A compliance checklist for financial institutions in New Zealand

Version: [insert date] 2018

Contents

Introduction: A compliance checklist for financial institutions in New Zealand

Overview

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

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

Microsoft is committed to providing a trusted set of cloud services to financial institutions in New Zealand. 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 New Zealand. We developed it to help financial institutions in New Zealand adopt Microsoft cloud services with confidence that they are meeting the applicable regulatory requirements.

What does this checklist contain?

This checklist contains:

1. an **Overview of the Regulatory Landscape**, which introduces the relevant regulatory requirements in New Zealand;

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 New Zealand who want to use Microsoft cloud services. We use the term "financial institutions" (**FIs**) broadly, to include any entity that is regulated by the Reserve Bank of New Zealand (**RBNZ**). 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 New Zealand, 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 New Zealand, 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 RBNZ, 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 New Zealand.

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 RBNZ. 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 Processing Terms (“DPT”) of Microsoft’s Online Services Terms.

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 Reserve Bank of New Zealand (**RBNZ**). Banks, credit unions, general insurers, life insurers, superannuation trustees and other financial institutions are regulated by RBNZ. The RBNZ website at www.rbnz.govt.nz 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. Large banks[1] using cloud services need to consider the RBNZ Outsourcing Policy of September 2017 (**RBNZ Outsourcing Policy**) 2. All FIs (whether large or small) need to consider their general RBNZ obligations to manage their business risks properly 3. The Privacy Act in relation to any outsourcing that may involve the processing of personal data. (A new Privacy Bill has been tabled for parliament which will repeal and replace the Privacy Act. At the date of this checklist, the Privacy Bill was not yet effective. The Privacy Bill contains small but notable changes to the Privacy Act, including mandatory breach notification.) 4. Cloud Computing: A guide to making the right choices, published by the Privacy Commissioner February 2013
Is regulatory approval required?	**No**, if the outsourcing arrangement is conducted directly between the bank and the CSP, regulatory approval is not required. Outsourcing arrangments made through a bank's related company (e.g. parent company) may require a non-objection from the RBNZ.
Are transfers of data outside of New Zealand permitted?	**Yes.** Subject to compliance with the Information Privacy Principles, personal information may be transferred to a third country without restriction.

[1] RBNZ will consider a bank as "large" if its liabilities net of amounts due to related parties exceed $10 billion.

	However, the Privacy Act will continue to apply to personal information even when it is transferred out of New Zealand. In addition, the Privacy Commissioner may prohibit transborder dataflows of information where the Privacy Commissioner is satisfied, on reasonable grounds, that: (i) the information has been received in New Zealand from another state and the transborder dataflow is likely to be to a third state where it will not be subject to a law providing comparable safeguards to the Privacy Act; and (ii) the transborder dataflow would be likely to lead to a contravention of the basic principles of national application set out in Part Two of the OECD Guidelines for Multinational Enterprises and Schedule 5A of the Privacy Act. The Privacy Commissioner's powers to prohibit transborder dataflows do not apply where the transborder dataflow is required by New Zealand law, or any convention or other instrument imposing international obligations on New Zealand.
Are public cloud services sufficiently secure?	**Yes.** Several financial institutions in New Zealand are already using public cloud services. In fact, public cloud typically enables customers to take advantage of the most advanced security capabilities and innovations because public cloud services generally adopt those innovations first and have a much larger pool of threat intelligence data to draw upon. An example of this type of innovation in Microsoft cloud services is Office 365 Advanced Threat Protection and the Azure Web Application Firewall, which provide a very sophisticated model to detect and mitigate previously unknown malware and provide customers with information security protections and analytics information.
Are there any mandatory terms that must be included in the contract with the services provider?	**Yes.** Section B2.9 of the RBNZ Outsourcing Policy contains prescribed contractual terms for outsourcing contracts. These are set out in detail in the table in Part 2 which also illustrates how contracts with Microsoft comply with the relevant requirements.
How do more general privacy laws in New Zealand apply to the use of cloud services by financial institutions?	Use of the cloud services should comply with the Privacy Act in relation to any outsourcing that may involve the processing of personal data. Additionally, the Privacy Commissioner has created a document called 'Cloud Computing: A guide to making the right choices', February 2013 which contains some useful items to check are included in the contract.

Compliance Checklist

How does this Compliance Checklist work?

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

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

How should we use the Compliance Checklist?

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

Which part(s) do we need to look at?

There are two parts to this Compliance Checklist:

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

Part 1: Key Considerations

Who does this Part 1 apply to?

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

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?	*RBNZ 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 organisation's own risk management purposes* If using public cloud: Microsoft Azure, on which most Microsoft business cloud services are built, hosts multiple tenants in a highly-secure way through logical data isolation. Data storage and processing for our tenant is isolated from each other tenants as described in section E. (Technical and Operational Risk Q&A) below. If using hybrid cloud: By using Microsoft hybrid cloud, customers can move to multi-tenant cloud at their own pace. Tenants may wish to identify the categories of data that they will store on their own servers using Windows Server virtual machines. All other categories of data will be stored in the multi-tenant cloud. Microsoft Azure, on which most Microsoft business cloud services are built, hosts multiple tenants in a highly-secure way through logical data isolation. Data storage and processing for our tenants is isolated from each other tenant as described in section E. (Technical and Operational Risk Q&A) below.
5.	What data will be processed by the service provider on behalf of the financial institution?	• 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).

Ref.	Question / requirement	Guidance
		- 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?	*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. **b. Track-record.** Many of the world's top companies use Microsoft cloud services. There are various case studies relating to the use of Microsoft cloud services at customers.microsoft.com. Customers have obtained regulatory approvals (when required) and are using Online Services in all regions of the globe including Asia, North America, Latin America, Europe, Middle East and Africa. Key countries of adoption include, by way of example: the United States, Canada, Hong Kong, Singapore, Australia, Japan, the United Kingdom, France, Germany, Italy, Spain, the Netherlands, Poland, Belgium, Denmark, Norway, Sweden, Czech Republic, Brazil, Luxembourg, Hungary, Mexico, Chile, Peru, Argentina, South Africa, and Israel. Office 365 has grown to have over 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

Ref.	Question / requirement	Guidance
		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 $500 billion, 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 ***RBNZ has no issue in principle with the use of service providers located outside of New Zealand. However, from our dealings with other customers and regulators we set out this this section how any potential risks are mitigated.***		
7.	Will the proposed outsourcing require offshoring? If so, from which territory(ies) will the outsourced cloud services be provided?	*Microsoft takes a regional approach to hosting of Microsoft Online Services data. For customers with a presence in the Asia-Pacific region, the applicable Microsoft Online Services are currently be hosted out of Microsoft's data centres in Sydney and Melbourne, 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 https://www.microsoft.com/en-us/TrustCenter/Privacy/where-your-data-is-located. 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:*

Ref.	Question / requirement	Guidance
		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:https://www.microsoft.com/en-us/TrustCenter/Privacy/where-your-data-is-located. Certain other categories of data may be stored outside of Australia and the relevant locations are also described in the interactive data centres map.
8.	What other risks have been considered in relation to the proposed offshoring arrangement? In particular, what measures are in place to ensure that performance by the service provider of the outsourced functions outside of New Zealand would not complicate the logistics of ensuring timely performance? For example, due to time zone differences, differences in statutory holidays, the extra time needed to access	Microsoft works with customers around the world (including many in New Zealand) and its operations are set up to ensure that logistical issues for international customers do not arise. For example, time zones and statutory holidays will not be an issue, since Microsoft's services are provided 24/7 without reference to statutory holidays. We do not see any issue in terms of needing extra time to access essential staff and systems, since we have audit and inspection rights (as detailed in section F below). The other considerations are also relevant to the location of Microsoft's data centres: **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. **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

Ref.	Question / requirement	Guidance
	essential staff and systems.	power management systems, 24-hour monitored physical hardware and seismically-braced racks. These requirements are covered by Microsoft's ISO/IEC 27001 accreditation. **e. Legal** Customers will have in place a binding negotiated contractual agreement with Microsoft in relation to the outsourced service, giving them direct contractual rights and maintaining regulatory oversight. The terms are summarised in Part 2.
9.	Would proceedings relating to the outsourcing have to be brought in another jurisdiction's court under that jurisdiction's laws?	The governing law is that of Washington, however the parties have the ability to bring proceedings in the locations as follows: • If Microsoft brings the action, the jurisdiction will be where the customer is located (i.e. New Zealand); • If the customer brings the action, the jurisdiction will be the state of Washington; and • Both parties can seek injunctive relief with respect to a violation of intellectual property rights or confidentiality obligations in any appropriate jurisdiction.
10.	Is there a risk that the duties and powers of the service provider's own regulator(s) in the country(ies) in which the service will be hosted could cause the regulator(s) to intervene in such a way as to intervene with the provider's performance?	Australia, Singapore and Hong Kong are (and have long been) recognised as stable, safe and reliable jurisdictions in respect of their legal systems, regulatory regime, technology and infrastructure. They have been ranked by the Asia Cloud Computing Association as being amongst the leading countries in Asia-Pacific in relation to issues such as data security and regulatory stability and enforcement. The circumstances in which authorities in these countries may have rights to access customer information are not considered to be unwarranted. Australia, Hong Kong and Singapore have been selected by Microsoft taking into careful account the country and socio-economic factors. We are confident that Singapore and Hong Kong offer extremely stable political and socio-economic environments with robust and transparent legal frameworks. Australia, Singapore, and Hong Kong score very highly in the Asia Pacific in terms of legal transparency and regulatory oversight which is undertaken in accordance with international standards. The duties and powers of the Australian, Singaporean, or Hong Kong authorities should not intervene in such a way as to intervene with Microsoft's performance.

<table>
<tr><th>Ref.</th><th>Question / requirement</th><th>Guidance</th></tr>
<tr><td>11.</td><td>What measures are in place to avoid the risk that competition for the service provider's resources could impede the performance of functions for the FI?</td><td>Microsoft is one of the largest providers of cloud services globally and has capacity to service a large number of customers without the risk of competition for resources. The customer would be subject to the same prioritization as any other customer of the same services from Microsoft. Of course, the services are protected by Microsoft's SLA and its coinciding terms and conditions. More information on SLA is available at: http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=37, and more details about Microsoft's Service Continuity are available at: http://office.microsoft.com/en-us/business/office-365-online-service-availability-FX104028266.aspx.
Microsoft provides a contractual, financially-backed 99.9% uptime guarantee for the Office 365 product.
Microsoft also ensures that a raft of different safeguards and arrangements are in place to prevent and minimise the impact of any technology failure. Microsoft is subject to very high international auditing standards in this regard which provide us with a great deal of comfort. The resources that Microsoft has in place also mean that Microsoft does not foresee risks in relation to the adequacy of Microsoft to fulfil obligations or provide remedies and restitution.
Microsoft is an industry leader in cloud computing. The Microsoft Online Services were built based on ISO 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. FI 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 the Microsoft Online Services meets their respective regulatory requirements.</td></tr>
<tr><td colspan="3"><b>C. COMPLIANCE WITH A BANK'S CONDITIONS OF REGISTRATION</b>
<b><i>New Zealand Banks are subject to various standard and non-standard conditions of registration. You will need to ensure that the proposed use of the Microsoft Online Services complies with any such conditions.</i></b></td></tr>
<tr><td>12.</td><td>Please confirm whether the FSI is a</td><td><i>Many of the RBNZ requirements only apply to "large banks". RBNZ will consider a bank as "large" if its liabilities net of amounts due to related parties exceed $10 billion. Note that since all large banks in New Zealand are currently owned by</i></td></tr>
</table>

Ref.	Question / requirement	Guidance
	"large bank" for the purposes of RBNZ policy.	*parent banks in Australia, those parent banks will be subject to Australian law and regulation (including the outsourcing and cloud computing requirements of the Australian Prudential Regulatory Authority (**"APRA"**)). Microsoft has prepared a similar Q&A for APRA requirements in Australia and can share this with you on request.*
13.	Please confirm whether any of the following activities will be affected by the proposed outsourcing: (a) clearing and settlement obligations; (b) identification of financial risk positions; (c) monitoring and management of financial risk positions; or (d) access by existing customers to payments facilities.	*RBNZ Outsourcing Policy, Sections B1.1 (3). One of the key objectives of the RBNZ Outsourcing Policy is to ensure that banks have the legal and practical ability to control each of these activities.* You should consider whether any of these core banking functions will be outsourced or affected by the outsourcing.

Ref.	Question / requirement	Guidance
14.	Will the proposed outsourcing have any impact on the ability of the board to manage, direct or supervise the business and affairs of the FI?	*RBNZ Outsourcing Policy, Appendix One: Conditions of Registration Section 1.1 (2) (a). The ability of the board to manage/direct/supervise is a condition of registration.* No. The customer's board will still have ultimate control of the business and affairs of the FI and the proposed use of Microsoft's Online Services will not change this. The contract in place with Microsoft contains various contractual and technical means for the customer to ensure that they have due supervision and control.
15.	Is the proposed outsourcing compliant with any other standard or non-standard conditions of registration imposed on the FI?	*RBNZ Outsourcing Policy, Section A.1.4 Some large banks are subject to non-standard conditions of registration which may apply to their outsourcing arrangements. The customer will need to consider whether such conditions exist and, if so, how (if at all) they may apply to the proposed use of Microsoft's Online Services.*
16.	What monitoring processes does the financial institution have in place to manage the outsourcing?	*Financial institutions should 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.

Ref.	Question / requirement	Guidance
		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 Microsoft's ability to facilitate compliance against the customer's policy, procedural, security control and regulatory requirements. The Microsoft Financial Services Amendment further gives the customer the opportunity to participate in the optional financial institution Customer Compliance Program at any time, which enables the customer to have additional monitoring, supervisory and audit rights and additional controls over Microsoft cloud services, such as (a) access to Microsoft personnel for raising questions and escalations relating to Microsoft cloud services, (b) invitation to participate in a webcast hosted by Microsoft to discuss audit results that leads to subsequent access to detailed information regarding planned remediation of any deficiencies identified by the audit, (c) receipt of communication from Microsoft on (1) the nature, common causes, and resolutions of security incidents and other circumstances that can reasonably be expected to have a material service impact on the customer's use of Microsoft cloud services, (2) Microsoft's risk-threat evaluations, and (3) significant changes to Microsoft's business resumption and contingency plans or other circumstances that might have a serious impact on the customer's use of Microsoft cloud services, (d) access to a summary report of the results of Microsoft's third party penetration testing against Microsoft cloud services (e.g. evidence of data isolation among tenants in the multi-tenanted services); and (e) access to Microsoft's subject matter experts through group events.

Ref.	Question / requirement	Guidance
17.	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 Platform, which provides confidential materials, such as third-party audit reports, to current customers and potential customers testing Microsoft's Online Services; • a Financial Services Compliance Program, which provides access to a team of specialists in banking, insurance, asset management, and financial services treasury and remediation services; • the Azure Security Center and Office 365 Advanced Threat Analytics, which enable customers to seamlessly obtain cybersecurity-related information about Online Services deployments; • Office 365 Secure Score, which provides insight into the strength of customers' Office 365 deployment based on the customer's configuration settings compared with recommendations from Microsoft, and Azure Advisor, which enables customers to optimise their Azure resources for high availability, security, performance, and cost; • the Office 365 Service Health Dashboard and Azure Status Dashboard, which broadcast real-time information regarding the status of Microsoft'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.

Ref.	Question / requirement	Guidance
18.	How does the financial institution ensure that it maintains ultimate responsibility for any outsourcing?	The contract with Microsoft provides the customer with legal mechanisms to manage the relationship including appropriate allocation of responsibilities, oversight and remedies.
C. RISK MANAGEMENT **RBNZ is particularly interested in the controls that the FI has in place in respect of the outsourcing and how risks are managed. This section looks at these requirements in more detail.**		
19.	How do the proposed arrangements ensure that the outsourcing does not create a risk that the operation and management of the FI might be interrupted for a material length of time?	*RBNZ Outsourcing Policy, Section B 2.2* We have minimised the risks in the following ways: 1. Through our choice of service provider a. **Competence and experience**. Microsoft is an industry leader in cloud computing. Microsoft Online Services were built based on ISO 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 Microsoft Online Services . We consulted various case studies relating to Office 365, which are available on the Microsoft website and also considered the fact that Microsoft has amongst its customers some of the world's largest organisations and FSIs.

Ref.	Question / requirement	Guidance
		c. **Specific financial services credentials**. FSI 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 Online Services 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 capitalisation. Microsoft's audited financial statements indicate that it has been profitable for each of the past three years. Its market capitalisation 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 99.9% uptime, hosted out of world class data centres in Singapore and Hong Kong. Microsoft has recently opened data centres in Sydney and Melbourne, Australia. Beginning in April 2015, Microsoft will offer the Microsoft Online Services out of the Australian Data Centres, 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.

Ref.	Question / requirement	Guidance
		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 centres of even the most sophisticated organisations. We have confidence in the security of the solution and the systems and controls offered by Microsoft. In addition to the ISO 27001 certification, Office 365 is designed for security with Bitlocker Advanced Encryption Standard (AES)encryption of email at rest and secure sockets layer ("SSL")/transport layer security ("TLS") encryption of data in transit. The Microsoft service is subject to the SSAE16 SOC1 Type II audit, an independent, third party audit. 2. Through specific technical measures in place to ensure that operation and management not affected Microsoft offers contractually-guaranteed 99.9% uptime, globally available data centres 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.
20.	What contractual controls does the FI have in respect of the outsourcing? Is the documentation clear on the rights and obligations of each party to the contract and on service levels and pricing, to a level commensurate with the function's time criticality, materiality and substitutability?	*RBNZ Outsourcing Policy, Section B2.9* The provision of the Microsoft Online Services is subject to the following contractual documents: • Microsoft Online Business and Services Agreement (a copy of which is available on request); and • Service Level Agreement (**SLA**), a copy of which is available at: http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=37 Both of these documents and the documents referred to therein very clearly set out the rights and obligations of each party, the service levels and the pricing. The documents provide us with a number of other contractual controls in respect of the outsourcing, notably: • Microsoft is only contractually permitted to use our data to provide the online services. Microsoft is not permitted to use our data for any other purposes, including for advertising or other commercial purposes. • Microsoft commits that it 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.

Ref.	Question / requirement	Guidance
		• Microsoft commits that it has in place audit mechanisms in order to verify that the online services meet appropriate security and compliance standards. • In addition, the contractual process can culminate in the regulator's examination of Microsoft's premises. We also have the opportunity to participate in the Office365 Customer Compliance Program, which is a for-fee program that facilitates our 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 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. • The SLA contains Microsoft's service level commitment, as well as the remedies for us in the event that Microsoft does not meet the commitment. Microsoft commits that it will not modify the terms of the SLA during the initial term of our subscription.
21.	What practical controls does the FI have in respect of the outsourcing?	*RBNZ Outsourcing Policy, Section B2.9* The solution provides a lot of tools which mean that you remain in practical control. Microsoft's SLA (as defined above) applies to the Microsoft Online Services. Your IT administrators also have, for example, access to the Office 365 Service Health Dashboard, which provides real-time and continuous monitoring of the Office 365 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 99.9% uptime guarantee for the Office 365 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 very extensive contractual audit and inspection rights, plus access to the independent SSAE16 SOC1 Type II audit, which enable us to verify their performance. As part of the support you receive from Microsoft, you also have access to a technical account manager who is responsible for understanding your challenges and providing expertise, accelerated support and strategic advice tailored to your organisation. This includes both continuous hands-on assistance and immediate escalation of urgent issues to speed resolution and keep

Ref.	Question / requirement	Guidance
		mission-critical systems functioning. You can be confident that such arrangements provide you with the appropriate mechanisms for managing performance and problems. Your contract with Microsoft clearly provides that ownership of your data remains with you and you retain rights to access your data at all times. On top of this, as mentioned above, Microsoft's services are audited by an independent third party and there are various audit and inspection rights. Your contractual agreements also allow you to terminate the arrangements with Microsoft for your convenience, which would enable you to move to another provider if required.
22.	What internal processes does the FI have in place to manage the risks to the business associated with any outsourcing arrangements?	*RBNZ Outsourcing Policy, Appendix One: "Conditions of Registration" Section 1.1 (2) (a). There are no minimum requirements or detail provided when it comes to internal processes but it would be usual to expect this to include:* • processes for management review and sign off by the board; • risk management policies; • business continuity and disaster recovery plans; and • outsourcing policies.
23.	Does the FI maintain a compendium (a formal and centralised record) of all outsourcing arrangements of the bank which complies with Section B4 of the RBNZ Outsourcing Policy?	*RBNZ Outsourcing Policy, Section B4.* You should maintain a compendium of all outsourcing arrangements which complies with Section B4 of the RBNZ Outsourcing Policy. Microsoft can assist with this on request.

Ref.	Question / requirement	Guidance
	Is the compendium annually reviewed?	
24.	Does the FI maintain a separation plan which complies with Section B5 of the RBNZ Outsourcing Policy?	*RBNZ Outsourcing Policy, Section B5.* You should maintain a separation plan which complies with Section B5 of the RBNZ Outsourcing Policy. Microsoft can assist with this on request.
25.	Has the FI scheduled an annual external review of its compliance with the RBNZ Outsourcing Policy during the five year transition period and a 3 yearly review after the five year transition period?	*RBNZ Outsourcing Policy, Section D.* Microsoft makes available to you extensive relevant information via the Service Trust Portal and, in particular, use of the Compliance Manager. Additionally, it is possible for you to obtain further assistance through the Compliance Program.
D. THE NEED FOR AN APPROPRIATE OUTSOURCING AGREEMENT ***Note: See also Part 2 of this Compliance Checklist for a list of useful standard contractual terms that the Privacy Commisioner recommends are 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 our experience with customers has shown are important to consider as part of the contractual negotiation but which are not necessarily mandatory contractual terms that should be included in all cases.***		

Ref.	Question / requirement	Guidance
26.	Are the outsourcing arrangements contained in a documented legally binding agreement that is signed by all parties?	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.
27.	Does the outsourcing agreement include a clause that allows RBNZ to access documentation and information relating to the outsourcing arrangement?	Yes. There are terms in the contract that enable RBNZ 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.
28.	Does the outsourcing agreement provide a guarantee of access to the minimum IT assets required to operate under a disaster scenario?	Yes. The uptime guarantee given by Microsoft applies to all IT assets, not just a minimum number required to operate in a disaster situation. Microsoft guarantees 99.9% of uptime for most of its Online Services. Uptime guarantees are set forth in Microsoft's contracts with its customers, and if service levels are not maintained, customers may be eligible for a credit towards a portion of their monthly service fees. For information regarding uptime for each Online Service, refer to the Service Level Agreement for Microsoft Online Services.
29.	Does the outsourcing agreement also include reporting mechanisms that ensure adequate	Yes as referenced in Question 17 above.

Ref.	Question / requirement	Guidance
	oversight of IT security risk management by the service provider?	
30.	Is the outsourcing agreement sufficiently flexible to accommodate changes to existing processes and to accommodate new processes in the future to meet changing circumstances?	Yes. The customer can always order additional services if required. The customer may terminate an Online Service at the express direction of a regulator with reasonable notice. Additionally, to ensure regulatory compliance, Microsoft and the customer may contemplate adding additional products or services, or if these are unable to satisfy the customer's new regulatory requirements, the customer may terminate the applicable Online Service without cause by giving 60 days' prior written notice.
31.	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	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.

Ref.	Question / requirement	Guidance
	transitioning the service?	
E. TECHNICAL AND OPERATIONAL RISK Q&A ***RBNZ guidance does not focus on detailed technical and operational requirements relating to the use of cloud services but, rather, focuses more generally on issues such as risk management. However, on the basis that technical and operational factors (for example, data security) are directly relevant to risk management strategy, this section provides some detailed information about the Microsoft's Online Services.***		
32.	Does the service provider permit audit by the financial institution and/or RBNZ?	*RBNZ Outsourcing Policy, Section B 2.9 (2) (b)* Yes. Pursuant to the Financial Services Amendment, Microsoft provides RBNZ 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 RBNZ 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 each Online Service. Customers may also participate in the optional Customer Compliance Program to have additional monitoring, supervisory and audit rights and additional controls over the Online Services. See Part 2 below for further detail.
33.	Are the provider's services subject to any third party 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 addition, the Financial Services Amendment further gives customers the opportunity to participate in the optional Financial Services Customer Compliance Program at any time, which enables them to (amongst other things) participate in a webcast hosted by Microsoft to discuss audit results that leads to subsequent access to detailed information regarding planned remediation of any deficiencies identified by the audit.

Ref.	Question / requirement	Guidance
34.	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?	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 basis.

Ref.	Question / requirement	Guidance
		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 scrutinized, manual-approval process. Preventing breach also involves automatically deleting unnecessary accounts when an employee leaves, changes groups, or does not use the account prior to its expiration. Data is also encrypted. Customer data in Microsoft cloud services exists in two states: • at rest on storage media; and • in transit from a data 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 Platform.
35.	How is the financial institution's data isolated from other data held by the service provider?	For all of its Online Services, Microsoft logically isolates customer data from the other data Microsoft holds. For example, Microsoft Office 365 is a multi-tenant service designed to host multiple tenants in a highly secure way through data isolation. Data storage and processing for each tenant is segregated through an "Active Directory" structure, which isolates customers using security boundaries ("silos"). The silos safeguard the customer's data such that the data cannot be accessed or compromised by co-tenants.
36.	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.
37.	What policies does the service provider have in place to	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.

Ref.	Question / requirement	Guidance
	monitor employees with access to confidential information?	Background screening takes place before Microsoft authorises the employee to access customer data. To the extent permitted by law, any criminal history involving dishonesty, breach of trust, money laundering, or job-related material misrepresentation, falsification, or omission of fact may disqualify a candidate from employment, or, if the individual has commenced employment, may result in termination of employment at a later day.
38.	Are there procedures to ensure that access to production data is restricted on a 'least privilege' basis? If yes, provide a description of these procedures.	Yes. Microsoft applies strict controls over which personnel roles and personnel will be granted access to customer data. Personnel 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.
39.	How are customers authenticated?	Microsoft cloud services use two-factor authentication to enhance security. Typical authentication practices that require only a password to access resources may not provide the appropriate level of protection for information that is sensitive or vulnerable. Two-factor authentication is an authentication method that applies a stronger means of identifying the user. The Microsoft phone-based two-factor authentication solution allows users to receive their PINs sent as messages to their phones, and then they enter their PINs as a second password to log on to their services.
40.	What are the procedures for identifying, reporting and responding to suspected security incidents and violations?	First, there are robust procedures offered by Microsoft that enable the **prevention** of security incidents and violations arising in the first place and **detection** if they do occur. Specifically: a. Microsoft implements 24 hour monitored physical hardware. Data centre 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.

Ref.	Question / requirement	Guidance
		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. In addition, Microsoft has anti-malware controls to help avoid malicious software from gaining unauthorised access to customer data. Microsoft implements traffic throttling to prevent denial-of-service attacks, and maintains a set of Security Rules for managed code to help ensure that application cybersecurity threats are detected and mitigated before the code is deployed. c. Microsoft employs some of the world’s top experts in cybersecurity, cloud compliance, and financial services regulation. Its Digital Crimes Unit, for example, employs cyber experts, many of whom previously worked for law enforcement, to use the most advanced tools to detect, protect, and respond to cybercriminals. Its Cyber Defense Operations Center brings together security response experts from across Microsoft to help protect, detect, and respond 24/7 to security threats against Microsoft’s infrastructure and Online Services in real-time. General information on cybersecurity can be found here. d. Microsoft conducts a risk assessment for Azure at least annually to identify internal and external threats and associated vulnerabilities in the Azure environment. Information is gathered from numerous data sources within Microsoft through interviews, workshops, documentation review, and analysis of empirical data. The assessment follows a documented process to produce consistent, valid, and comparable results year over year. e. Wherever possible, human intervention is replaced by an automated, tool-based process, including routine functions such as deployment, debugging, diagnostic collection, and restarting services. Microsoft continues to invest in systems automation that helps identify abnormal and suspicious behaviour and respond quickly to mitigate security risk. Microsoft is continuously developing a highly effective system of automated patch deployment that generates and deploys solutions to problems identified by the monitoring systems—all without human intervention. This greatly enhances the security and agility of the service.

Ref.	Question / requirement	Guidance
		f. Microsoft allows customers to monitor security threats on their server by providing access to the Azure Security Center, Office 365 Advanced Threat Analytics, Azure Status Dashboard, and the Office 365 Service Health Dashboard, among other online resources. g. Microsoft maintains 24-hour monitoring of its Online Services and records all security breaches. For security breaches resulting in unlawful or unauthorised access to Microsoft's equipment, facilities, or customer data, Microsoft notifies affected parties without unreasonable delay. Microsoft conducts a thorough review of all information security incidents. h. Microsoft conducts penetration tests to enable continuous improvement of incident response procedures. These internal tests help Microsoft cloud services security experts create a methodical, repeatable, and optimised stepwise response process and automation. In addition, Microsoft provides customers with the ability to conduct their own penetration testing of the services. This is done in accordance with Microsoft's rules of engagement, which do not require Microsoft's permission in advance of such testing. Second, if a security incident or violation is detected, Microsoft Customer Service and Support notifies customers by updating the Service Health Dashboard. Customers would have access to Microsoft's dedicated support staff, who have a deep knowledge of the service. Microsoft provides Recovery Time Objective (RTO) commitments. These differ depending on the applicable Microsoft service and are outlined further below. Finally, after the incident, Microsoft provides a thorough post-incident review report (PIR). The PIR includes: • An incident summary and event timeline. • Broad customer impact and root cause analysis. • Actions being taken for continuous improvement. If the customer is affected by a service incident, Microsoft shares the post-incident review with them.

Ref.	Question / requirement	Guidance
		Microsoft's commitment to cybersecurity and data privacy, including restrictions on access to customer data, are set forth in Microsoft's contracts with customers. In summary: • *Logical Isolation*. Microsoft logically isolates customer data from the other data Microsoft holds. This isolation safeguards customers' data such that the data cannot be accessed or compromised by co-tenants. • *24-Hour Monitoring & Review of Information Security Incidents*. Microsoft maintains 24-hour monitoring of its Online Services and records all security breaches. Microsoft conducts a thorough review of all information security incidents. For security breaches resulting in unlawful or unauthorised access to Microsoft's equipment, facilities, or customer data, Microsoft notifies affected parties without unreasonable delay. For more information regarding Microsoft's security incident management, refer to http://aka.ms/SecurityResponsepaper. • *Minimising Service Disruptions—Redundancy*. Microsoft makes every effort to minimise service disruptions, including by implementing physical redundancies at the disk, Network Interface Card ("NIC"), power supply, and server levels; constant content replication; robust backup, restoration, and failover capabilities; and real-time issue detection and automated response such that workloads can be moved off any failing infrastructure components with no perceptible impact on the service. • *Resiliency*. Microsoft's Online Services offer active load balancing, automated failover and human backup, and recovery testing across failure domains. • *Distributed Services*. Microsoft offers distributed component services to limit the scope and impact of any failures of a single component, and directory data is replicated across component services to insulate one service from another in the event of a failure.

Ref.	Question / requirement	Guidance
		- *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. - *Disaster Recovery Tests*. Microsoft conducts disaster recovery tests at least once per year. Customers also have access to the Azure Security Center, Office 365 Advanced Threat Analytics, Azure Status Dashboard, and the Office 365 Service Health Dashboard, among other online resources, which allow customers to monitor security threats on the cloud service provider's server.
41.	How is end-to-end application encryption security implemented to protect PINs and other sensitive data transmitted between terminals and hosts?	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

Ref.	Question / requirement	Guidance
		encryption protocols in the industry to provide a barrier against unauthorised access to our data. Proper key management is an essential element in encryption best practices, and Microsoft helps ensure that encryption keys are properly secured. Protocols and technologies examples include: a. Transport Layer Security (TLS), which uses symmetric cryptography based on a shared secret to encrypt communications as they travel over the network. b. Internet Protocol Security (IPsec), an industry-standard set of protocols used to provide authentication, integrity, and confidentiality of data at the IP packet level as it's transferred across the network. c. Office 365 servers using BitLocker to encrypt the disk drives containing log files and customer data at rest at the volume-level. BitLocker encryption is a data protection feature built into Windows to safeguard against threats caused by lapses in controls (e.g., access control or recycling of hardware) that could lead to someone gaining physical access to disks containing customer data. d. BitLocker deployed with Advanced Encryption Standard (AES) 256-bit encryption on disks containing customer data in Exchange Online, SharePoint Online, and Skype for Business. Advanced Encryption Standard (AES)-256 is the National Institute of Standards and Technology (NIST) specification for a symmetric key data encryption that was adopted by the US government to replace Data Encryption Standard (DES) and RSA 2048 public key encryption technology. 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.

Ref.	Question / requirement	Guidance
		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). 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.
42.	Are there procedures established to securely destroy or remove the data when the need arises (for example, when the contract terminates)?	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.
43.	Are there documented security procedures for safeguarding premises and restricted areas? If yes, provide	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.

Ref.	Question / requirement	Guidance
	descriptions of these procedures.	
44.	Are there documented security procedures for safeguarding hardware, software and data in the data centre?	Yes. These are described at length in the Microsoft Trust Center at microsoft.com/trust. 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
45.	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	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. 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

Ref.	Question / requirement	Guidance
	2 halves and each given to a different staff for custody).	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.
46.	Are the activities of privileged accounts captured (e.g. system audit logs) and reviewed regularly? Indicate the party reviewing the logs and the review frequency.	Yes. An internal, independent Microsoft team will audit the log at least once per quarter. More information is available at [microsoft.com/en-us/trustcenter/security/auditingandlogging]().
47.	Are the audit/activity logs protected against tampering by users with privileged accounts? Describe	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

Ref.	Question / requirement	Guidance
	the safeguards implemented.	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.
48.	Are file integrity checks in place to detect unauthorised changes to databases, files, programs and system configuration? Provide details of checks implemented.	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.
49.	Are password controls for critical applications/systems reviewed for compliance on a regular basis?	Yes. All access to production and customer data require multi-factor authentication. Use of strong password is enforced as mandatory and password must be changed on a regular basis.
50.	Is access to sensitive files, commands and services restricted and protected from manipulation? Provide details of	Yes. System level data such as configuration data/file and commands are managed as part of the configuration management system. Any changes or updates to or deletion of those data/files/commands will be automatically deleted by the configuration management system as anomalies. Further, Microsoft applies strict controls over access to customer data. Access to the IT systems that store customer data is strictly controlled via role-based access control (RBAC) and lock box processes. Access control is an automated process that follows the separation of duties principle and the principle of granting least privilege. This process ensures that the engineer

Ref.	Question / requirement	Guidance
	controls implemented.	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.
51.	Are remote access activities tracked and reviewed? What remote access controls are implemented?	Administrators who have rights to applications have no physical access to the production systems. So administrators have to securely access the applications remotely via a controlled, and monitored remote process called lockbox. All operations through this remote access facility are logged. Further, Microsoft applies strict controls over access to customer data. Access to the IT systems that store customer data is strictly controlled via role-based access control (RBAC) and lock box processes. Access control is an automated process that follows the separation of duties principle and the principle of granting least privilege. This process ensures that the engineer requesting access to these IT systems has met the eligibility requirements, such as a background screen, required security training, and access approvals. In addition, the access levels are reviewed on a periodic basis to ensure that only users who have appropriate business justification have access to the systems. This process ensures that the engineer requesting access to these IT systems has met the eligibility requirements. In addition, the Online Services include built-in approved Windows PowerShell Scripts, which minimise the access rights needed and the surface area available for misconfiguration. For more information regarding Microsoft identity and access management, see https://www.microsoft.com/en-us/trustcenter/security/identity.
52.	Does the service provider have a	*RBNZ Outsourcing Policy, Section B 2.2 (2) (a).*

Ref.	Question / requirement	Guidance
	disaster recovery or business continuity plan? Have you considered any dependencies between the plan(s) and those of your financial institution?	*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. ○ For Office 365, Microsoft maintains multiple copies of customer data across data centres for redundancy. ○ For Azure, Microsoft may copy customer data between regions within a given location for data redundancy or other operational purposes. For example, Azure GRS replicates certain data between two regions within the same location 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.

Ref.	Question / requirement	Guidance
		• *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 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.
53.	What are the recovery time objectives (RTO) of systems or applications	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

Ref.	Question / requirement	Guidance
	outsourced to the service provider?	- **SharePoint Online:** 6 hours or less - **Virtual Machines and Storage:** 30 minutes or less - **Virtual Network:** 1 hour or less
54.	What are the recovery point objectives (RPO) of systems or applications outsourced to the service provider?	- **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 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 ○ 45 minutes or less for Microsoft Exchange Online ○ 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 ○ 1 minute of less for Virtual Storage
55.	What are the data backup and recovery arrangements for your organisation's data that resides with the service provider?	**<u>Redundancy</u>** - 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,

Ref.	Question / requirement	Guidance
		Microsoft maintains multiple copies of customer data across for redundancy. For Azure, Microsoft may copy customer data between regions within a given location for data redundancy or other operational purposes. For example, Azure Globally-Redundant Storage replicates certain data between two regions within the same location for enhanced data durability in case of a major data centre disaster. **Resiliency** • Active/active load balancing. • Automated failover with human backup. • Recovery testing across failure domains. For example, Azure Traffic Manager provides load balancing between different regions, and the customer can use network virtual appliances in its Azure Virtual Networks for application delivery controllers (ADC/load balancing) functionality. Load balancing is also provided by Power BI Services, the Gateway, and Azure API Management roles. Office 365 services have been designed around specific resiliency principles that are designed to protect data from corruption, to separate data into different fault zones, to monitor data for failing any part of the ACID test, and to allow customers to recover on their own. **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.

Ref.	Question / requirement	Guidance
		• Outside-in monitoring raises alerts about incidents. • Extensive diagnostics provide logging, auditing, and granular tracing. **Simplification** • Standardised hardware reduces issue isolation complexities. • Fully automated deployment models. • Standard built-in management mechanism. **Human Backup** • Automated recovery actions with 24/7 on-call support. • Team with diverse skills on the call provides rapid response and resolution. • Continuous improvement by learning from the on-call teams. **Continuous Learning** • If an incident occurs, Microsoft does a thorough post-incident review every time. • Microsoft's post-incident review consists of analysis of what happened, Microsoft's response, and Microsoft's plan to prevent it in the future. • If the organisation was affected by a service incident, Microsoft shares the post-incident review with the organisation. **Disaster recovery tests** • Microsoft conducts disaster recovery tests at least once per year.
56.	How frequently does the service provider	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

Ref.	Question / requirement	Guidance
	conduct disaster recovery tests?	redundancy with offline functionality. Microsoft's redundant storage and its procedures for recovering data are designed to attempt to reconstruct customer data in its original or last-replicated state from before the time it was lost or destroyed. Microsoft maintains multiple live copies of data at all times. Live data is separated into "fault zones," which ensure continuous access to data. For Office 365, Microsoft maintains multiple copies of customer data across datacenters for redundancy. For Azure, Microsoft may copy customer data between regions within a given location for data redundancy or other operational purposes. For example, Azure Globally-Redundant Storage ("GRS") replicates certain data between two regions within the same location 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.
57.	Have you jointly tailored and tested your disaster recovery or business continuity plan with the service provider? If yes, please provide a report on the test results.	*You are welcome to raise this with your Microsoft contact if you have any questions about how your disaster recovery/business continuity plan would interface with that of Microsoft.* In general, it would be Microsoft that would need to take action to recover the Office 365 service in a disaster/business continuity situation. Any internal actions can be carried out by our organisation without coordinating with Microsoft.

Ref.	Question / requirement	Guidance
F. PRIVACY ***In addition to RBNZ requirements, FSIs in New Zealand are of course subject to privacy and data protection requirements under New Zealand law. This section looks at how the use of Microsoft's Online Services complies with these requirements.***		
58.	How does the service provider and the proposed solution comply with New Zealand privacy law requirements relating to the cloud?	*Office 365 can help you meet or exceed all the requirements in the Office of the Privacy Commissioner (OPC) checklist and guide. We hope that Office 365 will be able to play a part in helping many New Zealand organisations improve privacy, security, and service continuity disciplines in a cost effective way. For the most current and complete information privacy information, please refer to http://trust.office365.com/ and your Office 365 service agreement.*

Part 2: Contract Checklist

What are our contract documents?

Section B2 of the RBNZ Outsourcing Policy requires that all outsourcing arrangements must contain the prescribed contractual terms (as defined in Section 2.9 of the RBNZ Outsourcing Policy and described below). Additionally, the Privacy Commissioner has created a document called ‘Cloud Computing: A guide to making the right choices’, which contains some useful items to check are included in the contract. 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**[2]
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**[3] Materials available from the relevant **Trust Center**

What does this Part 2 cover?

The RBNZ Outsourcing Policy provides that, at a minimum, your agreement with the cloud services provider must address specified matters. Additionally, Section B2.9 (3) sets out terms that the RBNZ would expect but does not require. These are marked as Guidance (G) in the table below. This Part 2 sets out those specific

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

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

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.

Reference	Requirement	How and where is this dealt with in Microsoft's contract?
Section B2.9 (2) (a), The RBNZ Outsourcing Policy	(a) a provision that ensures continuing access, on arms-length commercial terms, to the relevant services and functions if the bank enters statutory management	The Financial Services Amendment ensures continuing access, on arms-length commercial terms, to the relevant services and functions if the customer enters statutory management.
Section B2.9 (3) (b), The RBNZ Outsourcing Policy	(c) (if a bank has entered into an outsourcing arrangement that is made through a parent or another related party) a term that enables the bank to ensure that it has parallel rights in relation to that outsourcing arrangement	Microsoft makes this commitment through the Financial Services Amendment.
Section B2.9 (3) G	(d) 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.

Reference	Requirement	How and where is this dealt with in Microsoft's contract?
Section B2.9 (3) G	(e) Commencement and end dates	Standard EA Enrollments have a three-year term and may be renewed for a further three-year term.
Section B2.9 (3) G	(f) 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 (at OST pages 10-14) 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 B2.9 (3) G **and** **Privacy Commissioner Cloud Computing: A guide to making the right choices, February 2013, p9.**	(h) 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 B2.9 (3) G	(i) The form in which data is to be kept and clear provisions	The customer will have the ability to access and extract its Customer Data stored in each Online Service at all times during the subscription and for a retention period of at least 90 days after it ends (see OST, page 5).

Reference	Requirement	How and where is this dealt with in Microsoft's contract?
	identifying ownership and control of data	Microsoft also makes specific commitments with respect to customer data in the OST. In summary, Microsoft commits that: 1. Ownership of customer data remains at all times with the customer (see OST, page 7). 2. Customer data will only be used to provide the online services to the customer. Customer data will not be used for any other purposes, including for advertising or other commercial purposes (see OST, page 7). 3. Microsoft will not disclose customer data to law enforcement unless it is legally obliged to do so, and only after not being able to redirect the request to the customer (see OST, page 7). 4. Microsoft will implement and maintain appropriate technical and organisational measures, internal controls, and information security routines intended to protect customer data against accidental, unauthorised or unlawful access, disclosure, alteration, loss, or destruction (see OST, page 8 and pages 10-14 for more details). 5. Microsoft will notify the customer if it becomes aware of any security incident, and will take reasonable steps to mitigate the effects and minimise the damage resulting from the security incident (see OST, pages 8 and 12-13). MBSA section 3 deals with confidentiality. Under this section Microsoft commits not to disclose confidential information (which includes customer data) to third parties (unless required by law) and to only use confidential information for the purposes of Microsoft's business relationship with the customer. If there is a breach of the contractual confidentiality obligations by Microsoft, the customer would be able to bring a claim for breach of contract against Microsoft.

Reference	Requirement	How and where is this dealt with in Microsoft's contract?
Section B2.9 (3) G **and** **Privacy Commissioner Cloud Computing: A guide to making the right choices, February 2013, p9.**	(j) Reporting requirements, including content and frequency of reporting and requirement to notify the customer if there is a material adverse development such as a security breach	The customer may monitor the performance of the Online Services via the administrative dashboard at any time, which includes information as to Microsoft's compliance with its SLA commitments. Microsoft also commits to providing the customer with Microsoft's audit reports, resulting from audits performed by a qualified, independent, third party security auditor that measure compliance against Microsoft's standards certifications (see OST, pages 13-14). 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.
Section B2.9 (2) (b), The RBNZ Outsourcing Policy **Section B2.9 (3) G** **and** **Privacy Commissioner**	(k) Audit and monitoring procedures (Including a provision that gives the Reserve Bank the ability to access documentation, and other information, that relates to the outsourcing arrangement.)	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 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.

Reference	Requirement	How and where is this dealt with in Microsoft’s contract?
Cloud Computing: A guide to making the right choices, February 2013, p9.		Microsoft makes available certain tools through the Service Trust Platform to enable customers to conduct their own virtual audits of the Online Services. Microsoft also provides customers with information to reconstruct financial transactions and develop audit trail information through two primary sources: Azure Active Directory reporting, which is a repository of audit logs and other information that can be retrieved to determine who has accessed customer transaction information and the actions they have taken with respect to such information, and Azure Monitor, which provides activity logs and diagnostic logs that can be used to determine the “what, who, and when” with respect to changes to customer cloud information and to obtain information about the operation of the Online Services, respectively. In addition, the Financial Services Amendment details the examination and audit rights that are granted to the customer and RBNZ. The “Regulator Right to Examine” sets out a process which can culminate in the regulator’s examination of Microsoft’s premises. To enable the customer to meet its examination, oversight and control, and audit requirements, Microsoft has developed specific rights and processes that provide the customer with access to information, Microsoft personnel and Microsoft’s external auditors. Microsoft will provide the customer with the following rights: 1. **Online Services Information Policy** Microsoft makes each Information Security Policy available to the customer, along with descriptions of the security controls in place for the applicable Online Service and other information reasonably requested by the customer regarding Microsoft security practices and policies. 2. **Audits of Online Services** On behalf of the customer, Microsoft will cause the performance of audits of the security of the computers, computing environment and physical 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. **Customer Compliance Program**

Reference	Requirement	How and where is this dealt with in Microsoft's contract?
		The customer also has the opportunity to participate in the Customer 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 Guidelines 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 B2.9 (3) G **and** **Privacy Commissioner Cloud Computing: A guide to making the right choices, February 2013, p9.**	(l) Business continuity and disaster recovery 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 (DPT, see OST page 13). Business continuity management also forms part of the scope of Microsoft's industry standards compliance commitments and regular third party compliance audits.
Section B2.9 (2) (b) and B2.9 (3)	(m) Confidentiality, privacy and security of information	The contractual documents include various confidentiality, privacy and security protections: • Microsoft will deal with customer data in accordance with the OST and makes various commitments in this respect.

Reference	Requirement	How and where is this dealt with in Microsoft's contract?
and **Privacy Commissioner Cloud Computing: A guide to making the right choices, February 2013, p9.**		- Microsoft commits to reimburse customer mitigation costs incurred as a consequence of a security incident involving customer data (see Financial Services Amendment, page 5 and OST, page 8 for the details of this commitment). The OST states that Microsoft and the customer each commit to comply with all applicable privacy and data protection laws and regulations. The customer owns its data that is stored on Microsoft cloud services at all times. The customer also retains the ability to access its customer data at all times, and Microsoft will deal with customer data in accordance with the terms and conditions of the Enrollment and the OST. Microsoft will retain customer data stored in the Online Service in a limited function account for 90 days after expiration or termination of customer's subscription so that the customer 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. (OST, page 7) 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. (OST, page 7) 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. (OST, page 36) Technical support personnel are only permitted to have access to customer information when needed. (OST, page 13)

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 (FSA, Section 3). Applicable limitation of liability provisions can be found in the MBSA. Microsoft further agrees to notify you if it becomes aware of any security incident, and to take reasonable steps to mitigate the effects and minimise the damage resulting from the security incident (OST).
Section B2.9 (3) G	(n) 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 B2.9 (3) G **and** **Privacy Commissioner Cloud**	(o) Dispute resolution arrangements and choice of law	In the event that a financial institution and Microsoft have a dispute, the choice-of-law and dispute resolution provisions would be clearly described in the agreement between Microsoft and the financial institution. MBSA clauses 10(g) and 10(h) contains terms that describe how a dispute under the contract is to be conducted. MBSA clause 11h deals with what countries laws apply if there is a legal dispute.

Reference	Requirement	How and where is this dealt with in Microsoft's contract?
Computing: A guide to making the right choices, February 2013, p9.		
Section B2.9 (3) G **and** **Privacy Commissioner Cloud Computing: A guide to making the right choices, February 2013, p9.**	(p) Liability and indemnity	MBSA clause 7 deals with liability. MBSA clause 6 sets out Microsoft's obligation to defend the regulated entity against third party infringement claims.
Section B2.9 (3) G	(q) 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 Microsoft's obligations in the OST, which Microsoft considers complies with section 30 of the Outsourcing Guidelines (OST, page 9). 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

Reference	Requirement	How and where is this dealt with in Microsoft's contract?
		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 (DPT, see OST, page 11). In addition, Microsoft's ISO/IEC 27018 certification requires Microsoft to ensure that its subcontractors are subject to the same security controls as Microsoft. Microsoft's ISO 27001 certification provides a layer of additional controls that impose stringent requirements on Microsoft's subcontractors to comply fully with Microsoft's privacy, security, and other commitments to its customers, including requirements for handling sensitive data, background checks, and non-disclosure agreements. Microsoft provides a website that lists subcontractors authorised to access customer data in the Online Services as well as the limited or ancillary services they provide. At least 6 months before authorising any new subcontractor to access Customer Data, Microsoft will update the website and provide the customer with a mechanism to obtain notice of that update. If the customer does not approve of a new subcontractor, then the customer may terminate the affected Online Service without penalty by providing, before the end of the notice period, written notice of termination that includes an explanation of the grounds for non-approval. If the affected cloud computing service is part of a suite (or similar single purchase of services), then any termination will apply to the entire suite. After termination, Microsoft will remove payment obligations for the terminated Online Services from subsequent customer invoices. (DPT, see OST, page 11)
Section B2.9 (3) G **and**	(r) 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

Reference	Requirement	How and where is this dealt with in Microsoft's contract?
Privacy Commissioner Cloud Computing: A guide to making the right choices, February 2013, p9.		its customers, given Microsoft's financial position set out in Microsoft's Annual Reports (see Part 1, Section 1 above).
Section B2.9 (3) G	(s) 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 (see OST, page 11). Microsoft also makes GDPR specific commitments (Attachment 4, OST) to all customers effective May 25, 2018.

Further Information

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

This document is not legal or regulatory advice and does not constitute any warranty or contractual commitment on the part of Microsoft. You should seek independent legal advice on your cloud services project and your legal and regulatory obligations.