Microsoft Cloud Services

Compliance with RBNZ Guidance on Cyber Resilience

Version: August 2021

Photo courtesy of Nico Rossi

Introduction

Microsoft is a leader in information security, and we embrace our responsibility to make the digital world a safer place. Microsoft welcomes the introduction by the Reserve Bank of New Zealand (*RBNZ*) of its Guidance on Cyber Resilience (the *Guidance*).

The Guidance will help RBNZ-regulated entities design and develop their own cyber resilience frameworks to govern and manage cyber risk, and shore up their resilience against information security incidents and their ability to respond swiftly and effectively in the event of a breach.

The Guidance provides a series of cyber resilience recommendations and has not been designed as a checklist of minimum requirements. However, the Guidance generally recommends that RBNZ-regulated entities:

- use good governance to manage cyber risk, including clearly defining information-security related roles and responsibilities;
- develop and maintain a cyber-resilience strategy and framework commensurate with their vulnerabilities and exposure to threats to their information assets;
- implement controls to protect information assets and undertake regular testing and assurance of the effectiveness of controls; and
- have in place processes enabling the sharing of information with external stakeholders, such as regulators, in a timely manner.

The Guidance draws on leading international and national cybersecurity standards, and closely mirrors the core Microsoft security framework: protect, detect and respond.

Deploying to Microsoft cloud services gives an RBNZ-regulated entity access to world-leading security technology, resources and controls, to help secure its data and operations, and meet the recommendations under the Guidance.

Microsoft cloud services deliver this information security capability and resilience against threats through:

- **Operations**: over 3,500 dedicated Microsoft cybersecurity professionals help protect, detect, and respond to threats – delivering security operations that work for your organisation.
- **Technology**: We use our experience to provide you with enterprise-class security technology.
- **Partnerships**: Microsoft is driving a broad set of technology, industry, and policy partnerships for a heterogeneous world.

This paper sets out each of the relevant recommendations from the Guidance, with particular focus on those recommendations relating to third party management, and maps those recommendations against Microsoft's cloud service controls, capabilities, functions, contract commitments and supporting information to help your RBNZ-regulated entity meet the recommendations.

Furthermore, Microsoft Consulting Services offers many information security consulting offerings, in addition to the Microsoft cloud product features and offerings described in this paper, that can help your RBNZ-regulated entity meet the recommendations under the Guidance.

RBNZ-regulated entities should also consult the "*Microsoft Cloud Services compliance checklist for financial institutions in New Zealand*" available on the Microsoft Trusted Cloud – Asia website to round out the picture of how Microsoft cloud services help achieve and exceed regulatory compliance.

Please be aware that this document is based on the current situation at the time of the creation of the document and all information contained within is provided "as-is." Taking into account that the regulatory environment as well as our catalogue of products and services and their respective technical features are continuously evolving, we recommend to always visit the Microsoft Trust Center (https://www.microsoft.com/en-nz/trust-center) and the Microsoft Service Trust Portal (https://servicetrust.microsoft.com) where Microsoft posts the most recent information related to its products and services. Information and views expressed in this document, including contract term references, URLs and other Internet Web site references, may change without notice.

You may copy and use this document for your internal reference purposes. You may modify this document for your internal reference purposes.

We hope you find our response useful, and we look forward to continuing the cloud conversation with you.

Microsoft Cloud Services: Compliance with RBNZ Guidance on Cyber Resilience

Issue	Guidance Sections	Compliance using Microsoft Cloud Services
Part D: Third-party management		
Planning (section D1)	D1.1 The entity should assess the criticality and sensitivity of the activities/data/processes being outsourced before entering into any outsourcing contracts.	In utilising Microsoft's cloud service offerings, an RBNZ-regulated entity is responsible for making an independent determination as to whether the technical and organisational security measures employed by Microsoft meet the entity's requirements, including with respect to the criticality and sensitivity of the activities, data, or processes being outsourced. Microsoft has cloud service offerings that leverage data classification and protection technologies to help RBNZ-regulated entities discover, classify, protect and monitor their sensitive data, across devices, apps, cloud services and on-premises. Examples of Microsoft Information Protection solutions can be found here, including Azure Information Protection, Office 365 Information Protection, Windows Information Protection, and Microsoft Cloud App Security. For example, customers could leverage the Azure Information Protection on-premises unified labelling scanner to inspect and automatically classify any files that Windows can index. Office 365 / Microsoft 365 also has further advanced capabilities that can help RBNZ-regulated entities meet higher levels of assurance and compliance. Examples include: • Advanced electronic discovery • Data governance and retention • Bring-your-own service encryption key • Control how Microsoft support engineers access your data • Privileged access management For Azure SQL, there are data security capabilities that support data discovery and classification, along with data masking and encryption.
Due Diligence (section D2)	D2.1 The entity should perform due diligence and document the due diligence results before signing any contracts, in order to evaluate the third parties' ability to meet the cyber resilience specification of the entity.	There are several avenues through which RBNZ-regulated entities can assess the information security capability of Microsoft and evaluate the design of the information security controls of Microsoft cloud services. Together they ensure that RBNZ-regulated entities can meet the recommendations under the Guidance to perform due diligence and evaluate Microsoft's ability to meet your cyber resilience specifications. First, Microsoft provides many built-in service capabilities to help you examine and verify access, control and service operation as part of your regular assurance processes. These include: • **Service Trust Portal** – for deep technical trust and compliance information, including recent audit reports for our services, as well as the International Standards Organisation (ISO) Statements of Applicability and penetration testing assessments. • **Compliance Manager** – a tool that provides detailed information about our internal controls, including test status and most recent test dates, and allows you to create your own assessments and monitor your own controls

Issue	Guidance Sections	Compliance using Microsoft Cloud Services
		• **Office 365 Audited Controls** – for detailed information about our internal control set, including mapping to international standards, and the most recent test dates • **Office 365 Management Activity API** – for visibility of user, admin, system and policy actions and events from your Office 365 and Azure Active Directory activity logs • **Office 365 Health Dashboard** – to immediately check service health, including current known services issues and ongoing resolution plans in progress • **Azure Security Center** – for visibility into the security state of your Azure resources and the ability to respond to threats and vulnerabilities • **Azure Advisor** – for continuous intelligent recommendation for how to further secure your Azure environment • **Microsoft Trust Center** – for information about data protection and security, including the location of our primary and backup data centres, subcontractor lists, and rules for when Microsoft service administrators have access to customer data. The Microsoft Security Policy Governance White Paper provides an overview of Microsoft's Security Policy Framework, with links to the key Microsoft Security Policy documents. RBNZ-regulated entities can also refer to the following resources to evaluate and assess Microsoft's security controls and capability (please note you may require a Microsoft account to access some of these documents): • Microsoft Cloud – Checklist for Financial Institutions in New Zealand available on the Microsoft Trusted Cloud – Asia website, created to assist RBNZ-regulated entities with their regulatory due diligence assessment; • Azure Response on Security, Privacy and Compliance to assess Microsoft security capability for Azure, and underpinning Office 365 / Microsoft 365 and Dynamics 365 cloud services; • Information Security Management System for Microsoft's Cloud Infrastructure; • Office 365 Security Incident Management; • Microsoft Azure Commercial System Security Plan and Microsoft Secure Score helps RBNZ-regulated entities find, assess and mitigate risks, and proactively manage security controls of Microsoft cloud services. Secure Score analyses an organisation's security based on regular activities and security settings of respective Microsoft cloud service offerings, giving RBNZ-regulated entities security posture visibility, report on areas that require attention, as well as recommendations for actions to further reduce the attack surface in your organization. Microsoft Secure Score covers a number of Microsoft cloud service workloads, devices, identity: see Office 365, Azure Security Center, Windows 10, and Azure Active Directory.
	D2.2 The entity could find it helpful to use a standard assessment questionnaire when doing its due diligence or develop a custom questionnaire according to the entity's risk appetite and its business requirement.	Through its Service Trust Portal, Microsoft has made available a template cloud security due diligence questionnaire (prepared by an independent third party) which RBNZ-regulated entities can use in assessing Microsoft's cyber resilience processes and controls. Refer to Microsoft's Risk Assessment & Compliance Guide for further information. RNBZ-regulated entities may also find the Microsoft Cloud - Checklist for Financial Institutions in New Zealand available on the Microsoft Trusted Cloud – Asia website helpful as a guidepost when conducting due diligence, including risk assessments, of Microsoft's Online Services.

Issue	Guidance Sections	Compliance using Microsoft Cloud Services
	D2.3 The entity could find it useful, when doing its due diligence, to obtain independent security attestation reports and certifications as a means to provide assurance as to the security posture of its third party service provider.	As discussed in more detail below in relation to **section D5 (Review and accountability)**, Microsoft engages regular (at least annual) audits of its cloud computing environment and services by qualified, independent third party security auditors, carried out in accordance with its Online Services DPA and Financial Services Amendment. The resulting audit reports are made available through the Service Trust Portal and within the Azure Portal in the Regulatory Compliance Blade covering Audit Reports Additional ongoing customer audit rights (under both the Online Services DPA and extended Financial Services Amendment contract terms for financial services customers) are discussed in more detail below.
Contract negotiation (section D3)	D3.1 The entity should use contracts with third parties to capture cyber security considerations that are commensurate with the entity's cyber risk appetite. This may include roles and responsibilities of each involved party regarding data access, incident response and communication, business continuity planning, termination, and data portability, etcetera.	Microsoft's commitments in regards to its technical and organisational security measures are detailed on its Product Terms site (formerly the Product Terms and Online Service Terms) and in the Online Services DPA. The Product Terms site and Online Services DPA form part of Microsoft's licensing agreements, and apply to all of Microsoft's cloud services (unless specifically identified otherwise). Microsoft also offers extended contractual terms to its financial services customers in its Financial Services Amendment, which addresses regulatory compliance requirements of financial institutions. An RBNZ-regulated entity is responsible for ensuring those commitments are commensurate with the entity's risk appetite. The commitments are described in more detail throughout this Paper, including in respect of Microsoft's data access commitments, incident response processes, business continuity and disaster recovery planning, termination and exit strategy guidance, and data portability.
	D3.2 The entity could find it useful to be fully informed about any related subcontracting by third parties that the entity has an outsourcing arrangement with. An entity could agree to allow a third-party to subcontract only when the subcontractors can fully meet the obligations existing between the entity and their outsourcing service providers.	In accordance with terms of its Online Services DPA, Microsoft may engage subprocessors to provide certain limited services which may involve processing by such subprocessors of customer and personal data. Microsoft remains responsible for the performance of its subprocessors, including their compliance with Microsoft's obligations under its DPA (see the "*Notice and Controls on use of Subprocessors*" section in the Online Services DPA). Microsoft makes available information about subprocessors at the Microsoft Online Services Subprocessor List, and RBNZ-regulated entities may subscribe to receive notifications of updates to this list by following the instructions that describe "My Library" functionality. As set out in the "*Notice and Controls on use of Subprocessors*" section in the Online Services DPA, Microsoft undertakes to ensure, via a written contract with each subprocessor that each subprocessor: • may only access and use any customer data or personal data to the extent necessary to deliver the services Microsoft has retained them to provide; • is prohibited from using such data for any other purpose; • is required to provide at least the level of data protection required of Microsoft under the Online Services DPA, and Microsoft agrees to oversee its subprocessors to ensure that those contractual obligations are met. Where Microsoft engages new subprocessors, it commits under the Online Services DPA to notify that appointment to its customers at least 6 months in advance of providing that subprocessor with customer data and at least 30 days in advance of providing that subprocessor with any personal data. If an RBNZ-regulated

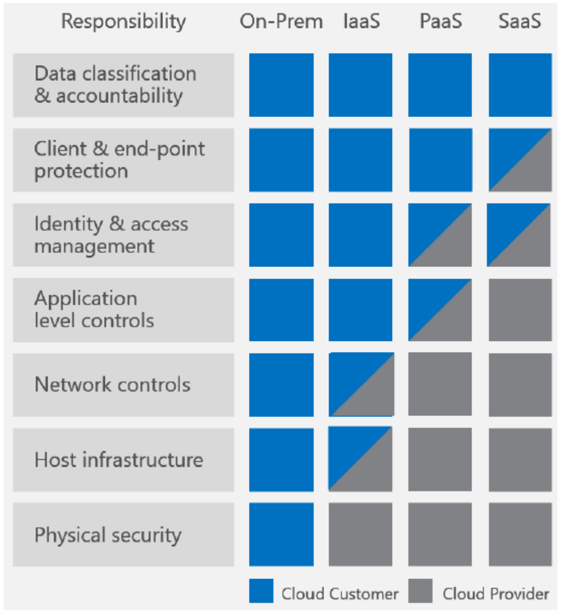
Issue	Guidance Sections	Compliance using Microsoft Cloud Services
		entity doesn't approve of a new subprocessor then the entity may terminate any affected subscription without penalty.
	D3.3 The entity may find it helpful to consider portability and interoperability of their data and applications and include provisions in its outsourcing contracts to avoid vendor lock-in.	Vendor lock-in is where a third-party vendor provides a unique service for which no suitable alternatives are available in the market or on-premises, or when the service does not offer good data portability solutions making it difficult to completely end the vendor relationship. Use of cloud will typically reduce vendor lock-in risks due to use of standardised technology that is flexible/portable and therefore easy to transfer. Microsoft is alive to these issues and has outlined the ways in which customers can reduce and mitigate risk in its Concentration Risk: Perspectives from Microsoft paper, and its suggestions to financial services organisations with respect to hybrid and multicloud strategies. At all times during its use of Microsoft's cloud services an RBNZ-regulated entity will have the ability to access, extract and delete Customer Data stored in each cloud service, including for example where it is transitioning to an alternative service provider or taking functions in-house. Customer data stored in Microsoft's cloud services will also remain available for 90 days after a subscription expires or is terminated for the customer to access, extract and/or delete. Financial institution customers can also request migration assistance from Microsoft, including to a different online service, as per Microsoft's commitment in the Financial Services Amendment. Data portability ensures an RBNZ-regulated entity can transfer its data to another solution, which is a foundational necessity in order to establish a working exit plan (discussed below in respect of **section D7**). At a global level, regulatory requirements relating to data portability led to the establishment of the SWIPO (Switching Cloud Providers and Porting Data) initiative. SWIPO is a multi-stakeholder group facilitated by the European Commission that has developed voluntary Codes of Conduct for the proper application of the EU Free Flow of Non-Personal Data Regulation / Article 6 "Porting of Data". Microsoft is a part of the SWIPO initiative and extends those commitments to its customers globally.
Ongoing cyber risk management (section D4)	The entity should consider the cyber risk associated with its third parties in each stage of its own capability building described in Part B. The entity should: D4.1.1 Clearly identify and document the cyber risk associated with using third-party service providers and update this information on a regular basis.	This document is intended to assist RBNZ-regulated entities identify and document the cyber risk associated with using Microsoft Cloud Services, and provide resources to help RBNZ-regulated entities updated the information regularly.
	D4.1.2 Design and verify security controls to detect and prevent intrusions from third-party connections	Under its extended Financial Services Amendment contract terms for financial services customers, Microsoft provides customers with the ability to conduct vulnerability and penetration testing of the customer's deployments in the cloud services or other similar testing as applicable to a specific cloud service that the customer is using. At least annually, Microsoft will commission third-party penetration testing against the

Issue	Guidance Sections	Compliance using Microsoft Cloud Services
		Online Services, including evidence of data isolation among tenants in the multi-tenant Online Services. Such information is available to customers through the Service Trust Portal. The Incident Management Implementation Guidance for Azure and Office 365 is a comprehensive document all customers can use to harden the security posture of their Microsoft cloud environment. It outlines the best methods for configuring the tenant for optimal security incident management: prevention, detection, alerts, anomalous activity monitoring, and post-incident investigations, made possible by in-product logging capability. Microsoft's Office 365 Security Incident Management and Microsoft Azure Commercial System Security Plan program documents also help RBNZ-regulated entities assess Microsoft's own incident management capabilities, policies and processes. It is important to note that security incident monitoring and detection is a shared responsibility. Microsoft cloud customers are responsible for detecting some types of security incidents (e.g. those that are wholly within the customer's control), and are not dependent upon Microsoft to detect those incidents. Microsoft provides the tools and resources outlined above to empower customers to identify security concerns and detect certain security incidents.
	D4.1.3 Ensure that third-party employee access to the entity's confidential data is tracked actively, based on the principle of least privilege.	Under its Online Service DPA, Microsoft commits to employing least privilege access mechanisms to control access to Customer Data. There is no standing access by Microsoft personnel to Customer Data and role-based access controls are employed to ensure that access to Customer Data required for service operations is for an appropriate purpose, for a limited time, and approved with management oversight. Further, Microsoft commits to ensuring that its personnel engaged in the processing of customer data (i) will process such data only on instructions from the relevant customer or as otherwise described in Microsoft's Online Services DPA, and (ii) will be obligated to maintain the confidentiality and security of such data even after their engagement ends. Microsoft shall provides periodic and mandatory data privacy and security training and awareness to its employees who have access to customer data in accordance with applicable data protection laws and industry standards. Microsoft logs, and enables customers to log, access to 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.
	D4.1.4 Integrate third parties that provide services for the entity's critical functions into the entity's response plan.	Microsoft has an Enterprise Business Continuity Management Program that aligns to the international standard for business continuity management, ISO 22301. Microsoft undertakes quarterly validation testing on business continuity processes across Azure, Dynamics and Office 365 with Validation Reports and ISO 22301 certificates available on the Microsoft Service Trust Portal. Microsoft has and will maintain adequate business continuity and disaster recovery plans intended to restore normal operations and the proper provision of its cloud services in the event of an emergency and in accordance with applicable laws and regulations.

Issue	Guidance Sections	Compliance using Microsoft Cloud Services
		The controls supporting such plans are validated through ISO 27001, ISO 22301 and SSAE 18 SOC 2 Type II audits, which are initiated for each cloud service at least annually and are performed by qualified, independent, third-party auditors. Under its Financial Services Amendment, Microsoft agrees to make available the necessary information to enable RBNZ-regulated entities to understand Microsoft's approaches to business continuity and disaster recovery, including providing notification of significant changes to Microsoft's business resumption and contingency plans, or other circumstances, that might have a serious impact on an entity's use of the cloud services. Each RBNZ-regulated entity can use the above resources to integrate the Microsoft commitments into the RBNZ-regulated entity's response plan.
	D4.2 The entity should assess the substitutability of the third parties that provide services for the entity's critical functions, and include transitioning to alternative service providers or performing critical services in-house in its business continuity plan that is commensurate with the criticality of the services and the entity's risk appetite.	As noted in D3.3, Microsoft provides customers with resources to help understand and address concentration risk and vendor lock-in, particularly through the use of hybrid-cloud or multi-cloud strategies. Microsoft notes that concentration risk is not unique to cloud services and remains relatively low in respect of public cloud services where there is a high level of competition. Refer to Microsoft's blog post on hybrid and multi-cloud strategies and its white paper on concentration risk for more information. Also refer to additional information in this Paper discussing access to, and portability of, customer data (including between cloud service providers) (**section D3.3**) and exit planning (**section D7.1**).
	D4.3 The entity could find it useful to conduct response and recovery testing with its third-party service providers and use the testing results to improve its response and recovery plans.	A customer is free at any time to conduct response and recovery testing within its Microsoft online services tenant and use the testing results to improve its response and recovery plans. Joint testing is not feasible in the case of a hyperscale cloud service provider, and is not necessary as there is no part of the business continuity plan that requires joint action. Microsoft's Enterprise Business Continuity Management Validation Report provides more information about Microsoft's business continuity plan validation and testing activities for Microsoft Online Services, available through the Service Trust Portal.
Review and accountability (section D5)	D5.1 The entity should regularly assess its third-party service providers' cybersecurity capabilities. The assessment can be achieved through the services providers' self-assessment, the entity's own assessment, or assessment by independent third parties. D5.2 The entity could find it useful to obtain assurance of its third-party service providers' cyber resilience capabilities by using tools such as certifications, external audits, summary of test reports, etcetera.	Microsoft facilitates compliance with audit and testing recommendations with respect to tests of the Microsoft cloud services through its "Auditing Compliance" contractual commitments in the Online Services DPA: "**Auditing Compliance** Microsoft will conduct audits of the security of the computers, computing environment and physical data centers that it uses in processing Customer Data and Personal Data, as follows: • Where a standard or framework provides for audits, an audit of such control standard or framework will be initiated at least annually. • Each audit will be performed according to the standards and rules of the regulatory or accreditation body for each applicable control standard or framework. • Each audit will be performed by qualified, independent, third party security auditors at Microsoft's selection and expense."

Issue	Guidance Sections	Compliance using Microsoft Cloud Services
		Each such audit will result in the generation of an audit report, which Microsoft will make available at https://servicetrust.microsoft.com/ (or another location identified by Microsoft) which customers can then use to assess the effectiveness of Microsoft's security practices and controls. Each audit report will clearly disclose any material findings of the auditor. Microsoft undertakes to promptly remediate any issues raised in an audit report to the satisfaction of the auditor." Other certifications and test reports, such as penetration testing assessments, are also available on the Service Trust Portal.
Documentation (section D6)	D6.1 The entity should maintain an up-to-date, comprehensive inventory of its third-party service providers and interconnection with other entities, as well as regularly updating the networking map of its external dependencies.	The Microsoft account team can assist an RBNZ-regulated customer in meeting this recommendation, for example by providing information to assist any mapping of dependencies on Microsoft.
Termination (section D7)	D7.1 The entity should establish a termination/exit strategy for the third parties that provide services related to the critical functions of the entity.	Microsoft recognises that exit plans are an effective risk mitigation mechanism for cloud service provider failures or other situations where an RBNZ-regulated entity is unable or unwilling to continue using their existing cloud service provider. For more information and guidance on cloud service exit planning, refer to Microsoft's cloud exit planning guideline blog post and its Exit planning for Microsoft Cloud Services white paper which provides a template approach towards exit planning and a summary of high-level migration scenarios specific to exiting Microsoft's cloud services. Microsoft's Financial Services Amendment allows financial services customers, on expiry or termination of a subscription for Microsoft cloud services, to extend the customer's use of such services on a month-to-month basis for up to 12 months. During such period, Microsoft will continue to provide the cloud services and the customer will be able to retrieve its data through Microsoft's standard processes and tools. The customer may also choose to engage with Microsoft Professional Services or another provider for assistance in transferring its data, including assistance with migration/transition to a different cloud service.
Outsourcing to Cloud Service Providers (section D8)	D8.1 The entity should inform the Reserve Bank about their outsourcing of critical functions to cloud service providers early in their decision-making process.	The Microsoft account team can assist an RBNZ-regulated customer in meeting this recommendation, for example by providing information about the online services to be deployed and the associated security controls.
	D8.2 The entity should evaluate and have a clear understanding of the rationale and the potential impacts of outsourcing to cloud service providers.	The implementation of cloud-based innovations and the shift to use of cloud computing services does not require any compromise of security or resilience. In many respects, hyperscale public cloud services are fundamentally more secure than on-premises software or private datacentres, and can provide superior overall capabilities when it comes to addressing challenges around security, compliance, privacy, operational resiliency, and data portability.

Issue	Guidance Sections	Compliance using Microsoft Cloud Services
		Microsoft is happy to discuss with RBNZ-regulated entities the potential impacts of outsourcing to the cloud, including in respect of specific use cases for relevant functions, activities or data sets.
	D8.3 The entity should be aware of the jurisdiction risk associated with data stored, processed and transmitted in the cloud, including data replicated for provision of backup or availability services. The entity should assess the potential legal risk, compliance issues and oversight limitations associated with outsourcing to cloud service providers.	Microsoft makes commitments in its Product Terms site (formerly OST) and Online Services DPA, in relation to its Core Online Services, to store customer data at rest in certain major geographic areas (each, a Geo). For example, in respect of Azure Core Services, if an RBNZ-regulated entity deploys a service within a Geo then, for that service, Microsoft will store the entity's Customer Data at rest within the specified Geo. Customers may access additional details pertaining to the data residency and transfer policies specific to a cloud service by visiting https://www.microsoft.com/en-us/TrustCenter/Privacy/where-your-data-is-located. Customer data that is transmitted or otherwise processed is not subject to geographical restrictions but instead subject to technical and organizational measures that comply with ISO 27001, ISO 27002, and ISO 27018 to protect such data. Customer data in transit is encrypted by default. Microsoft cannot control or limit the regions from which an entity, or that entity's end users, may access or move Customer Data. Microsoft offers contract terms in its Financial Services Amendment that specifically address regulatory compliance requirements for regulated financial institutions, including oversight of the outsourcing arrangement by the customer and its regulators.
	D8.4 The entity should carefully consider the different levels of roles and responsibilities when entering into an agreement with its cloud service provider using the shared responsibility model. The entity may refer to NCSC's high-level guidance on the shared responsibility model.	Where an RBNZ-regulated entity is utilising hyperscale cloud services, its cyber resilience strategy and/or framework should include: • details of how hyperscale cloud services technology will be used to manage cyber resilience; and • appropriate roles for Microsoft as cloud services provider, in each case, consistent with the customer-side and service-side controls in the shared responsibility model (see diagram below), and with contractual commitments in the Product Terms Site (formerly OST) and Online Services DPA (as described in this paper). The figure below describes how shared responsibility works across the cloud service models.

<table>
<tr><th>Issue</th><th>Guidance Sections</th><th>Compliance using Microsoft Cloud Services</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><th>Responsibility</th><th>On-Prem</th><th>IaaS</th><th>PaaS</th><th>SaaS</th></tr>
<tr><td>Data classification &amp; accountability</td><td>🟦</td><td>🟦</td><td>🟦</td><td>🟦</td></tr>
<tr><td>Client &amp; end-point protection</td><td>🟦</td><td>🟦</td><td>🟦</td><td>◩</td></tr>
<tr><td>Identity &amp; access management</td><td>🟦</td><td>🟦</td><td>◩</td><td>◩</td></tr>
<tr><td>Application level controls</td><td>🟦</td><td>🟦</td><td>◩</td><td>⬛</td></tr>
<tr><td>Network controls</td><td>🟦</td><td>◩</td><td>⬛</td><td>⬛</td></tr>
<tr><td>Host infrastructure</td><td>🟦</td><td>◩</td><td>⬛</td><td>⬛</td></tr>
<tr><td>Physical security</td><td>🟦</td><td>⬛</td><td>⬛</td><td>⬛</td></tr>
</table>
🟦 Cloud Customer ⬛ Cloud Provider
For more information, see:
• Microsoft’s White Paper on Shared Responsibilities for Cloud Computing and related Blog Post; and
• other information referred to in this Paper, particularly in relation to Microsoft’s internal audit controls and compliance.</td></tr>
<tr><td></td><td>D8.5 The entity should consider and make it clear in the outsourcing agreement about how data will be segregated if using a public cloud service provider.</td><td>Under its Financial Services Amendment, Microsoft commits to employing logical separation for the storage and processing of Customer Data to prevent commingling of such data with the data of other Microsoft customers. Tenant Isolation in Microsoft 365 and Isolation in the Azure Public Cloud provides more information on how Microsoft achieves logical separation.</td></tr>
<tr><td></td><td>D8.6 The entity may find it helpful, when conducting its own due diligence, to take account of the cloud service provider’s adherence to international standards as relevant.</td><td>Microsoft’s technical and organisational security measures comply with ISO 27001, ISO 27002, ISO 27018, and ISO 22301 and Microsoft commits to ensuring that its measures will comply with such standards at all times. Each Microsoft Core Online Service also complies with the SSAE 18 SOC 1 Type II and SSAE 18 SOC 2 Type II control standards and frameworks, as specified in the Product Terms site.</td></tr>
</table>

Issue	Guidance Sections	Compliance using Microsoft Cloud Services
		Microsoft will not eliminate ISO 27001, ISO 27002, ISO 27018, ISO 22301 or SSAE 18 SOC 1 Type II and SSAE 18 SOC 2 Type II (in relation to Core Online Services only), unless such control standards or frameworks are no longer used in the industry and are replaced with a successor (if any), as specified in the Product Terms site.
	D8.7 The assessment of the design and operating effectiveness of controls within the shared responsibility model (for both provider and the entity itself) should be commensurate with the impact of the outsourced functions/systems on the entity.	As noted earlier, in deploying or using Microsoft products, an RBNZ-regulated entity will be responsible for making an independent determination as to whether the technical and organisational measures implemented by Microsoft, and the design and operating effectiveness or those measures, are commensurate with the impact of the relevant outsourced functions or system on the entity. The information in this Paper is designed to assist RBNZ-regulated entities in making that assessment and identifying the shared responsibility.
Part A: Governance		
Cyber Resilience Strategy and Framework (Section A2)	Section A2 of the Guidance recommends that an RBNZ-regulated entity develop a clear cyber resilience strategy and framework commensurate with its vulnerabilities, exposure to threats and risk tolerance. The Guidance also recommends that an entity's cyber-resilience strategy should clearly define relevant roles and responsibilities, should be audited to assess implementation and effectiveness, and should be reviewed and updated regularly.	As noted previously, where an RBNZ-regulated entity is utilising hyperscale cloud services, its cyber resilience strategy and/or framework should address details of how hyperscale cloud services technology will, or could, be used to manage the entity's cyber resilience requirements in a manner consistent with the shared responsibility model. The information in this Paper is designed to assist RBNZ-regulated entities to develop, assess and review its cyber resilience strategy and framework. Microsoft cloud services comply with several security frameworks, such as ISO 27001, ISO 27002, ISO 27018, PCI- DSS and FedRAMP etc. These frameworks mandate Microsoft to implement a comprehensive Vulnerability Management Framework for continuous assessment of known and unknown threats. Microsoft commits to cloud security policy framework compliance offerings in the "*Security Practices and Policies*" section of the Online Services Data Protection Addendum (DPA) and are summarised at the Trust Centre Compliance Offerings page.
Culture and awareness (section A3)	Section A3 of the Guidance recommends that RBNZ-regulated entities should promote a culture that recognises that staff at all levels have important responsibilities in ensuring the entity's cyber resilience, including by developing and maintaining a programme for continuing cyber resilience training for staff at all levels.	The Microsoft account team can assist an RBNZ-regulated customer in meeting this recommendation, for example by providing training about how Microsoft online services' security controls and compliance settings can be utilised to better support cyber resilience. There are also a number of online resources that customers can utilise, for example through the online Security documentation, which provides technical guidance to help security professionals build and implement cybersecurity strategy, architecture, and prioritized roadmaps. Microsoft Defender for Office 365 provides attack simulation training for end users to help organisations understand their current security policies and practices, enabling end users to be training in different attack simulations.
Part B: Capability Building		
Identify (Section B1)	Section B1 of the Guidance recommends that an RBNZ-regulated entity should identify, classify according to criticality and sensitivity, record, and regularly update all of its critical functions, in order to	The detail in this Paper Is designed to assist RBNZ-regulated entities to meet its identification obligations in relation to capability. In particular: • as discussed above, Microsoft's security and data protection commitments are outlined in its Online Services DPA which help protect customer data against accidental or unlawful destruction, loss, or

Issue	Guidance Sections	Compliance using Microsoft Cloud Services
	enable the entity to prioritise the processes of protection, detection, response and recovery for each of these functions. Section B1 also recommends that an entity should: • identify and maintain up-to-date records of individual and system accounts, including those with remote access or privileged access rights; • identify network resources that support its critical functions, including external network links; and • conduct cyber risk assessments before new technologies are introduced as well as on a regular basis.	alteration, or unauthorized disclosure of, or access to, such data where that data is transmitted, stored or otherwise processed through use of Microsoft's cloud services; • Microsoft has implemented and commits to maintain specified security measures for customer data in the Core Online Services, including Personnel Roles and Responsibilities, Security Training, Asset Inventory and Asset Handling practices, Access Control practices and other security commitments, which are set out in Appendix A (Security Measures) to the Online Services DPA; • Microsoft has several cloud service offerings that can assist RBNZ-regulated entities discover and classify data; and • the information Microsoft provides can be used by RBNZ-regulated entities to help identify and assess cyber risk in connection with the entity's cloud services provided by Microsoft. The Capability Building sections of this Whitepaper are based on NIST's Cybersecurity Framework (CSF). Microsoft has published a guide for customers to understand how to Map Microsoft Cyber Offerings to: NIST CSF, CIS Controls, ISO27001:2013 and HITRUST CSF Both Azure and Azure Government maintains a FedRAMP High Provisional Authorization to Operate (P-ATO) issued by the FedRAMP Joint Authorization Board (JAB). Given the close alignment between NIST CSF and NIST SP 800-53 controls, existing Azure FedRAMP High authorizations provide strong customer assurances that Azure services in FedRAMP audit scope conform to the NIST CSF risk management practices. Also, through a validated assessment performed by HITRUST, a leading security and privacy standards development and accreditation organization, Office 365 is certified to the objectives specified in the NIST CSF. Microsoft would recommend, that in addition to the guidance provided in this document, that RBNZ-regulated entities adopt a Zero Trust approach to Security for Identities, Endpoints, Applications, Networks, Infrastructure, and Data.
Protect (Section B2)	Section B2 of the Guidance recommends that an RBNZ-regulated entity should have security controls in place, based on the identified critical functions, which allow it to: • ensure the continuity and availability of its information systems; • protect the integrity, confidentiality and availability of data and information while stored, in use or in transit; and • meet its business requirements while minimising the probability and potential impact of a cyberattack. Controls recommended in the Guidance include, but are not limited to: • system monitoring and installation of updates; • decommission and replacement of legacy systems where vulnerabilities cannot be patched or mitigated;	Microsoft's security capabilities, and avenues through which RBNZ-regulated entities can assess those capabilities, are described earlier in this Paper. See in particular sections D2, D4 and D5. Organisations can leverage Microsoft Azure Security capabilities to protect resources against Distributed Denial of Service attacks, protect files and emails across multiple devices, and classify and protect documents and emails.

Issue	Guidance Sections	Compliance using Microsoft Cloud Services
	- having appropriate system access controls in place (based on the principle of least privilege); and - having appropriate controls in place to identify and prevent data loss.	
Detect (Section B3)	Section B3 of the Guidance recommends that an RBNZ-regulated entity should have the right capabilities in place in terms of people, processes and technologies to monitor and detect cyber incidents and deviations from normal system activity, including: - documenting normal baseline performance for identified critical functions and supporting systems, so that deviations from the baseline can be detected and flagged for investigation; - having criteria in place to trigger alerts when anomalous activities occur; - having appropriate thresholds in place for triggering its incident response plan; - collection of sufficient information to support forensic investigation of events and incidents; and - regularly reviewing and testing its detection and monitoring capabilities.	As noted earlier (in relation to section D4.1.2) Microsoft has several resources available which can assist RBNZ-regulated entities to enhance their detection and monitoring capabilities when utilising Microsoft's cloud services, and configure their cloud services tenant for optimal security incident management. RBNZ-regulated entities can also refer to Microsoft's Office 365 Security Incident Management and Microsoft Azure System Security Plan program documents also help you assess Microsoft's own incident management capabilities, policies and processes. To support Detection and Response activities, Azure Sentinel is a cloud native, Security Information Event Management (SIEM) and Security Orchestration Automated Response (SOAR) solution that customers can leverage for alert detection, threat visibility, proactive hunting, and threat response. Additionally, Microsoft provide a range of security monitoring tools to support Protection, Detection and Response operations. Security Monitoring tools in Azure.
Respond and recover (Section B4)	Section B4 of the Guidance recommends that an RBNZ-regulated entity should have in place appropriate response and recovery plans for when a cyber incident or breach occurs. The Guidance recommends that an entity should: - regularly review and test its response and recovery plans to ensure their continued effectiveness; - have processes in place that enable it to collate and review information from cyber incidents and testing results, so that it can improve its response and recovery plans; and - have processes and procedures in place to conduct post-incident analyses of its cybersecurity incidents, and integrate its findings back into its response and recovery plans. .	Microsoft supports an entity's response and recovery processes through its "*Security Incident Notification*" commitments in the Online Services DPA: **"Security Incident Notification** If Microsoft becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data or Personal Data while processed by Microsoft (each a "Security Incident"), Microsoft will promptly and without undue delay (1) notify Customer of the Security Incident; (2) investigate the Security Incident and provide Customer with detailed information about the Security Incident; (3) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident." Microsoft makes the following further commitments as part of its security measures, detailed in Appendix A to the Online Services DPA: "Microsoft has implemented and will maintain for Customer Data in the Core Online Services the following security measures: … **Incident Response Process**

Issue	Guidance Sections	Compliance using Microsoft Cloud Services
		- Microsoft maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data. - For each security breach that is a Security Incident, notification by Microsoft (as described in the "Security Incident Notification" section above) will be made without undue delay and, in any event, within 72 hours. - Microsoft tracks, or enables Customer to track, disclosures of Customer Data, including what data has been disclosed, to whom, and at what time. Microsoft has developed a set of guidelines to help customers develop an Incident management response process that aligns to NIST's Computer Security Incident Handling Guide. **Service Monitoring**. Microsoft security personnel verify logs at least every six months to propose remediation efforts if necessary." Microsoft Defender 365 and Azure Defender provide a comprehensive set of security capabilities that can help RBNZ-regulated customers to comply with these recommendations. Defender provides protection across Identities, Endpoint, User Data, Cloud Applications and Infrastructure. Microsoft facilitates compliance with the recommendation to regularly review and test the Microsoft cloud service information security response plans, to ensure they remain effective and fit-for-purpose, through our "Auditing Compliance" contractual commitments in the Online Services DPA described earlier in this Paper.
Part C: Information Sharing		

Issue	Guidance Sections	Compliance using Microsoft Cloud Services
Channels (section C1) and Process (section C2)	Sections C1 and C2 of the Guidance recommend that RBNZ-regulated entities should plan for information sharing through trusted channels to facilitate the detection, response and recovery of its systems from cyber incidents, including: • sharing information with external stakeholders (for example, regulators and cybersecurity agencies) in a timely manner, including to meet any regulatory reporting requirements/timeframes; and • participation in information sharing groups and collectives to gather, distribute and assess information about cyber practices, cyber risk, and early warning indicators relating to cyber threats.	Microsoft regularly organizes workshops and other fora for regulated financial institution customers and regulators to share best practices relating to cybersecurity among other topics relevant to regulatory compliance. In addition, RBNZ-regulated entities can join Microsoft's Customer Assurance Program. This programme provides customers that opt in with access to additional cloud-based risk, compliance, security, privacy and audit information to provide the assurance needed when using Microsoft's cloud services. In addition to the self-service assurance resources referred to elsewhere in this Paper (including online resources such as the Service Trust Portal and Azure Security Centre, and Microsoft independent third party audit reports), the customer assurance program can provide RBNZ-regulated entities with direct access to Microsoft's engineering experts to assist with risk and compliance requirements. Microsoft's engineers can provide: • detailed responses to questions regarding: ○ how Microsoft meets compliance regulation; ○ your organisation's compliance configurations in the cloud; and ○ specific regulatory, risk and privacy topics; • onboarding and training in the use of learning resources and self-services tools relating to risk, compliance, security, privacy and data protection; and • hands-on support with risk and compliance assessment questionnaires. The customer assurance program also includes engagement pathways for customers to speak with industry peers about best practices.