authority from the Board, in approving the agreement;	*Outsourcing Guidelines, section 22(d). 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.*
		considered all of the minimum contractual requirements required by	*Outsourcing Guidelines, section 22(e).*

Ref.	Question/requirement	Template response and guidance	
		APRA;	Yes. These are set out in Appendix Two, below.
		established procedures for monitoring performance under the outsourcing agreement on a continuing basis;	*Outsourcing Guidelines, section 22(f).* Yes. See response to question 12, below.
		addressed the renewal process for outsourcing agreements and how the renewal will be conducted; and	*Outsourcing Guidelines, section 22(g).* Yes. The outsourcing agreement with Microsoft runs on an ongoing basis but we have the right to terminate for convenience at any time. As such, there is no formal renewal process to be conducted but we have flexibility.
		developed contingency plans that would enable the outsourced business activity to be provided by an alternative service provider or brought in-house if required?	*Outsourcing Guidelines, section 22(h).* As above – the outsourcing agreement with Microsoft allows us to terminate for convenience at any time, which would enable it to bring the activity in-house or to be provided by an alternative service provider if required.

Ref.	Question/requirement	Template response and guidance
10.	Does the FSI have a policy, approved by the Board, relating to the outsourcing?	*APRA requires that FSIs have a Board-approved policy in relation to the outsourcing, which must "set out its approach to outsourcing of material business activities, including a detailed framework for managing all such outsourcing arrangements" (Outsourcing Guidelines, section 18). The appropriate policy will depend on the organization in question but will typically include:* • *a framework to identify, assess, manage, mitigate and report on risks associated with the outsourcing to ensure that the organization 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.*
11.	What procedures does the FSI have in place to ensure that all its relevant business units are fully aware of, and comply with, the outsourcing policy?	*You will need to explain how the relevant business units are brought under the scope of the outsourcing policy.*

Ref.	Question/requirement	Template response and guidance
12.	What monitoring processes does the FSI have in place to manage the outsourcing?	*APRA requires that FSIs 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 "template response" below explains how the Azure dashboard could be used by your organization as part of these monitoring processes.* We have reviewed the monitoring processes (set out in more detail in the following paragraphs) and we are confident that appropriate processes are in place. Microsoft's Service Level Agreement applies to the Azure product. Our IT administrators also have access to the Azure Service Health Dashboard, which provides real-time and continuous monitoring of the Azure service. The Service Health Dashboard provides our IT administrators with information about the current availability of each service or tool (and history of availability status) details about service disruption or outage, scheduled maintenance times. The information is provided via an RSS feed. Amongst other things, it provides a contractual uptime guarantee for the Azure product and covers performance monitoring and reporting requirements which enable us to monitor Microsoft's performance on a continuous basis against service levels. We also have access to the independent SSAE16 SOC1 Type II audit, which enables us to verify their performance. Please find a copy of the SLA at: http://azure.microsoft.com/en-us/support/legal/sla/ As part of the support we receive from Microsoft, we also have access to a technical account manager who is responsible for understanding our challenges and providing expertise, accelerated support and strategic advice tailored to our organization. This includes both continuous hands-on assistance and immediate escalation of urgent issues to speed resolution and keep mission-critical systems functioning.

Ref.	Question/requirement	Template response and guidance
		We are confident that such arrangements provide us with the appropriate mechanisms for managing performance and problems.
13.	How does the FSI ensure that it maintains ultimate responsibility for any outsourcing?	The handing over of certain day to day responsibility to an outsourcing provider does present some challenges in relation to control. Essential to us is that, despite the outsourcing, we retain control over our own business operations, including control of who can access data and how they can use it. At a contractual level, we have dealt with this via our contract with Microsoft, which provides us with legal mechanisms to manage the relationship including appropriate allocation of responsibilities, oversight and remedies and the mandatory provisions required by APRA. At a practical level, we have selected the Azure product since it provides us with control over data location, authentication and advanced encryption controls. We (not Microsoft) will continue to own and retain all rights to our data and our data will not be used for any purpose other than to provide us with the Azure services. As part of Microsoft's certification requirements, they are required to undergo regular independent third party auditing (via the SSAE16 SOC1 Type II audit, a globally-recognized standard), and Microsoft shares with us the independent third party audit reports. We are confident that all of these arrangements ensure that we maintain ultimate responsibility for this outsourcing arrangement.
D. OUTSOURCING AGREEMENT ***Note: See also Appendix Two of this guidance document for a list of the standard contractual terms that APRA mandates should 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 suggests are considered as part of the contractual negotiation but which are not necessarily mandatory contractual terms that should be included in all cases.***		
14.	Are the outsourcing arrangements contained in a documented legally binding agreement	*This is a requirement of the Outsourcing Guidelines, section 24.*

Ref.	Question/requirement	Template response and guidance
	that is signed by all parties?	Yes. The arrangements are all documented in the Microsoft contractual documents, which are legally binding and signed both on behalf of Microsoft and on behalf of our organization. The provision of Azure is subject to the following contractual documents: • Microsoft Online Business and Services Agreement (a copy of which is available on request); • Service Level Agreement, a copy of which is available at: http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=37; and • various ancillary documents (copies of which are available on request).
15.	Does the outsourcing agreement address the following matters: (a) the scope of the arrangement and services to be supplied; (b) commencement and end dates; (c) review provisions; (d) pricing and fee structure;	*As mandated by the Outsourcing Guidelines, section 25. Appendix Two maps these mandatory requirements against section references in the Microsoft contractual documents. The answer to question (n) will depend on the region you are in. You may discuss this with your Microsoft contact. Microsoft enables customers to select the region that it is provisioned from.* Yes. The Microsoft contractual documents address each of these requirements. Taking each requirement in turn: **a. Scope of the arrangement and services to be supplied**

Ref.	Question/requirement	Template response and guidance
	(e) service levels and performance requirements; (f) audit and monitoring procedures; (g) business continuity management; (h) confidentiality, privacy and security of information; (i) default arrangements and termination provisions; (j) dispute resolution arrangements; (k) liability and indemnity; (l) sub-contracting; (m) insurance; and (n) to the extent applicable, offshoring arrangements (including through subcontracting)?	Yes. Full details of the services to be supplied and the scope are set out in the Microsoft contractual documents. **b. Commencement and end dates** Yes. The period of time for which Microsoft must provide the services is clearly set out. **c. Review provisions** Yes. We can monitor the performance of the online services via the administrative dashboard, which includes information as to Microsoft compliance with its SLA commitments. Microsoft also commits to providing us with a summary of its annual audit report, which is performed by an independent third party and measures compliance against Microsoft's certifications. **d. Pricing and fee structure** Yes. Details of how much we have to pay and when are set out in the contract.

Ref.	Question/requirement	Template response and guidance
		e. Service levels and performance requirements Yes. We have a detailed SLA with Microsoft. Microsoft provides a contractual financially-backed uptime guarantee for the Azure product and covers performance monitoring and reporting requirements which enable us to monitor Microsoft's performance on a continuous basis against service levels. Under the service credits mechanism in the SLA, we may be entitled to a service credit of up to 100% of the service charges. If a failure by Microsoft also constitutes a breach of contract to which the service credits regime does not apply, we would of course have ordinary contractual claims available to us too under the contract. **f. Audit and monitoring procedures** Yes. There are provisions in the contract that enable APRA to carry out inspection or examination of Microsoft's facilities, systems, processes and data relating to the services. This is a key advantage of the Microsoft product over competitor products, which often provide only very limited (or no) audit and inspection rights. **g. Business continuity management** Yes. Microsoft commits to maintain a data security policy that complies with its accreditations, which in turn

Ref.	Question/requirement	Template response and guidance
		require Microsoft to have in place appropriate business continuity management processes. **h. Confidentiality, privacy and security of information** Yes. The contract has standard confidentiality provisions, whilst Microsoft also commits to complying with applicable data privacy legislation. We also took into account the fact that the European Union's data protection authorities have found that Microsoft's enterprise cloud contracts meet the high standards of EU privacy law. Microsoft is the first – and so far the only – company to receive this approval. **i. Default arrangements and termination provisions** Yes. The contract is clear as to the obligations on Microsoft and what acts or omissions would constitute a default. We also have various termination rights, including a right to terminate the agreement for convenience at any time. **j. Dispute resolution arrangements** Yes. In the unlikely event that we ended up in a dispute with Microsoft, the governing law and jurisdiction of that dispute are clearly described in the contract.

Ref.	Question/requirement	Template response and guidance
		k. Liability and indemnity Yes. There are provisions regarding the liability of both us and of Microsoft under the contract. There are also indemnities that apply in certain situations, such as if there were a breach of confidence claim. **l. Sub-contracting** Yes. Microsoft is permitted to sub-contract but it retains overall responsibility for delivery of the services. Microsoft does not engage sub-contractors in critical path roles. **m. Insurance** Yes. This is addressed. In practice, Microsoft self-insures, and we do not believe this exposes us to any substantial risk. **n. To the extent applicable, offshoring arrangements (including through subcontracting)** Yes. The contract does include commitments as to data location.. Azure is hosted out of […..].
16.	Does the outsourcing agreement include a clause that allows APRA to access	*Outsourcing Guidelines, section 30.*

Ref.	Question/requirement	Template response and guidance
	documentation and information relating to the outsourcing arrangement?	Yes. The contract with Microsoft does permit this. This is a key advantage of the Microsoft product over competitor products, which often provide only very limited (or no) audit and inspection rights.
17.	Does the outsourcing agreement provide a guarantee of access to the minimum IT assets required to operate under a disaster scenario?	*APRA Prudential Practice Guide: Management of Security Risk in Information and Information Technology, Attachment B, section 14.* Although this is not expressly dealt with as described in the relevant section of the guidance, it is actually covered more widely through the service level obligations on Microsoft as part of the contract. The uptime guarantee given by Microsoft applies to all IT assets, not just a minimum number required to operate in a disaster situation.
18.	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, Attachment C, section 4.* Yes. As stated above, we can monitor the performance of the online services via the administrative dashboard, which includes information as to Microsoft compliance with its SLA commitments. Microsoft also commits to providing us with a summary of its annual audit report, which is performed by an independent third party and measures compliance against Microsoft's certifications.
19.	Is the outsourcing agreement sufficiently flexible to accommodate changes to existing processes and to accommodate new processes in the future to meet changing	*APRA Prudential Practice Guide: Outsourcing, section 11.* Yes.

Ref.	Question/requirement	Template response and guidance
	circumstances?	We can always order additional services if required and ultimately we also have the ability to terminate the agreement and move to another provider or to bring the service in-house.
20.	In the event of termination, do transitional arrangements address access to, and ownership of, documents, records, software and hardware, and the role of the service provider in transitioning the service?	*APRA Prudential Practice Guide: Outsourcing, section 15.* Ownership of documents, records and other data remain with our organization 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. Microsoft will retain our data for 90 days following termination so that we may extract our data. If we request that Microsoft end the retention period earlier, Microsoft will do so. As set out on page 33 of the OST, upon expiration or termination, the customer may extract its data and the Service Provider will delete the data. Additional transition arrangements are not required upon termination.
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) FSIs 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 the Azure service which should address many of the technical and operational questions that may arise in any discussions with APRA. If other questions arise, please do not hesitate to get in touch with your Microsoft contact.***		
21.	Does the service provider permit audit by the FSI and/or APRA?	*Outsourcing Guidelines, section 41.* Yes.

Ref.	Question/requirement	Template response and guidance
		There are provisions in the contract that enable APRA to carry out inspection or examination of Microsoft's facilities, systems, processes and data relating to the services. This is a key advantage of the Microsoft product over competitor products, which often provide only very limited (or no) audit and inspection rights. *Microsoft also offers a Compliance Framework Program. If you take-up the Compliance Framework Program, you may add this additional information about its key features: the regulator audit/inspection right, access to Microsoft's security policy, the right to participate at events to discuss Microsoft's compliance program, the right to receive audit reports and updates on significant events, including security incidents, risk-threat evaluations and significant changes to the business resumption and contingency plans.*
22.	Are the provider's services subject to any third party audit?	*APRA Prudential Practice Guide: Management of Security Risk in Information and Information Technology, section 74: "APRA envisages that a regulated institution would ensure audit trails exist for IT assets that…facilitate independent audit".* Yes. As part of Microsoft's certification requirements, they are required to undergo regular independent third party auditing (via the SSAE16 SOC1 Type II audit, a globally-recognized standard), and Microsoft shares with us the independent third party audit reports.
23.	What security controls are in place to protect the transmission and storage of confidential information such as customer data within the infrastructure of the service provider?	*The APRA guidance focuses on confidentiality in a number of places, both in terms of general requirements and as something that should be addressed in the outsourcing contract. For example, the APRA Prudential Practice Guide: Management of Security Risk in Information and Information Technology, section 13, states that "IT security risk…can be described as the risk of loss due to inadequate or failed internal processes, people and systems or from external events, resulting in a*

Ref.	Question/requirement	Template response and guidance
		compromise of an IT asset’s confidentiality, integrity or availability”. 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 centers of even the most sophisticated organizations. Azure was built based on ISO/IEC 27001 standards, a rigorous set of global standards covering physical, logical, process and management controls. The Microsoft Azure 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 software and services, including Azure. Through design requirements, analysis of attack surface and threat modeling, the SDL helps Microsoft predict, identify and mitigate vulnerabilities and threats from before a service is launched through its entire production lifecycle. Networks within the Azure data centers are segmented to provide physical separation of critical back-end servers and storage devices from the public-facing interfaces. Edge router security allows the ability to detect intrusions and signs of vulnerability. Azure uses industry-standard transport protocols such as SSL and TLS between user devices and Microsoft data centers, and within data centers themselves. With virtual networks, industry standard IPsec protocol can be used to encrypt traffic between the corporate VPN gateway and Azure. Encryption can be enabled for traffic between VMs and end users. 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-

Ref.	Question/requirement	Template response and guidance
		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. 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 segregation 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 scrutinized, manual-approval process. Preventing breach also involves automatically deleting unnecessary accounts when an employee leaves, changes groups, or does not use the account prior to its expiration. Azure offers a wide range of data encryption capabilities up to AES-256. Options include .NET cryptographic services, Windows Server public key infrastructure (PKK) components, Active Directory Rights Management Services (AD RMS), and Bitlocker for data import/export scenarios.
24.	How are customers authenticated?	*APRA Prudential Practice Guide: Management of Security Risk in Information and Information Technology, section 40: “A regulated institution would normally take appropriate measures to identify and authenticate users or IT assets”.* Azure can 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.

Ref.	Question/requirement	Template response and guidance
25.	What are the procedures for identifying, reporting and responding to suspected security incidents and violations?	*APRA Prudential Practice Guide: Management of Security Risk in Information and Information Technology, section 71: "APRA envisages that a regulated institution would develop appropriate processes to manage all stages of an incident that could impact on services".* This is an issue that we take very seriously. We have therefore checked these procedures in detail with Microsoft and are confident that they provide excellent means to enable us to identify, report and respond properly and promptly in the event of any security incident or violation. We are assured that Microsoft is committed to protecting the privacy of our and Microsoft makes this statement in its Azure Privacy Statement. First, there are robust procedures offered by Microsoft that enable the **prevention** of security incidents and violations arising in the first place and **detection** in the event that they do occur. Specifically: **a.** Microsoft implements 24 hour monitored physical hardware. Data center access is restricted 24 hours per day by job function so that only essential personnel have access to customer applications and services. Physical access control uses multiple authentication and security processes, including badges and smart cards, biometric scanners, on-premises security officers, continuous video surveillance, and two-factor authentication. **b.** Microsoft implements "prevent, detect, and mitigate breach", which is a defensive strategy aimed at predicting and preventing a security breach before it happens. This involves continuous improvements to built-in security features, including port scanning and remediation, perimeter vulnerability scanning, OS patching to the latest updated security software, network-level DDOS (distributed denial-of-service) detection and prevention, and multi-factor authentication for service access. **c.** Wherever possible, human intervention is replaced by an automated, tool-based process, including

Ref.	Question/requirement	Template response and guidance
		routine functions such as deployment, debugging, diagnostic collection, and restarting services. Azure continues to invest in systems automation that helps identify abnormal and suspicious behavior and respond quickly to mitigate security risk. Microsoft is continuously developing a highly effective system of automated patch deployment that generates and deploys solutions to problems identified by the monitoring systems—all without human intervention. This greatly enhances the security and agility of the service. **d.** Microsoft conducts penetration tests to enable continuous improvement of incident response procedures. These internal tests help Azure security experts create a methodical, repeatable, and optimized stepwise response process and automation. Second, in the event that a security incident or violation is detected, Microsoft Customer Service and Support notifies Azure subscribers by updating the Service Health Dashboard that is available on the Azure portal. We would have access to Microsoft's dedicated support staff, who have a deep knowledge of the service. Microsoft provides a Recovery Time Objective (RTO) of 30 min or less for Virtual Machines and Storage, 1 hour or less for Virtual Network, and a Recovery Point Objective (RPO) of 1 minute or less for Storage. Finally, after the incident, Microsoft provides a thorough post-incident review report (PIR). The PIR includes: • An incident summary and event timeline. • Broad customer impact and root cause analysis. • Actions being taken for continuous improvement.

Ref.	Question/requirement	Template response and guidance
		Microsoft will provide the PIR within five business days following resolution of the service incident. Administrators can also request a PIR using a standard online service request submission through the Azure portal or a phone call to Microsoft Customer Service and Support.
26.	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, sections 50 and 51: "In APRA's view, cryptographic techniques would normally be used to control access to sensitive data/information, both in storage and in transit".* Azure offers a wide range of data encryption capabilities up to AES-256. Options include .NET cryptographic services, Windows Server public key infrastructure (PKK) components, Active Directory Rights Management Services (AD RMS), and Bitlocker for data import/export scenarios. Networks within the Azure data centers are segmented to provide physical separation of critical back-end servers and storage devices from the public-facing interfaces. Edge router security allows the ability to detect intrusions and signs of vulnerability. Azure uses industry-standard transport protocols such as SSL and TLS between user devices and Microsoft data centers, and within data centers themselves. With virtual networks, industry standard IPsec protocol can be used to encrypt traffic between the corporate VPN gateway and Azure. Encryption can be enabled for traffic between VMs and end users.
27.	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, section 55, 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.*

Ref.	Question/requirement	Template response and guidance
		Yes. Microsoft uses best practice procedures and a wiping solution that is NIST 800-88 compliant. For hard drives that can't 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 utilize approved media storage and disposal management services. Paper documents are destroyed by approved means at the pre-determined end-of-life cycle. "Secure disposal or re-use of equipment and disposal of media" is covered under the ISO/IEC 27001 standards against which Microsoft is certified.
28.	Are there documented security procedures for safeguarding premises and restricted areas? If yes, provide descriptions of these procedures.	*APRA Prudential Practice Guide: Management of Security Risk in Information and Information Technology, section 56, states that "The absence of physical security could compromise the effectiveness of other IT security controls".* 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 centers are monitored using motion sensors, video surveillance and security breach alarms.
29.	Are there documented security procedures for safeguarding hardware, software and	*APRA Prudential Practice Guide: Management of Security Risk in Information and Information Technology, section 56, states that "The absence of physical security could compromise the*

Ref.	Question/requirement	Template response and guidance
	data in the data center?	*effectiveness of other IT security controls".* Yes. The security procedures for safeguarding hardware, software and security are documented by Microsoft in its Standard Response to Request for Information – Security and Privacy. This confirms how the following aspects of Microsoft's operations safeguard hardware, software and data: • Compliance • Data Governance • Facility • Human Resources • Information Security • Legal • Operations • Risk Management • Release Management • Resiliency

Ref.	Question/requirement	Template response and guidance
		- Security Architecture
30.	How are privileged system administration accounts managed? Describe the procedures governing the issuance (including emergency usage), protection, maintenance and destruction of these accounts. Please describe how the privileged accounts are subjected to dual control (e.g. password is split into 2 halves and each given to a different staff for custody).	*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, section 42 lists "administration or other privileged access to sensitive or critical IT assets" as one of a number of "examples where increased authentication strength is typically required, given the risks involved".* 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, fingerprinting, 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. User access to data is also limited by user role. For example, system administrators are not provided with database administrative access. 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.
31.	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, section 44(g), 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.

Ref.	Question/requirement	Template response and guidance
		An internal, independent Microsoft team will audit the log at least once per quarter.
32.	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. 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.
33.	Is access to sensitive files, commands and services restricted and protected from manipulation? Provide details of controls implemented.	*APRA Prudential Practice Guide: Management of Security Risk in Information and Information Technology, section 37: "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.
34.	What remote access controls are implemented?	*APRA Prudential Practice Guide: Management of Security Risk in Information and Information Technology, section 42, lists "remote access (i.e. via public networks) to sensitive or critical IT assets" as being one of a number of "examples where increased authentication strength is required".* Administrators who have access to applications have no physical access to the production so administrators have to remotely access the controlled, monitored remote access facility. All operations

Ref.	Question/requirement	Template response and guidance
		through this remote access facility are logged.
35.	Does the service provider have a disaster recovery or business continuity plan? If yes, provide documentation or details.	*Various obligations regarding disaster recovery and business continuity management that apply to FSIs 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.* Yes. Microsoft offers contractually-guaranteed uptime, globally available data centers for primary and backup storage, physical redundancy at disk, NIC, power supply and server levels, constant content replication, robust backup, restoration and failover capabilities, 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, 24/7 on-call engineering teams.
36.	What are the recovery time objectives (RTO) of systems or applications outsourced to the service provider?	*APRA Prudential Standard: Business Continuity Management, section 25, states that an FSI "must identify and document appropriate recovery objectives and implementation strategies". No maximum RTO is specified.* 1 hour or less for Microsoft Exchange Online, 6 hours or less for SharePoint Online.
37.	What are the recovery point objectives (RPO) of systems or applications outsourced to the service provider?	*APRA Prudential Standard: Business Continuity Management, section 25, states that an FSI "must identify and document appropriate recovery objectives and implementation strategies". No maximum RPO is specified.* 1 minute or less for Storage.
38.	What are the data backup and recovery	*APRA Prudential Practice Guide: Management of Security Risk in Information and Information*

Ref.	Question/requirement	Template response and guidance
	arrangements for your organization’s data that resided with the service provider?	*Technology, section 12: “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 center, and service levels. • Data redundancy with robust failover capabilities. • Functional redundancy with offline functionality. **Resiliency** • Active load balancing. • Automated failover with human backup. • Recovery testing across failure domains. **Distributed Services** • Distributed component services 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.

Ref.	Question/requirement	Template response and guidance
		Monitoring • Internal monitoring built to drive automatic recovery. • Outside-in monitoring raises alerts about incidents. • Extensive diagnostics provide logging, auditing, and granular tracing. **Simplification** • Standardized hardware reduces issue isolation complexities. • Fully automated deployment models. • Standard built-in management mechanism. **Human backup** • Automated recovery actions with 24/7 on-call support. • Team with diverse skills on the call provides rapid response and resolution. • Continuous improvement by learning from the on-call teams. **Continuous learning** • If an incident occurs, Microsoft does a thorough post-incident review every time.

Ref.	Question/requirement	Template response and guidance
		- Microsoft's post-incident review consists of analysis of what happened, Microsoft's response, and Microsoft's plan to prevent it in the future. In the event the organization was affected by a service incident, Microsoft shares the post-incident review with the organization.
39.	How frequently does the service provider conduct disaster recovery tests?	*APRA Prudential Standard: Business Continuity Management, section 29: "A regulated institution must review and test its BCP at least annually, or more frequently if there are material changes to business operations".* At least once per year.

APPENDIX ONE

MICROSOFT AZURE

AUSTRALIA

FINANCIAL SERVICES PROVIDER FACT SHEET

Australia Office 365
Financial Services Fac

APPENDIX TWO

MANDATORY CONTRACTUAL REQUIREMENTS

This table sets out the specific items that must be covered in the FSI's agreement with the Service Provider.

Key:

Where relevant, a cross-reference is included in *red italics* to the underlying regulation that sets out the contractual requirement.

In blue text, Microsoft has provided you with a reference to where in the agreement the contractual requirement is covered for ease of reference.

Terms used below as follows:

OST = *Online Services Terms*

EA = *Enterprise Agreement*

Enrolment = *Enterprise Enrolment*

FSA = *Financial Services Amendment*

MBSA = *Microsoft Business and Services Agreement*

PUR = *Product Use Rights*

SLA = *Online Services Service Level Agreement*

Ref.	Requirement	Microsoft agreement reference
1.	(a) The scope of the arrangement and services to be supplied	*Section 25, Outsourcing Guidelines* 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 Enrollment, and the order will set out the online services and relevant prices. The services are described, along with the applicable usage rights, in the Product List and OST (pages 14 and 15). The services are described in detail in the Services Description, which is not part of the contract. However, Microsoft makes a functionality commitment in the Core Features Amendment and as a minimum the online services will meet that commitment.
2.	(b) Commencement and end dates	*Section 25, Outsourcing Guidelines* *Please insert the proposed start date of the outsourcing service.* Enrollments have a three year term, and may be renewed for a further three year term.
3.	(c) Review provisions	*Section 25, Outsourcing Guidelines* The OST specifies the audit and monitoring mechanisms that Microsoft puts in place in order to verify that the online services meet appropriate security and compliance standards. This commitment is reiterated in the FSA. Clause 1f of the FSA gives the customer the opportunity to participate in the Microsoft Online Services Customer Compliance Program, which is a for-fee program that facilitates the customer's ability to (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 additional notification of changes that may materially impact Microsoft's ability to

Ref.	Requirement	Microsoft agreement reference
		provide the services, and (e) provide feedback on areas for improvement in the services. 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. In addition, Customers can review the manner in which Microsoft provides the online services. As set out on page 13 of the OST, the customer is entitled to access the Microsoft Online Information Security Policy, which is the document where Microsoft sets out its information security management processes. Microsoft also commits to providing the customer with a summary of Microsoft's annual audit report, which is performed by an independent third party and measures compliance against Microsoft's certifications.
4.	(d) Pricing and fee structure	*Section 25, Outsourcing Guidelines* Sales of Microsoft product to enterprise customers are made via a Microsoft reseller, who sets the end price with the customer. The basis for the pricing will therefore be set out in a separate agreement with Microsoft's reseller. Microsoft has a variety of flexible licensing models. In general, the customer is required to commit to annual payments (payable in advance) based upon the customer's number of users. Please refer to the arrangements with your Microsoft reseller for more information. *Further information about the applicable pricing model can be provided upon request.*
5.	(e) Service levels and performance requirements	*Section 25, Outsourcing Guidelines* The SLA contains Microsoft's service level commitment, as well as the remedies for the customer in the event that Microsoft does not meet the commitment. The terms of the SLA current at the start of the applicable initial or renewal term of the Enrollment are fixed for the duration of that term.

Ref.	Requirement	Microsoft agreement reference
		Microsoft supports compliance with CPS 231 requirements[1] to monitor performance of the online services via the administrative dashboard, which includes information as to Microsoft compliance with its SLA commitments.
6.	(f) Audit and monitoring procedures	*Section 25, Outsourcing Guidelines* The OST specifies the audit and monitoring mechanisms that Microsoft puts in place in order to verify that the online services meet appropriate security and compliance standards. This commitment is reiterated in the FSA. In addition, the FSA details the examination and influence 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. Under the FSA, the customer also has the opportunity to participate in the Microsoft Online Services Customer Compliance Program, which is a for-fee program that facilitates the customer's ability to (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 additional 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 CPS 231 requirement that requires the regulated entity to obtain examination and access rights from the service provider,[2] Microsoft believes that the FSA meets this requirement.

[1] Note: Paragraph 38(b) provides: "*A regulated institution must ensure it has sufficient and appropriate resources to manage and monitor the outsourcing relationship at all times. … At a minimum, the monitoring must include: …(b) a process for regular monitoring of performance under the agreement, including meeting criteria concerning service levels.*"

[2] Paragraph 30 of CPS 231 contains the following: "*An outsourcing agreement must include a clause that allows APRA access to documentation and information related to the outsourcing arrangement. In the normal course, APRA will seek to obtain whatever information it requires from the regulated institution; however, the outsourcing agreement must include the right for APRA to conduct on-site visits to*

Ref.	Requirement	Microsoft agreement reference
7.	(g) Business continuity management	*Section 25, Outsourcing Guidelines* Business Continuity Management forms part of the scope of the accreditation that Microsoft remains in relation to the online services, and Microsoft commits to maintain a data security policy that complies with these accreditations (see OST page 13). Business Continuity Management also forms part of the scope of Microsoft's annual third party compliance audit.
8.	(h) Confidentiality, privacy and security of information	*Section 25, Outsourcing Guidelines* MBSA section 3 deals with confidentiality. Under this section Microsoft commits not to disclose our confidential information (which includes our data) to third parties and to only use our confidential information for the purposes of Microsoft's business relationship with us. Further, Microsoft commits to take reasonable steps to protect our confidential information, to notify us if there is any unauthorized use or disclosure of our confidential information and to cooperate with us to help to regain control of our confidential information and prevent further unauthorized use or disclosure of it. Microsoft also makes specific commitments with respect to safeguarding our data in the OST. In summary Microsoft commits that: 1. Ownership of our data remains at all times with us (see OST, page 8). 2. Our data will only be used to provide the online services to us and our data will not be used for any other purposes, including for advertising or other commercial purposes (see OST, page 8). 3. Microsoft will not disclose our data to law enforcement unless it is legally obliged to do so, and only after not

the service provider if APRA considers this necessary in its role as prudential supervisor. APRA expects service providers to cooperate with APRA's requests for information and assistance. If APRA intends to undertake an on-site visit to a service provider, it will normally inform the regulated institution of its intention to do so."

Ref.	Requirement	Microsoft agreement reference
		being able to redirect the request to us (see OST, page 8). 4. Microsoft will implement and maintain appropriate technical and organizational measures, internal controls, and information security routines intended to protect our data against accidental, unauthorized or unlawful access, disclosure, alteration, loss, or destruction (see OST, page 8 and pages 11-13 for more details). 5. Microsoft will notify us if it becomes aware of any security incident, and will take reasonable steps to mitigate the effects and minimize the damage resulting from the security incident (see OST, page 9).
9.	(i) Default arrangements and termination provisions	*Section 25, Outsourcing Guidelines* Termination rights for the Enrollment are set out in the Enrollment itself, and in section 6 of the EA. If the Enrollment is terminated, this will terminate all products and services ordered under the Enrollment (except to the extent that the customer has perpetual rights). Online services may also be terminated or suspended in the circumstances described in section 6d of the EA, and as specified in the OST, pages 5, 11 and 30. In the event of default, the provisions of the SLA will apply to service level failures and page 9 of the OST sets out arrangements in the event of security incidents. Other defaults are addressed in the MBSA and EA. A termination right for cause is set out at section 6c of the EA. The contract allows the customer to terminate the arrangement with Microsoft for convenience (MBSA section 8) which means the customer has the right to terminate in the event of default including change of ownership, insolvency or where there is a breach of security or confidentiality or demonstrable deterioration in the ability of the Service Provider to perform the service as contracted.

Ref.	Requirement	Microsoft agreement reference
		Note also that customers have control over the use they make of, and data they load into, the online service. In the event of default, the provisions of the SLA will apply to service level failures and page 9 of the OST sets out arrangements in the event of security incidents. Other defaults are addressed in the MBSA and EA. A termination right for cause is set out at section 6c of the EA.
10.	(j) Dispute resolution arrangements	*Section 25, Outsourcing Guidelines* MBSA section 11 contains provisions that describe how a dispute under the contract is to be conducted. MBSA section 11e sets out the jurisdictions in which parties should bring their actions. Microsoft must bring actions against the customer in the countries where the customer's contracting party is headquartered. The customer must bring actions against: (a) in Ireland if the action is against a Microsoft affiliates in Europe; (b) in the State of Washington, if the action is against a Microsoft affiliate outside of Europe; or (c) in the country where the Microsoft affiliate delivering the services has its headquarters if the action is to enforce a Statement of Services. MBSA section 11h sets out the choice of law provision. Either, the contract is governed by the laws of the State of Washington if the contract is with a Microsoft affiliate located outside of Europe; or the contract is governed by the laws of Ireland if the contract is with a European Microsoft affiliate.
11.	(k) Liability and indemnity	*Section 25, Outsourcing Guidelines* The SLA contains Microsoft's service level commitment, as well as the remedies for the customer in the event that Microsoft does not meet the commitment, including services credits. MBSA section 6 deals with liability. MBSA section 5 sets out Microsoft's obligation to defend the regulated entity against third party infringement and breach of confidence claims. Microsoft's liability under section 5 is unlimited.

Ref.	Requirement	Microsoft agreement reference
12.	(I) Sub-contracting[3]	*Section 25, Outsourcing Guidelines* See page 9 of the OST, under which Microsoft is permitted to hire subcontractors. The confidentiality of our data is protected when Microsoft uses subcontractors because 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” (OST, page 9). Microsoft commits that any subcontractors to whom Microsoft transfers our data will have entered into written agreements with Microsoft that are no less protective than the data processing terms in the OST (OST, page 11). Under the terms of the OST, Microsoft remains contractually responsible (and therefore liable) for its subcontractors’ compliance with Microsoft’s obligations in the OST (OST, page 9). In addition, Microsoft’s commitment to ISO/IEC 27018, requires Microsoft to ensure that its subcontractors are subject to the same security controls as Microsoft is subject to. Finally, the EU Model Clauses, which are included in the OST, require Microsoft to ensure that its subcontractors outside of Europe comply with the same requirements as Microsoft and set out in detail how Microsoft must achieve this. Microsoft maintains a list of authorized subcontractors for the online services that have access to our data and provides us with a mechanism to obtain notice of any updates to that list (OST, page 10). The actual list is published on the applicable Trust Center. If we do not approve of a subcontractor that is added to the list, then we are entitled to terminate the affected online services.

[3] Paragraph 27 of the Outsourcing Guidelines contains the following: “*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.*”

Ref.	Requirement	Microsoft agreement reference
13.	(m) Insurance	*Section 25, Outsourcing Guidelines* MBSA section 10 deals with insurance. In practice, Microsoft maintains self-insurance arrangements for much of the areas where third party insurance is typically obtained. Microsoft has taken the commercial decision to take this approach, and does not believe that this detrimentally impacts upon its customers given that Microsoft is an extremely substantial entity.
14.	(n) To the extent applicable, offshoring arrangements (including through subcontracting)[4]	*Section 25, Outsourcing Guidelines* Pages 9-11 of the OST contain general commitments around data location. Microsoft will ensure that Customer Data will always be stored and processed in accordance with the EU and Swiss Safe Harbour Frameworks as maintained by the US Government. Microsoft also commits that Customer Data transfers out of the EU will be governed by the EU Model Clauses set out at pages 29-33 of the OST. Also, as noted on page 11 of the OST: "Any subcontractors to whom Microsoft transfers Customer Data, even those used for storage purposes, will have entered into written agreements with Microsoft that are no less protective than the DPT". Commitments on the location of data at rest are discussed at p 10 of the OST, and may depend on where a customer provisions its service tenancy or specify as a Geo for the online service. More details are set out on the Trust Centers for each applicable online service. Microsoft data center locations are made public on the Microsoft Trust Center. We do not consider that additional terms are necessary, over and above the current terms in the contract, to address this fact. *Microsoft notes that APRA has the power under CPS 231 to direct the regulated entity to cease using the*

[4] Paragraph 37 of the Outsourcing Guidelines contains the following: "*If, in APRA's view, the offshoring agreement involves risks that the regulated institution is not managing appropriately, APRA may require the regulated institution to make other arrangements for the outsourced activity as soon as practicable.*"

Ref.	Requirement	Microsoft agreement reference
		outsourced service. In the unlikely event that this occurs in relation to Azure, Microsoft has equivalent on-premise products that the customer can use itself or host with a Microsoft partner (there are a number of partners located in Australia). The customer also has the flexibility to maintain a hybrid solution, which involves part of its business using on-premise and part of its business using online services, with a consistent interface and experience for all users.