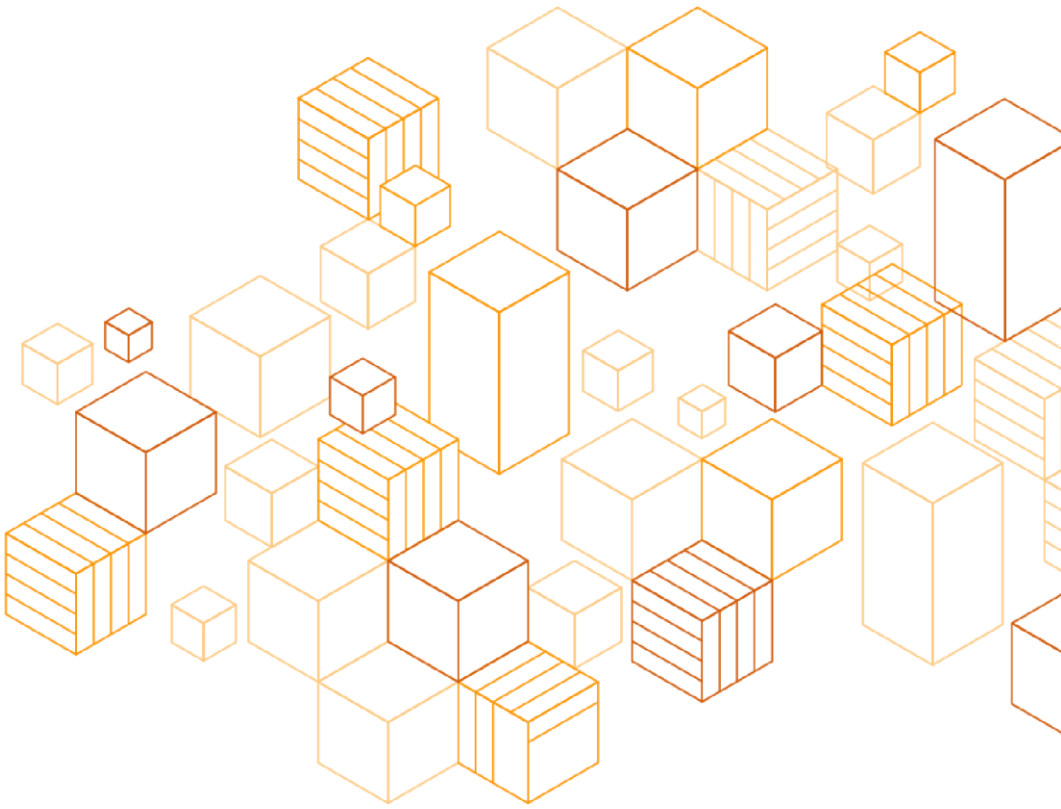
AWS User Guide to Financial Services Regulations and Guidelines in New Zealand

May 2022



Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current Amazon Web Services (AWS) product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. AWS products or services are provided “as is” without warranties, representations, or conditions of any kind, whether express or implied. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Contents

Abstract

This document provides information to assist financial services institutions in New Zealand that are regulated by the Reserve Bank of New Zealand as they accelerate their use of AWS Cloud services.

Introduction

The Reserve Bank of New Zealand (RBNZ) is the prudential regulator of financial institutions in New Zealand. RBNZ oversees banks, insurers, and non-bank deposit-takers.

In April 2020, RBNZ updated Outsourcing Policy BS11 (BS11). BS11 requires large banks (that is, New Zealand incorporated registered banks with liabilities, net of amounts owed to related parties, of NZD$10 billion or more) to have the legal and practical ability to control and execute outsourced functions, including via their use of cloud services. From April 2021, RBNZ regulated entities have also been given non-binding Guidance on Cyber Resilience which aims to raise awareness of, and promote accountability for, managing cyber risk within RBNZ regulated entities.

Although the use of AWS by RBNZ regulated entities substantially predates the release of the updated BS11 and Guidance on Cyber Resilience, AWS welcomes the increased clarity and guidance provided by RBNZ.

This document provides considerations for RBNZ regulated entities as they assess their responsibilities with regard to the following guidelines and requirements:

- **Reserve Bank of New Zealand, Outsourcing Policy, BS11, 2020** – This policy outlines the outsourcing requirements for large banks in New Zealand.
- **Reserve Bank of New Zealand, Guidance on Cyber Resilience, 2021** – This guidance sets out RBNZ's non-binding expectations of all RBNZ regulated entities regarding cyber resilience.

Taken together, RBNZ regulated entities can use this information to commence their due diligence and assess how to implement appropriate programs for their use of AWS.

Security and shared responsibility

Cloud security is a shared responsibility. AWS manages security of the cloud by ensuring that AWS infrastructure complies with global and regional regulatory requirements and best practices, but security in the cloud is the responsibility of the customer. What this means is that customers retain control of the security program they choose to implement to protect their own content, applications, systems, and networks, no differently than they would for applications in an on-premises data centre.

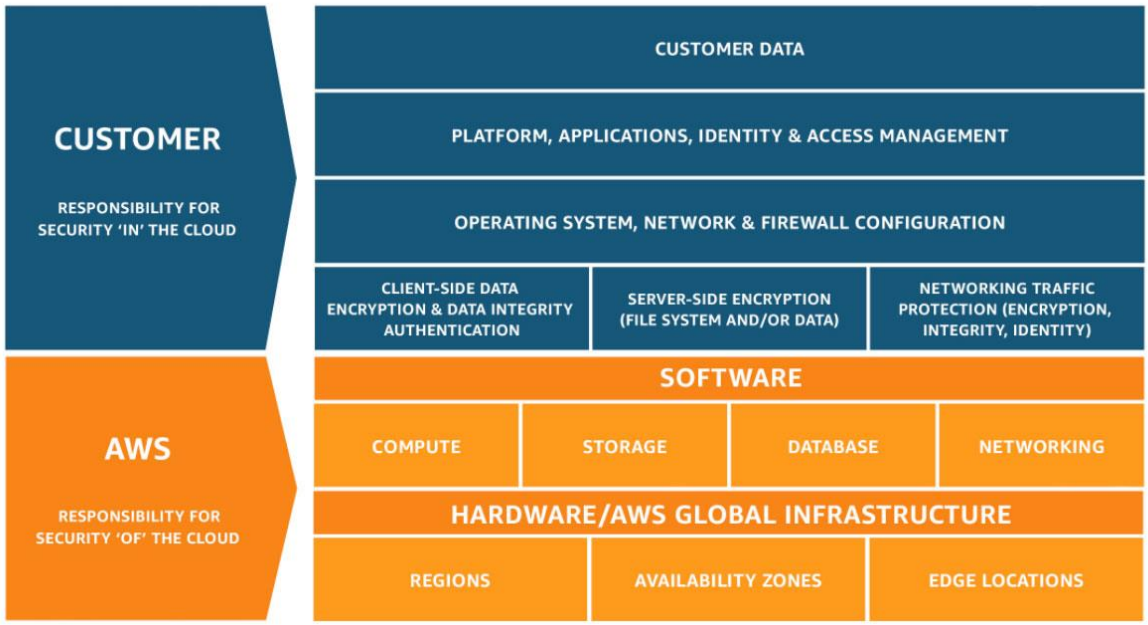


Figure 1: Shared Responsibility Model

The Shared Responsibility Model is fundamental to understanding the respective roles of the customer and AWS in the context of cloud security principles. AWS operates, manages, and controls the IT components, from the host operating system and virtualisation layer down to the physical security of the facilities in which the services operate. For abstracted services, such as Amazon Simple Storage Service (Amazon S3) and Amazon DynamoDB, AWS operates the infrastructure layer, the operating system, and platforms, and customers access the endpoints to store and retrieve data.

Security in the cloud

Customers are responsible for their security in the cloud. Much like a traditional data centre, the customer is responsible for managing the guest operating system (including installing updates and security patches) and other associated application software, as well as any applicable network security controls. Customers should carefully consider the services they choose, because their responsibilities vary depending on the services they use, the integration of those services into their IT environments, and applicable laws and regulations. It is important to note that when

using AWS services, customers maintain control over their content and are responsible for managing critical content security requirements, including:

- The content that they choose to store on AWS
- The AWS services that are used with the content
- The country and Region where they store their content
- The format and structure of their content and whether it is masked, anonymised, or encrypted
- How their data is encrypted and where the keys are stored
- Who has access to their content and how those access rights are granted, managed, and revoked

Because customers, rather than AWS, control these important factors, customers retain responsibility for their choices. Customer responsibility is determined by the AWS services that a customer selects. This selection, in turn, determines the amount of configuration work the customer must perform as part of their security responsibilities. For example, a service such as Amazon Elastic Compute Cloud (Amazon EC2) is categorized as Infrastructure as a Service (IaaS) and, as such, requires the customer to perform all of the necessary security configuration and management tasks. Customers that deploy an Amazon EC2 instance are responsible for management of the guest operating system (including updates and security patches), any application software or utilities installed by the customer on the instances, and the configuration of the AWS-provided firewall (called a security group) on each instance.

For abstracted services, such as Amazon Simple Storage Service (Amazon S3) and Amazon DynamoDB, AWS operates the infrastructure layer, the operating system, and platforms, and customers access the endpoints to store and retrieve data. Customers are responsible for managing their data (including encryption options), classifying their assets, and using Identity and Access Management (IAM) tools to apply the appropriate permissions.

Security of the cloud

AWS's infrastructure and services are approved to operate under several compliance standards and industry certifications across geographies and industries. Customers can use AWS's compliance certifications to validate the implementation and effectiveness of AWS's security controls, including internationally-recognized security best practices and certifications. You can learn more by downloading our whitepaper AWS & Cybersecurity in the Financial Services Sector. The AWS compliance program is based on the following actions:

- **Validate** that AWS services and facilities across the globe maintain a ubiquitous control environment that is operating effectively. The AWS control environment encompasses the people, processes, and technology necessary to establish and maintain an environment that supports the operating effectiveness of the AWS control framework. AWS has integrated applicable cloud-specific controls identified by leading cloud computing industry bodies into the AWS control framework. AWS monitors these industry groups to identify leading practices that customers can implement, and to better assist customers with managing their control environment.

- **Demonstrate** the AWS compliance posture to help customers verify compliance with industry and government requirements. AWS engages with external certifying bodies and independent auditors to provide customers with information regarding the policies, processes, and controls established and operated by AWS. Customers can use this information to perform their control evaluation and verification procedures, as required under the applicable compliance standard.

- **Monitor** through applicable security controls, that AWS maintains compliance with global standards and best practices.

AWS compliance programs

AWS has obtained certifications and independent third-party attestations for a variety of industry specific workloads; however, the following are of particular importance to RBNZ regulated entities:

- **ISO 27001** – ISO 27001 is a security management standard that specifies security management best practices and comprehensive security controls that follow the ISO 27002 best practice guidance. The basis of this certification is the development and implementation of a rigorous security program, which includes the development and implementation of an Information Security Management System which defines how AWS perpetually manages security in a holistic, comprehensive manner. For more information, or to download the AWS ISO 27001 certification, see the ISO 27001 Compliance webpage.

- **ISO 27017** – ISO 27017 provides guidance on the information security aspects of cloud computing, recommending the implementation of cloud-specific information security controls that supplement the guidance of the ISO 27002 and ISO 27001 standards. This code of practice provides additional implementation guidance for information security controls that is specific to cloud service providers. For more information, or to download the AWS ISO 27017 certification, see the ISO 27017 Compliance webpage.

- **ISO 27018** – ISO 27018 is a code of practice that focuses on protection of personal data in the cloud. It is based on ISO information security standard

27002 and provides implementation guidance on ISO 27002 controls that is applicable to public cloud Personally Identifiable Information (PII). It also provides a set of additional controls and associated guidance intended to address public cloud PII protection requirements that are not addressed by the existing ISO 27002 control set. For more information, or to download the AWS ISO 27018 certification, see the ISO 27018 Compliance webpage.

- **ISO 9001** – ISO 9001 outlines a process-oriented approach to documenting and reviewing the structure, responsibilities, and procedures that are required to achieve effective quality management within an organisation. The key to the ongoing certification under this standard is establishing, maintaining, and improving the organisational structure, responsibilities, procedures, processes, and resources in a manner where AWS products and services consistently satisfy ISO 9001 quality requirements. For more information, or to download the AWS ISO 9001 certification, see the ISO 9001 Compliance webpage.

- **PCI DSS Level 1** – The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard administered by the PCI Security Standards Council. PCI DSS applies to all entities that store, process, or transmit cardholder data (CHD) or sensitive authentication data (SAD), including merchants, processors, acquirers, issuers, and service providers. The PCI DSS is mandated by the card brands and administered by the Payment Card Industry Security Standards Council. For more information, or to request the PCI DSS Attestation of Compliance and Responsibility Summary, see the PCI DSS Compliance webpage.

- **SOC** – AWS System and Organisation Control (SOC) Reports are independent third-party examination reports that demonstrate how AWS achieves key compliance controls and objectives. The purpose of these reports is to help customers and their auditors understand the AWS controls that have been established to support operations and compliance. For more information, see the SOC Compliance webpage. There are five types of AWS SOC Reports:

    - **SOC 1:** Provides information about the AWS control environment that may be relevant to a customer's internal controls over financial reporting, as well as information for assessment of the effectiveness of internal controls over financial reporting.

    - **SOC 2:** Provides customers and their service users who have a business need with an independent assessment of the AWS control environment relevant to system security, availability, and confidentiality.

    - **SOC 2 (Amazon DocumentDB):** Provides customers and their service users who have a business need with an independent assessment of the AWS control environment relevant to Amazon DocumentDB system security, availability, and confidentiality.

- **SOC 2 Privacy Type I Report:** Provides customers with an independent assessment of AWS systems and the suitability of the design of AWS privacy controls.
- **SOC 3:** Provides customers and their service users who have a business need with an independent assessment of the AWS control environment relevant to system security, availability, and confidentiality, without disclosing AWS internal information.

By tying together governance-focused, audit-friendly service features with such certifications, attestations, and audit standards, AWS Compliance enablers build on traditional programs, helping customers to establish and operate in an AWS security control environment.

For more information about other AWS certifications and attestations, see the AWS Compliance Programs webpage. For information about general AWS security controls and service-specific security, see the Best Practices for Security, Identity, & Compliance website.

AWS Artifact

Customers can use AWS Artifact to review and download reports and details about more than 2,600 security controls. The AWS Artifact portal provides on-demand access to AWS security and compliance documents, including SOC reports, Payment Card Industry (PCI) reports, and certifications from accreditation bodies across geographies and compliance verticals.

AWS Global Infrastructure

The AWS Global Cloud Infrastructure comprises AWS Regions and Availability Zones. A Region is a physical location around the world where we cluster data centres. We call each group of logical data centres an Availability Zone (AZ). Each AWS Region consists of multiple, isolated, and physically separate AZs within a geographic area. Each AZ has independent power, cooling, and physical security and is connected via redundant, ultra-low-latency networks. AWS customers focused on high availability can design their applications to run in multiple AZs to achieve even greater fault-tolerance. Customers can learn more about these topics by downloading our Whitepaper on Amazon Web Services' Approach to Operational Resilience in the Financial Sector & Beyond.

AWS customers choose the AWS Region(s) in which their content and servers are located. This allows customers to establish environments that meet specific geographic or regulatory requirements. Additionally, this allows customers with business continuity and disaster recovery objectives to establish primary and backup environments in a location or locations of their choice. More information on our disaster

recovery recommendations is available at Disaster Recovery of Workloads on AWS: Recovery in the Cloud.

BS11 outsourcing policy

BS11 outlines RBNZ's requirements for outsourcing by large banks in New Zealand. RBNZ can also require other RBNZ regulated banks to comply with part, or all, of BS11 as a condition of their registration.

BS11 defines the measures that a bank must take when intending to enter into an outsourcing arrangement. Under BS11, "outsourcing" occurs when a bank uses a third-party (including a related party within the banking group) to perform services or functions on a regular or continuing basis that could be undertaken by the bank (excluding any services or functions listed on RBNZ's White list). BS11 requires banks to have the legal and practical ability to control and execute these outsourced functions in order to ensure that the outsourcing arrangement does not compromise the bank's ability to:

- Be effectively administered under statutory management, and operated for the purposes of continuing to provide and circulate liquidity to the financial system and wider economy
- Facilitate the carrying on of basic banking services by any new owner of all or part of the bank
- Address the impact that the failure of a service or function provider may have on the bank's ability to carry on all or part of the business of the bank

BS11 outlines the different considerations that banks must take when entering into outsourcing arrangements with any of the following:

- An independent third-party
- A subsidiary (or made through a subsidiary)
- Another related party (or made through a parent or other related party)
- Any other type of arrangement

A full analysis of BS11 is beyond the scope of this document. However, the following sections address the considerations in BS11 that most frequently arise in the interactions of AWS with RBNZ regulated banks.

Risk mitigation requirements when outsourcing to an independent third-party

Section B2.1(2) of BS11 defines two scenarios where a bank may outsource services or functions to an independent third-party such as AWS, either (1) directly with an independent third-party, or (2) through another related party (for example, where a bank enters into an arrangement with the outsourcing service provider through its parent company or an affiliate). Irrespective of the outsourcing scenario, BS11 requires a bank to ensure that the following risk mitigation requirements are in place at all times:

- **The business continuity programme / disaster recovery capability (BCP / DR capability) of the independent third-party is evidenced as being in place (Sections B2.2(2)(a) and B2.6(2)(a) of BS11).**

  The AWS infrastructure has a high level of availability and provides customers the features to deploy a resilient IT architecture. AWS has designed its systems to tolerate system or hardware failures with minimal customer impact.

  AWS provides customers with the flexibility to place instances and store data within multiple geographic Regions as well as across multiple Availability Zones within each Region. Each Availability Zone is designed as an independent failure zone. This means that Availability Zones are physically separated within a typical metropolitan region and are located in lower risk flood plains (specific flood zone categorization varies by Region). In addition to discrete uninterruptable power supply (UPS) and onsite backup generation facilities, they are each fed via different grids from independent utilities to further reduce single points of failure. Availability Zones are all redundantly connected to multiple tier-1 transit providers.

  Additionally, the AWS business continuity plan details the process that AWS follows in the case of an outage, from detection to deactivation. This plan has been designed to recover and reconstitute AWS by using a three-phased approach: Activation and Notification Phase, Recovery Phase, and Reconstitution Phase. This approach helps AWS perform system recovery and reconstitution efforts in a methodical sequence, aiming to maximize the effectiveness of the recovery and reconstitution efforts and minimize system outage time due to errors and omissions.

  A range of security and compliance reports are available for free through AWS Artifact, which gives AWS customers assurance regarding AWS business continuity testing and planning, including ISO 27001, and SOC 1 and 2 reports (see the AWS Compliance Programs mentioned earlier).

- **The prescribed contractual terms are included in the outsourcing arrangement (Sections B2.2(2)(b) and B2.6(2)(b) of BS11).**

A bank must have a contractual arrangement (outsourcing arrangement) in place with an outsourcing service provider. Section B2.9 of BS11 defines the prescribed contractual terms that a bank must include in an outsourcing arrangement.

Section B2.9(2)(a) of BS11 requires an outsourcing arrangement to include a contractual provision that ensures the continuing access to the third-party's relevant services and functions on "arms-length commercial terms" if the bank enters statutory management. RBNZ outlines that arms-length commercial terms includes a term that requires the bank to continue to pay for the service or function under the existing contract with the third-party.

Section B2.9(2)(b) of BS11 requires an outsourcing arrangement to also include a contractual provision that allows RBNZ to access documentation, and other information, that relates to the outsourcing arrangement (only if such documentation and information belongs to, or is accessible to, the third-party provider itself).

AWS customers have the option to enrol in an AWS Enterprise Agreement with AWS. AWS Enterprise Agreements give customers the option to tailor agreements that best suit their needs. AWS also provides an introductory guide to help banks assess the terms of the AWS Enterprise Agreement against BS11. For more information about AWS Enterprise Agreements, customers should contact their AWS representative.

- **The outsourcing arrangement is entered into the bank's compendium (Sections B2.2(2)(b) and B2.6(2)(b) of BS11).**

  AWS considers this an activity for a bank to independently complete.

RBNZ notification and non-objection

Section B3.1(d) of BS11 outlines that a bank is exempt from notifying RBNZ and obtaining a non-objection when it proposes to enter into an outsourcing arrangement directly with an independent third-party (such as AWS).

We note that under the non-binding Guidance on Cyber Resilience, RBNZ suggests that it is appropriate for RBNZ regulated entities to at least inform RBNZ about their outsourcing of critical functions to cloud service providers early in their decision-making process.

RBNZ's Guidance on Cyber Resilience

The Guidance on Cyber Resilience sets out RBNZ's non-binding expectations regarding cyber resilience of all RBNZ regulated entities, including registered banks, licensed non-bank deposit takers, licensed insurers and designated financial market infrastructures (RRIs).

The Guidance on Cyber Resilience states that RRIs may determine themselves how to meet RBNZ's expectations in a manner proportionate to their size, structure and operational environment and the nature, scope, complexity, and risk profile of their products and services. This gives RRIs the flexibility to address RBNZ's expectations in a number of different ways, taking into account the RRI's own specific needs and technologies provided the RRI can still demonstrate it understands the risks it is facing and is managing them appropriately.

A full analysis of the Guidance on Cyber Resilience is beyond the scope of this document. However, the following sections address the considerations that most frequently arise in interactions with RRIs. For a more detailed insight into the AWS control environment, customers may access our audit and assurance reports through AWS Artifact. Customers may also download the AWS Reserve Bank of New Zealand Guidance on Cyber Resilience (RBNZ-GCR) Workbook, which maps RBNZ's Guidance to control statements from the AWS Compliance Programs and the five pillars of the AWS Well-Architected Framework.

Part A: Governance

Part A of the Guidance on Cyber Resilience outlines foundational steps that RBNZ expects an RRI to take in order to adopt a sound cyber risk management framework. Although compliance with Part A is the responsibility of the RRI, the following table outlines AWS tools, services, security, identity, and compliance whitepapers, and AWS Training and Certification Programs to assist the RRI to develop and maintain an information security capability to meet RBNZ's expectations.

Area for consideration	Summary of RBNZ's Guidance	AWS services and resources
Section A1 - Board and Senior Management Responsibilities	**Sections A1.1 to A1.6** outline the roles and responsibilities of an RRI's board and senior management to ensure the cyber resilience of the RRI. The board is responsible for (a) the cyber resilience of an RRI, (b) understanding the RRI's cyber risk environment, (c) determining the RRI's cyber risk tolerance and appetite, (d) overseeing, developing and implementing a cyber resilience strategy and framework, and (e) ensuring senior executives and all staff with cyber resilience-related roles and responsibilities have the appropriate skills, knowledge, experience, and resources to perform their required tasks effectively. **Section A1.7**: requires senior management to regularly keep the board updated on the RRI's cyber resilience posture.	AWS considers this to be an action for the RRI to independently complete. AWS customers can use AWS tools, services, security, identity, and compliance whitepapers, and AWS Training and Certification Programs to develop and maintain an information security capability to help meet RBNZ's recommendations. AWS customers can access the AWS C-suite Guide to Shared Responsibility for Cloud Security and Data Safe Cloud eBook on the AWS Data Safe Cloud Checklist site to educate themselves on the benefits and risks of operating in the AWS Cloud, and to help build the necessary understanding of their cyber risk environment. AWS customers can utilise the following AWS services to assist with policy implementation and compliance monitoring: • AWS Control Tower allows AWS customers to set up and govern a secure, compliant, multi-account AWS environment based on best practices that AWS established by working with thousands of enterprises. • AWS Identity and Access Management (IAM) policies and AWS Organizations to implement service control policy (SCP) permission guardrails to ensure that users can only perform actions that meet corporate security and compliance policy requirements.

Area for consideration	Summary of RBNZ's Guidance	AWS services and resources
		• AWS CloudTrail to configure central logging of actions performed across their organisation and centrally aggregate data for AWS Config, enabling AWS customers to audit their environment for compliance, and react quickly to changes. • AWS Managed Services (AMS) and AWS Security Competency Partners to augment internal capabilities or to fill gaps where recruiting in-house resources is cost-prohibitive or while in-house capability is being developed. AWS customers can use the AWS Security Bulletins website to keep updated on security announcements and the AWS Service Health Dashboard for up-to-the-minute information on service availability in AWS Regions around the world. AWS customers can also use the information available in near real-time monitoring and alerting services such as AWS CloudTrail, Amazon CloudWatch, Amazon GuardDuty, and AWS Security Hub as inputs to board reports.
Section A2 - Cyber Resilience Strategy and Framework	The RRI should develop and maintain a cyber resilience strategy and framework that is commensurate with the RRI's vulnerabilities and exposure to threats. RBNZ outlines considerations that an RRI should take into account when designing a cyber resilience strategy and framework. RBNZ recommends that the RRI have an internal audit process to help monitor and measure the implementation progress, adequacy and effectiveness of its cyber resilience strategy and framework.	AWS considers this to be an action for the RRI to independently complete. The AWS resources and services outlined in Section A1 can help AWS customers address RBNZ's expectations. AWS customers can also use AWS Audit Manager to automate evidence collection, reduce manual effort associated with audits, and enable scaling of audit capability in the cloud as business grows.

Area for consideration	Summary of RBNZ's Guidance	AWS services and resources
Section A3 - Culture and Awareness	The RRIs should promote a culture that (a) recognises that staff at all levels have important responsibilities in ensuring its cyber resilience, and (b) a strong level of awareness of, and commitment to, cyber resilience business-wide. The RRI should develop and maintain a program for continuing cyber resilience training for staff at all levels, in line with recognised industry standards for cybersecurity.	AWS considers this to be an action for the RRI to independently complete. The AWS resources and services outlined in Section A1 may assist AWS customers with staff education. AWS also offers Amazon Security Awareness Training free of charge. AWS customers can access the AWS Security Bulletins (where AWS keeps its customers informed of security announcements) and the AWS Service Health Dashboard (that publishes up-to-the-minute information on service availability in AWS Regions around the world). AWS customers can also use the information available in near real-time monitoring and alerting services such as AWS CloudTrail, Amazon CloudWatch, Amazon GuardDuty, and AWS Security Hub as inputs to board reports.

Part B: Capability Building

Part B of the Guidance on Cyber Resilience follows the structure of the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity and outlines RBNZ's expectations for how an RRI should utilise and improve (where necessary) their identification, protection, detection, response, and recovery capabilities to lay the foundation for building robust cyber resilience.

Although compliance with Part B is the responsibility of the RRI, the following table outlines AWS tools, services, security, identity, and compliance whitepapers, and AWS Training and Certification Programs to assist the RRI to build the capability to help address RBNZ's expectations.

Area for consideration	Summary of RBNZ's Guidance	AWS services and resources
Section B1 - Identify	**Section B1.1**: The RRI should identify, classify (according to criticality and sensitivity), record, and regularly update all of its critical functions, including the information assets, key personnel roles, and processes that support these functions.	AWS considers this to be an action for the RRI to independently complete. AWS customers may use the following AWS services and resources to assist them: • AWS Config provides a detailed inventory of customers' AWS resources and configuration, and continuously records configuration changes. • Amazon CloudWatch provides data and actionable insights to monitor applications, understand and respond to system-wide performance changes, optimise resource utilisation, and get a unified view of operational health. • AWS Systems Manager gives visibility and control of customer infrastructure on AWS. AWS Systems Manager provides a unified user interface to view operational data from multiple AWS services and allows automation of operational tasks across AWS resources.

Area for consideration	Summary of RBNZ's Guidance	AWS services and resources
		AWS Systems Manager Inventory provides visibility into Amazon Elastic Compute Cloud (Amazon EC2) and on-premises computing.
	Section B1.2: The RRI should create and maintain an up-to-date inventory of all individual and system accounts (including those with remote access or privileged access rights) to ensure that access to sensitive information and supporting systems is kept on an as-needed basis only.	AWS considers this to be an action for the RRI to independently complete. AWS customers can use AWS Identity and Access Management (IAM) to create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources. IAM Access Analyzer helps customers analyse access across their AWS environments. AWS customers can also use AWS Single Sign-On (AWS SSO) to create, or connect, workforce identities in AWS once and manage access centrally across the customer's organization. AWS SSO can be configured to run alongside or replace AWS account access management via IAM.
	Section B1.3: The RRI should create and regularly update a map of its network resources, including IPs, devices, servers, and any external network links that support the RRI's critical functions.	AWS considers this to be an action for the RRI to independently complete. AWS customers can use AWS Network Manager console, which provides a dashboard that enables them to visualise and monitor their global network. It includes information about the resources in their global network, their geographic location, the network topology, and Amazon CloudWatch metrics and events, and enables customers to perform route analysis.
	Section B1.4: The RRI should make sure its identification and classification efforts are integrated with other relevant processes (for example, acquisition and change management) to ensure that inventories are kept up-	AWS considers this to be an action for the RRI to independently complete.

Area for consideration	Summary of RBNZ's Guidance	AWS services and resources
	to-date, accurate, and complete. Cyber risk assessments should be conducted before new or updated technologies, products, services, or processes are introduced, to identify any associated threats or vulnerabilities. **Section B1.5**: As an enhanced measure, the RRI should carry out risk assessments on a regular basis.	
Section B2 - Protect	**Section B2.1**: The RRI should have security controls in place, which allow them to achieve its security objectives and meet business requirements while minimising the probability and potential impact of a cyberattack. Security objectives should include ensuring the continuity and availability of the information systems as well as protection of the integrity, confidentiality and availability of data and information while stored, in use, or in transit. **Section B2.2**: The RRI should regularly update its security controls to ensure that the approaches it adopts remain commensurate to the RRI's critical functions, cyber threat landscape, and systemic importance.	AWS considers this to be an action for the RRI to independently complete. AWS defines the most important aspects of security "in" the cloud for customers through mechanisms like the AWS Well-Architected Framework (which includes a specific Financial Services Industry Lens) and the AWS Cloud Adoption Framework. Both of those frameworks have specific security areas, including detailed whitepapers, that help focus on how to design and build secure cloud environments.

Area for consideration	Summary of RBNZ's Guidance	AWS services and resources
	Section B2.3: The RRI should: (a) regularly monitor systems throughout their life cycle to identify weaknesses, (b) ensure that all available updates are installed and sufficient support is maintained (as appropriate), (c) implement and test additional layers of security where vulnerabilities are identified in systems, and (d) decommission and replace outdated legacy systems that have limited or no support, or have vulnerabilities that cannot be adequately patched or mitigated through segregation.	AWS considers this to be an action for the RRI to independently complete. AWS customers may use the following AWS services and resources to assist them: • AWS Config provides a detailed inventory of customers' AWS resources and configuration, and continuously records configuration changes. • Amazon CloudWatch provides data and actionable insights to monitor applications, understand and respond to system-wide performance changes, optimise resource utilisation, and get a unified view of operational health. • AWS Systems Manager gives visibility and control of customer infrastructure on AWS. AWS Systems Manager helps maintain security and compliance by scanning instances against customers' patch, configuration, and custom policies. The AWS Systems Manager Patch Manager feature helps customers select and deploy operating system and software patches automatically across large groups of Amazon Elastic Compute Cloud (Amazon EC2) or on-premises instances. Customers can use features of Amazon Virtual Private Cloud (Amazon VPC) to create virtual networks and to control access to systems via security groups and network access control lists.
	Section B2.4: The RRI should ensure that access to systems and information is controlled so that only staff who are authorised to access them can do so. Access should be restricted according to the principle of least privilege, and	AWS considers this to be an action for the RRI to independently complete. Using AWS Identity and Access Management (IAM), AWS customers can create and manage AWS users and groups, and use permissions to

Area for consideration	Summary of RBNZ's Guidance	AWS services and resources
	additional controls should be implemented for accounts with elevated privileges. The RRI should have processes in place to monitor system and information access and initiate an alert when unauthorised access is attempted or granted, and to monitor employees changing roles or leaving the RRI, to ensure that all access rights are updated accordingly.	allow and deny their access to AWS resources. IAM Access Analyzer helps customers analyse access across their AWS environments. AWS customers can also use AWS Single Sign-On (AWS SSO) to create, or connect, workforce identities in AWS once and manage access centrally across the customer's organization. AWS SSO can be configured to run alongside or replace AWS account access management via IAM. AWS Multi-factor Authentication (MFA) for highly privileged users is a security feature that augments user name and password credentials. MFA requires users to prove physical possession of a hardware MFA token or MFA-enabled mobile device by providing a valid MFA code.
	Section B2.5: The RRI should have policies, procedures and controls in place for change management and ensure that cyber security is considered throughout the life cycle of the change management process.	AWS considers this to be an action for the RRI to independently complete.
	Section B2.6: The RRI should implement screening and background checks for all new employees and contractors before they are hired/contracted. When an employee is changing responsibilities, the RRI should ensure that all access rights that are not necessary for the employee's new responsibilities are revoked in due time. Employees in sensitive positions (for example, those	AWS considers this to be an action for the RRI to independently complete. AWS customers can use IAM Access Analyzer to analyse access across their AWS environments.

Area for consideration	Summary of RBNZ's Guidance	AWS services and resources
	who change to roles requiring privileged access to critical systems or who become high-risk staff) should be pre-screened.	
	Section B2.7: The RRI should have strong controls in place to identify and prevent data loss through removal from the RRI's systems.	AWS considers this to be an action for the RRI to independently complete. AWS customers can use Amazon Macie, a fully managed data security and data privacy service that uses machine learning and pattern matching to discover and protect sensitive data on AWS. Amazon Macie maintains a growing list of sensitive data types that include common personally identifiable information (PII) and other sensitive data types as defined by data privacy regulations, such as the European Union's General Data Protection Regulation (GDPR), the Payment Card Industry Data Security Standard (PCI-DSS), and the US Health Insurance Portability and Accountability Act (HIPAA). Amazon Macie also allows customers to add custom-defined data types to enable Macie to discover proprietary or unique sensitive data for their businesses.
	Section B2.8: As an enhanced measure, the RRI should adopt a 'resilience by design' approach to designing its systems, processes, products, and services. This means embedding the resilience measures within the systems, processes, products, and services from the first stage of design and development.	AWS considers this to be an action for the RRI to independently complete. AWS customers may refer to the Reliability Pillar of the AWS Well-Architected Framework (which includes a specific Financial Services Industry Lens). A whitepaper on Amazon Web Services' Approach to Operational Resilience in the Financial Sector & Beyond is also available for download.

Area for consideration	Summary of RBNZ's Guidance	AWS services and resources
	Section B2.9: As an enhanced measure, the RRI could find it useful to implement automated mechanisms that can isolate affected information assets in the case of an adverse event, as appropriate.	AWS considers this to be an action for the RRI to independently complete. AWS customers may refer to the Reliability Pillar of the AWS Well-Architected Framework (which includes a specific Financial Services Industry Lens).
Section B3 - Detect	**Section B3.1**: The RRI should document normal baseline performance for critical functions and supporting systems, and set alert thresholds so that any deviation from the baseline can be detected and anomalous activities and events flagged for investigation. The RRI should have the right people, processes, and technologies in place to support these activities. These capabilities should be regularly reviewed, tested, and updated.	AWS considers this to be an action for the RRI to independently complete. AWS customers can use the following AWS services and tools to assist: • AWS Config to create resource baselines for supported AWS resources within their accounts (for example, Amazon Elastic Compute Cloud (Amazon EC2) instances, Amazon Elastic Block Store (Amazon EBS) volumes, security groups, and Amazon Virtual Private Cloud (Amazon VPC)) by creating configuration items for each resource, which includes metadata, attributes, relationships, and current configuration. AWS Config allows customers to continuously audit and assess the overall compliance of AWS resource configurations with organisational policies and guidelines. • AWS CloudTrail to discover and troubleshoot security and operational issues by capturing a comprehensive history of changes that occurred in an AWS account within a specified period of time. • Amazon GuardDuty to continuously monitor for malicious activity and unauthorised behaviour to protect customer AWS accounts and workloads. • Amazon Detective to automatically collect log data from AWS resources and use machine learning, statistical analysis, and graph

Area for consideration	Summary of RBNZ's Guidance	AWS services and resources
		theory to build a linked set of data that enables faster and more efficient security investigations.
	Section B3.2: The RRI should define an alert threshold for monitoring and detection systems in order to trigger and facilitate the incident response plan.	AWS considers this to be an action for the RRI to independently complete. AWS customers can use the following AWS services and tools to assist: • AWS Config to create resource baselines for supported AWS resources within their accounts (for example, Amazon Elastic Compute Cloud (Amazon EC2) instances, Amazon Elastic Block Store (Amazon EBS) volumes, security groups, and Amazon Virtual Private Cloud (Amazon VPC)) by creating configuration items for each resource, which includes metadata, attributes, relationships, and current configuration. AWS Config allows customers to continuously audit and assess the overall compliance of AWS resource configurations with organisational policies and guidelines. • AWS CloudTrail to discover and troubleshoot security and operational issues by capturing a comprehensive history of changes that occurred in an AWS account within a specified period of time. • Amazon GuardDuty to continuously monitor for malicious activity and unauthorised behaviour to protect customer AWS accounts and workloads. • Amazon Detective to automatically collect log data from AWS resources and use machine learning, statistical analysis, and graph theory to build a linked set of data that enables faster and more efficient security investigations.
	Section B3.3: The RRI should ensure that the relevant staff are trained to be able to identify and report anomalous	AWS considers this to be an action for the RRI to independently complete.

Area for consideration	Summary of RBNZ's Guidance	AWS services and resources
	activities, events, and incidents. This training should be updated regularly to be commensurate with any changes to the RRI's cyber threat environment.	AWS customers can use the free digital courses, classroom-based training, and AWS certifications offered by AWS Training and Certification Programs to develop and maintain an information security capability to help customers meet RBNZ's recommendations. A wide range of AWS security, identity, and compliance whitepapers are also available for download to help keep staff skills current and relevant. AWS also offers Amazon Security Awareness Training free of charge.
	Section B3.4: The RRI should incorporate multiple layers in its detection controls, including people, processes, and technology. These controls should have the capability to detect cyberattacks and isolate the point of corruption.	AWS considers this to be an action for the RRI to independently complete. AWS customers can use the following AWS services and tools to assist: • AWS Config to create resource baselines for supported AWS resources within their accounts (for example, Amazon Elastic Compute Cloud (Amazon EC2) instances, Amazon Elastic Block Store (Amazon EBS) volumes, security groups, and Amazon Virtual Private Cloud (Amazon VPC)) by creating configuration items for each resource, which includes metadata, attributes, relationships, and current configuration. AWS Config allows customers to continuously audit and assess the overall compliance of AWS resource configurations with organisational policies and guidelines. • AWS CloudTrail to discover and troubleshoot security and operational issues by capturing a comprehensive history of changes that occurred in an AWS account within a specified period of time. • Amazon GuardDuty to continuously monitor for malicious activity and unauthorised behaviour to protect customer AWS accounts and workloads. • Amazon Detective to automatically collect log data from AWS resources and use machine learning, statistical analysis, and graph

Area for consideration	Summary of RBNZ's Guidance	AWS services and resources
		theory to build a linked set of data that enables faster and more efficient security investigations. • AWS Marketplace to utilise third-party intrusion prevention and intrusion detection systems to alert administrators of malicious activity and policy violations, as well as identifying and taking action against attacks.
	Section B3.5: The RRI should ensure that its detection and monitoring capabilities allow for sufficient information collection to support forensic investigation of events and incidents. Information, systems, and data logs should be backed up to a secure location and have controls in place to ensure the logs remain accurate, uncompromised, and free from interference.	AWS considers this to be an action for the RRI to independently complete. Third-party products that are available through AWS Marketplace can assist customers in implementing this capability. Logs can be backed up to Amazon Simple Storage Service (Amazon S3) which can be configured to prevent unauthorised access.
	Section B3.6: The RRI should ensure that analysis of the information collected from the monitoring of systems and user activity is carried out in a timely manner; this analysis should be used to enhance detection capabilities, tactics, and incident response process.	AWS considers this to be an action for the RRI to independently complete. AWS customers can use Amazon Detective to automatically collect log data from AWS resources and use machine learning, statistical analysis, and graph theory to build a linked set of data that enables faster and more efficient security investigations.
	Section B3.7: The RRI should conduct security tests on its systems and	AWS considers this to be an action for the RRI to independently complete.

Area for consideration	Summary of RBNZ's Guidance	AWS services and resources
	networks to detect weaknesses that could be exploited by a cyberattack or leave them exposed to a cyber incident. Tests should be conducted regularly, as well as upon a major change to the RRI's cyber threat status. If necessary, tests should involve all relevant internal staff and departments that are critical to the cyber resilience of the RRI and relevant third-parties.	
Section B4 - Respond and Recover	**Section B4.1**: The RRI should have response and recovery plans in place for when a cyber incident or breach occurs. Plans should consider criticality of identified functions in enacting recovery, and clearly define recovery roles and responsibilities, escalation paths, and internal and external communication strategies. **Sections B4.1.1 to B4.1.6**: List the key considerations an RRI should consider when designing response and recovery plans for when a cyber incident or breach occurs.	AWS considers this to be an action for the RRI to independently complete. AWS customers can use the following AWS tools and services to assist: • The AWS Security Incident Response Guide, which presents an overview of the fundamentals of responding to security incidents within a customer's AWS Cloud environment. It focuses on an overview of cloud security and incident response concepts, and identifies cloud capabilities, services, and mechanisms that are available to customers who are responding to security issues. • The AWS whitepaper Disaster Recovery of Workloads on AWS: Recovery in the Cloud that outlines the best practices for planning and testing disaster recovery for workloads deployed to AWS, and offers different approaches to mitigate risks and meet the Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) for those workloads. • Amazon Detective, which automatically collects log data from AWS resources and uses machine learning, statistical analysis, and graph

Area for consideration	Summary of RBNZ's Guidance	AWS services and resources
		theory to build a linked set of data that enables faster and more efficient security investigations. • The AWS Incident Response Playbooks available on GitHub.
	Section B4.2: The RRI's cyber incident response and recovery plans should be aligned with its business continuity plan, as well as any other relevant plans.	AWS considers this to be an action for the RRI to independently complete. AWS customers can refer to the AWS Security Incident Response Guide and the AWS whitepaper Disaster Recovery of Workloads on AWS: Recovery in the Cloud to assist.
	Section B4.3: The RRI should ensure that the staff responsible for responding to cyber incidents and breaches have the required skills and training to address the situation appropriately.	AWS considers this to be an action for the RRI to independently complete. AWS customers can refer to the AWS Security Incident Response Guide to assist. Customers can also use AWS Managed Services (AMS) and AWS Security Competency Partners to augment internal capabilities or to fill gaps where recruiting in-house resources is cost-prohibitive or while in-house capability is being developed.
	Section B4.4: The RRI should utilise its process for initiating cyber incident alerts, outlined under 'Detect', to ensure that the right staff are aware of the incident or breach and have the most up-to-date information so that they can respond accordingly. **Section B4.5**: The RRI should regularly review and test its response and recovery plans, using a range of	AWS considers these to be actions for the RRI to independently complete. AWS customers can refer to the AWS Security Incident Response Guide and the AWS whitepaper Disaster Recovery of Workloads on AWS: Recovery in the Cloud to assist.

Area for consideration	Summary of RBNZ's Guidance	AWS services and resources
	different scenarios, to ensure their continued effectiveness. **Section B4.6**: The RRI should have processes in place that enable it to collate and review information from cyber incidents and testing results, so that it can constantly improve its response and recovery plans to be commensurate with the ever-evolving cyber risk environment. **Section B4.7**: The RRI should have processes and procedures in place to conduct post-incident analyses to identify root causes of its cybersecurity incidents, and integrate its findings back into its response and recovery plans. **Section B4.8**: As an enhanced measure, the RRI should consult with relevant external stakeholders to develop common response and recovery plans for cyber incidents that may affect the financial sector.	

Part C: Information Sharing

Part C of the Guidance on Cyber Resilience outlines how an RRI should prepare for sharing information through trusted channels, and have a process in place to ensure the such sharing is safe and timely, to promote the cyber resilience of the RRI and the New Zealand financial system.

Although compliance with Part C is the RRI's responsibility, AWS offers tools and features that an RRI can use to help it the meet the recommendations outlined in the Guidance on Cyber Resilience. The best source of security and privacy events related to AWS services is the AWS Security Bulletins website, where AWS keeps its customers appraised of security announcements, including AWS timelines for remediation. The AWS Service Health Dashboard publishes up-to-the-minute information on service availability in AWS Regions around the world. AWS customers can also use near real-time monitoring and alerting services such as AWS CloudTrail, Amazon CloudWatch, Amazon GuardDuty, and AWS Security Hub. AWS customers are advised to also keep their accounts up to date with accurate email addresses and security contact information to facilitate timely response and notification.

Part D: Third-Party Management

Part D outlines how an RRI should plan, screen, review, and use contracts to manage its relationship with third-party service providers, while also undertaking ongoing cyber risk management to ensure that cyber risks arising from third-parties are under control.

Part D addresses how an RRI should manage the cyber-risk management of *all* third-parties and activities that could be conducted under outsourcing arrangements (for example, third-party access to confidential data when engaging in business process outsourcing).

Although compliance with Part D is the responsibility of the RRI, the following table outlines AWS tools, services, security, identity, and compliance whitepapers, and AWS Training and Certification Programs to assist the RRI to build the capability to help address RBNZ's expectations.

Area for consideration	Summary of RBNZ's Guidance	AWS services and resources
Section D1. Planning	The RRI should assess the criticality and sensitivity of the activities, data, and processes that are being outsourced before entering into any outsourcing contracts.	AWS considers this to be an action for the RRI to independently complete.
Section D2. Due Diligence	The RRI should perform due diligence and document the due diligence results before signing any contracts, in order to evaluate a third-parties' ability to meet the cyber resilience specification of the RRI. As an enhanced measure, RBNZ recommends that the RRI may find it helpful to use a standard or custom assessment questionnaire and obtain independent security attestation reports and certifications to provide assurance as to the security posture of its third-party service provider.	AWS considers this to be an action for the RRI to independently complete. Since 2006, AWS has provided flexible, scalable, and secure IT infrastructure to businesses of all sizes around the world. AWS continues to grow and scale, allowing us to provide new services that help millions of active customers. AWS has an internal information security management system policy that establishes guidelines for protecting the confidentiality, integrity, and availability of customers' systems and content. AWS performs a continuous risk assessment process to identify, evaluate, and mitigate risks across the company. The process involves developing and implementing risk treatment plans to mitigate risks as necessary. The AWS risk management team monitors and escalates risks on a continuous basis, performing risk assessments on newly implemented controls at least every six months. Customers can evaluate the effectiveness of AWS-managed controls through audit reports and compliance evaluations available for free through AWS Artifact. Refer to the following AWS Audit Reports for additional details: SOC 2, PCI DSS, ISO 27001, and ISO 27017.
Section D3. Contract Negotiation	**Section D3.1**: The RRI should use contracts with third-parties to capture cyber security considerations that are commensurate with the RRI's cyber	AWS customers have the option to enroll in an Enterprise Agreement with AWS. Enterprise Agreements give customers the option to tailor agreements that best suit their needs.

Area for consideration	Summary of RBNZ's Guidance	AWS services and resources
	risk appetite (for example, roles and responsibilities of each involved party regarding data access, incident response and communication, business continuity planning, termination, and data portability).	
	Section D3.2: As an enhanced measure, RBNZ recommends that the RRI may find it useful to be fully informed about any related subcontracting by third-parties that the RRI has an outsourcing arrangement with.	AWS uses a number of third-party subcontractors to assist with the provision of its services. However, its subcontractors do not have access to customers' content. In addition, AWS only uses subcontractors that it trusts, and it uses appropriate contractual safeguards that it monitors to ensure that the required standards are maintained. Details of any subcontractors who have access to customer content, including personal data, are set out on the AWS website. See the AWS GDPR Data Processing Addendum (DPA) for more information.
	Section D3.3: As an enhanced measure, RBNZ recommends that the RRI may find it helpful to consider portability and interoperability of its data and applications and include provisions in its outsourcing contracts to avoid vendor lock-in.	AWS customers manage access to their content and to AWS services and resources, including the ability to import and export data. AWS provides services such as AWS Snowball to transfer large amounts of data into and out of the AWS Cloud by using physical storage appliances. For more information, see Cloud Storage on AWS. Additionally, AWS offers AWS Database Migration Service, a web service that customers can use to migrate a database from an AWS service to an on-premises database. Further, the agreements AWS has with its customers for the provision of AWS services allow customers to terminate their use of AWS services for convenience at any time and for any reason. AWS also provides customers with a post-termination period in which the customer can migrate off AWS. In the event that customers require further assistance during migration, AWS Professional Services can be engaged to provide assistance in the development of an exit strategy, as well as post-

Area for consideration	Summary of RBNZ's Guidance	AWS services and resources
		termination assistance. For additional information, contact your AWS Account Manager.
Section D4. Ongoing Cyber Risk Management	**Section D4.1**: The RRI should consider the cyber risk associated with its third-parties in each stage of its own capability building, as described in Part B. This includes, (a) clearly identifying, documenting, and regularly updating the cyber risk associated with using third-party service providers, (b) designing and verifying security controls to detect and prevent intrusions from third-party connections, (c) ensuring that third-party employee access to the RRI's confidential data is tracked actively (based on the principle of least privilege), and (d) integrating third-parties that provide services for the RRI's critical functions into the RRI's response plan.	AWS considers these as actions for the RRI to independently complete. However, AWS customers can access the AWS C-suite Guide to Shared Responsibility for Cloud Security and Data Safe Cloud eBook on the AWS Data Safe Cloud Checklist site to educate themselves on the benefit and risks of operating in the AWS Cloud, and to help build the necessary understanding of their cyber risk environment. Customers can evaluate the effectiveness of AWS managed controls through audit reports and compliance evaluations available for free through AWS Artifact. Customers manage access to their customer content and AWS services and resources. AWS offers an advanced set of access, encryption, and logging features to help customers do this effectively (such as AWS CloudTrail). AWS does not access or use customer content for any purpose other than as legally required and for maintaining the AWS services and providing them to our customers and their end users. Customers choose how their customer content is secured. AWS offers our customers strong encryption for customer content in transit or at rest, and AWS provides customers with the option to manage their own encryption keys.
	Section D4.2: The RRI should assess the substitutability of the third-parties that provide services for the RRI's critical functions, and include transitioning to alternative service providers or performing critical	AWS considers these as actions for the RRI to independently complete. AWS customers manage access to their content and to AWS services and resources, including the ability to import and export data. AWS provides services such as AWS Snowball to transfer large amounts of data into and out of AWS by using physical storage appliances. For more information, see Cloud Storage on AWS. Additionally, AWS offers AWS Database

Area for consideration	Summary of RBNZ's Guidance	AWS services and resources
	services in-house in its business continuity plan.	Migration Service, a web service that customers can use to migrate a database from an AWS service to an on-premises database.
	Section D4.3: As an enhanced measure, the RBNZ suggests that the RRI 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.	AWS considers this to be an action for the RRI to independently complete. AWS customers can consult the AWS whitepaper Disaster Recovery of Workloads on AWS: Recovery in the Cloud that outlines the best practices for planning and testing disaster recovery for workloads deployed to AWS, and offers different approaches to mitigate risks and meet the Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) for those workloads.
Section D5. Review and Accountability	The RRI should regularly assess its third-party service providers' cybersecurity capabilities. This can be achieved through the services providers' self-assessment, the RRI's own assessment, or assessment by independent third-parties. The RBNZ suggests that the RRI may find it useful to obtain assurance of its third-party service providers' cyber resilience capabilities by using tools such as certifications, external audits, and summary of test reports.	AWS considers this to be an action for the RRI to independently complete. AWS customers can use AWS Artifact to review and download reports and details about more than 2,600 security controls. The AWS Artifact portal provides on-demand access to AWS security and compliance documents, including SOC reports, PCI reports and certifications from accreditation bodies across geographies, and compliance verticals.
Section D6. Documentation	The RRI should maintain an up-to-date, comprehensive inventory of its third-party service providers and interconnection with other entities, as	AWS considers this to be an action for the RRI to independently complete.

Area for consideration	Summary of RBNZ's Guidance	AWS services and resources
	well as regularly update the networking map of its external dependencies.	
Section D7. Termination	The RRI should establish a termination or exit strategy for the third-parties that provide services related to the critical functions of the RRI.	AWS considers this to be an action for the RRI to independently complete. AWS customers manage access to their content and to AWS services and resources, including the ability to import and export data. AWS provides services such as AWS Snowball to transfer large amounts of data into and out of AWS by using physical storage appliances. For more information, see Cloud Storage on AWS. Additionally, AWS offers AWS Database Migration Service, a web service that customers can use to migrate a database from an AWS service to an on-premises database. Further, the agreements AWS has with its customers for the provision of AWS services allow customers to terminate their use of AWS services for convenience at any time and for any reason. AWS also provides customers with a post-termination period in which the customer can migrate off AWS. In the event that customers require further assistance during migration, AWS Professional Services can be engaged to provide assistance in the development of an exit strategy, as well as post-termination assistance. For additional information, contact your AWS Account Manager.

Area for consideration	Summary of RBNZ's Guidance	AWS services and resources
Section D8. Outsourcing to Cloud Service Providers	**Section D8.1**: The RRI should inform RBNZ about its outsourcing of critical functions to cloud service providers early in its decision-making process. **Section D8.2**: The RRI should evaluate and have a clear understanding of the rationale and the potential impacts of outsourcing to cloud service providers.	AWS considers this to be an action for the RRI to independently complete. We note that under BS11, banks are not required to notify RBNZ when they propose to enter into an outsourcing arrangement directly with an independent third-party (such as AWS). However, under this Section D8.1, RBNZ suggests that an AWS customer should inform RBNZ about their outsourcing of critical functions to cloud service providers early in their decision-making process.
	Section D8.3: The RRI should be aware of the jurisdiction risk associated with data that is stored, processed, and transmitted in the cloud, including data replicated for provision of backup or availability services. The RRI should assess the potential legal risk, compliance issues, and oversight limitations associated with outsourcing to cloud service providers.	AWS considers this to be an action for the RRI to independently complete. AWS customers choose the AWS Region or Regions in which their content is stored. Customers can replicate and back up their content in more than one AWS Region. AWS will not move or replicate a customer's content outside of its chosen AWS Regions without the customer's agreement, except as necessary to comply with the law or a binding order of a governmental body. For information on data privacy at AWS, visit the Data Privacy Center website.
	Section D8.4: The RRI 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 RRI may refer to National Cyber Security	AWS considers this to be an action for the RRI to independently complete. See the "Security and shared responsibility" section earlier in this document, where we outline how the implementation of controls to protect information assets is a shared responsibility between AWS and customers. For further resources on the shared responsibility model, you can visit the AWS shared responsibility model website.

Area for consideration	Summary of RBNZ's Guidance	AWS services and resources
	Centre's high-level guidance on the shared responsibility model.	
	Section D8.5: The RRI should consider and make it clear in the outsourcing agreement about how data will be segregated if using a public cloud service provider.	AWS considers this to be an action for the RRI to independently complete. AWS customer environments are logically segregated to prevent users and customers from accessing resources not assigned to them. Customers maintain full control over who has access to their data. Services which provide virtualised operational environments to customers (that is, Amazon Elastic Compute Cloud (Amazon EC2)) ensure that customers are segregated from one another and prevent cross-tenant privilege escalation and information disclosure via hypervisors and instance isolation. Customer instances have no access to physical disk devices, but instead are presented with virtualised disks. The AWS proprietary disk virtualisation layer automatically erases every block of storage before making it available for use, which protects one customer's data from being unintentionally exposed to another. Customers can further protect their data by using traditional file system encryption mechanisms, or, in the case of Amazon Elastic Block Store (Amazon EBS) volumes, by enabling AWS managed disk encryption.
	Section D8.6: As an enhanced measure, the RBNZ suggests that an RRI may find it helpful, when conducting its own due diligence, to take account of the cloud service provider's adherence to international standards.	AWS management has implemented a formal audit program that monitors and audits controls that are designed to protect against organisation risks and to protect customer data. This includes external independent assessments against regulatory, internal, and external control frameworks. The internal and external audits are planned, performed, and reported to the Audit Committee. The AWS compliance team performs and reviews the audit plan according to the documented audit schedule, and communicates the audit requirements based on a standard criteria that

Area for consideration	Summary of RBNZ's Guidance	AWS services and resources
		verifies compliance with the regulatory requirements and reported risk to the Audit Committee. AWS Security Assurance works with third-party assessors to obtain an independent assessment of risk management content and processes by performing periodic security assessments and compliance audits or examinations (for example, SOC, FedRAMP, ISO, PCI) to evaluate the security, integrity, confidentiality, and availability of information and resources. AWS management also collaborates with Internal Audit to determine the health of the AWS control environment and uses this information to fairly present the assertions made within the reports.
	Section D8.7: As an enhanced measure, the RBNZ suggests that the assessment of the design and operating effectiveness of controls within the shared responsibility model (for both provider and the RRI) should be commensurate with the impact of the outsourced functions or systems on the RRI.	AWS customers can use AWS Artifact to review and download reports and details about more than 2,600 security controls. The AWS Artifact portal provides on-demand access to AWS security and compliance documents, including SOC reports, PCI reports, and certifications from accreditation bodies across geographies and compliance verticals.

Next steps

Each organisation's cloud adoption journey is unique. In order to successfully execute your adoption, you need to understand your organisation's current state, the target state, and the transition that is required to achieve the target state. Knowing this will help you set goals and create work streams that will enable staff to thrive in the cloud.

The AWS Cloud Adoption Framework (AWS CAF) offers structure to help organisations develop an efficient and effective plan for their cloud adoption journey. Guidance and best practices prescribed within the framework can help you build a comprehensive approach to cloud computing across your organisation, throughout your IT lifecycle. The AWS CAF breaks down the complicated process of planning into manageable areas of focus.

Many organisations choose to apply the AWS CAF methodology with a facilitator-led workshop. To find more about such workshops, contact your AWS representative. Alternatively, AWS provides access to tools and resources for self-service application of the AWS CAF methodology at AWS Cloud Adoption Framework.

For RBNZ regulated entities in New Zealand, next steps would typically include the following:

- Contact your AWS representative to discuss how the AWS Partner Network, AWS Solution Architects, AWS Professional Services teams, and AWS Training instructors can assist with your cloud adoption journey. If you do not have an AWS representative, please contact us.
- Obtain and review a copy of the latest AWS SOC 1 and 2 reports, PCI-DSS Attestation of Compliance and Responsibility Summary, and ISO 27001 certification, from AWS Artifact (accessible via the AWS Management Console).
- Obtain and review a copy of the AWS Reserve Bank of New Zealand Guidance on Cyber Resilience (RBNZ-GCR) Workbook.
- Consider the relevance and application of the CIS AWS Foundations Benchmark available at CIS Amazon Web Services Foundations and the CIS Amazon Web Services Three-tier Web, as appropriate for your cloud journey and use cases. These industry-accepted best practices published by the Center for Internet Security go beyond the high-level security guidance already available, providing AWS users with clear, step-by-step implementation and assessment recommendations.
- Dive deeper on other governance and risk management practices as necessary in light of your due diligence and risk assessment, using the tools and resources

referenced throughout this whitepaper and in the "Additional resources" section that follows.

- Speak to your AWS representative about an AWS Enterprise Agreement and the introductory guide designed to help RBNZ regulated entities assess the AWS Enterprise Agreement against BS11.

Additional resources

For additional information, see:

- AWS Reserve Bank of New Zealand Guidance on Cyber Resilience (RBNZ-GCR) Workbook
- Using AWS in Context of NZ Privacy Considerations
- Financial Services Industry Lens – AWS Well-Architected Framework
- AWS Best Practices for DDoS Resiliency
- AWS Security Checklist
- An Overview of the Cloud Adoption Framework
- Best Practices for Security, Identity, & Compliance
- AWS Risk and Compliance

Document revisions

Date	Description
May 2022	First publication.