Reserve Bank of New Zealand
Te Pūtea Matua

RBNZ technology management

Policy statement | Te ito o te kaupapa-here

This policy sets out our principles for managing our technology to ensure the confidentiality, integrity, and availability of our information, to support changing business needs, and to ensure value for money.

It ensures our information technology is:

- modern, secure and resilient
- flexible and scalable
- comprehensive and coherent
- well-managed throughout its lifecycle.

This policy should be read in conjunction with the following:

- RBNZ protective security policies
- RBNZ Information and Data Management policy
- RBNZ risk management policies
- Personal information held by RBNZ (privacy).

Application | Te whakamahinga

This policy applies to all IT assets and services purchased, used, or maintained by Te Pūtea Matua.

Contents | Te kiko

Definitions | Tautuhi

IT Asset – any software or application, computer, mobile device, storage, network, or other physical infrastructure used to create, access, process, store, secure and exchange all forms of electronic data. This includes software or applications that are stored on the cloud.

Critical system – a system that is essential to the operation of Te Pūtea Matua, where a service interruption would cause reputational damage and / or significant cost to users. An IT asset that supports one or more critical systems is also a critical system.

1. Principles

1. We maintain an IT environment that is as simple as possible. We prioritise Software as a Service (SaaS) and develop bespoke applications only when other options are not suitable.
2. We prefer simple and standard solutions. We limit customisation of software and, where possible, meet business requirements through configuration.
3. We think cloud first, relieving the burden of maintaining and operating custom-built information technology infrastructure.
4. We use an enterprise perspective, seek solutions that integrate with existing technology and provide for a comprehensive and coherent enterprise architecture.

5. We are agile and user-centric, ensuring technology solutions support our people to work efficiently, collaboratively, and effectively.
6. We ensure the security and supportability of any technology before we implement a solution.
7. The secure and stable operation of our critical systems are our highest priority, and in the event of a disaster, are our priority for restoration.

2. Strategy and investment

As our IT assets must meet current and future needs of the RBNZ, we will:

- have a vision for information technology that aligns with the strategic direction for Te Pūtea Matua and its business objectives.
- articulate and resource a digital strategy to achieve the vision and enable the use of technology to maximise productivity, enhance the use of data in decision making, and facilitate collaboration between Te Pūtea Matua staff, external and industry stakeholders.
- prioritise the delivery of strategic initiatives based on business value and risk.
- avoid functional duplication in IT assets and promote the use of enterprise assets across the RBNZ.
- align IT assets with our strategic direction and architecture target states. Our enterprise architecture capability informs the development and continual renewal of our digital strategy and supports the investment profile planning required to deliver upon the strategy.

3. Enterprise architecture

Enterprise architecture provides a roadmap for investment in IT assets and governance to ensure consistency in delivery.

- We ensure IT assets and associated solutions comply with technology target state architectures and information security standards and principles.
- Enterprise architecture provides a governance point for the management of technology debt (IT assets that are unsupported, end of life, or no longer meeting business needs, and IT assets that do not align with architecture target states or our digital strategy). We uphold the enterprise architecture, so the level of technology diversity, complexity and technical debt is kept to manageable levels.
- We ensure that information technology investments support business objectives and strategic plans, and that the design and implementation of technology initiatives are consistent with our digital strategy.

4. Acceptable use

Correct use of our technology and applications is a key control in the operation and consumption of IT services.

- We ensure our information technology is used in a manner that keeps our information, property, and people safe.
- We ensure users know their responsibilities when connecting with and using our information technology.
- We comply with mandates and guidance set by the New Zealand Government on the use of technology.

5. Information and data security

Protection of our IT assets and data is a foundational component of IT operations.

- We ensure the confidentiality, integrity and availability of our information and data in accordance with the RBNZ Information and Data Management policy and the Information Security policy.
- We proactively identify, assess, report on, and remediate cyber vulnerabilities across endpoints, workloads, and systems.
- We comply with our internal Protective Security Requirements (including the New Zealand Information Security Manual (NZISM)) for information technology deployment, management, and operation.
- We protect the interests of all authorised users of our information systems as well as the interests of all third parties who supply data by preventing unauthorised access.
- We provide user access that is authorised, granular, auditable, and appropriate for the user.

6. Service management

Effective service management ensures technology change is well planned and managed, aligns with our digital strategy and is executed well, minimising service outages.

- We ensure service requests are recorded, evaluated, documented, and responded to in a controlled and timely manner, and actively seek ways to improve our service delivery.
- We maintain incident response capability to ensure all incidents are responded to appropriately. We test incident response systems annually and evolve our practices to meet the evolving needs of the Bank.

- We support business continuity by ensuring digital services can be resumed within required timeframes, with an agreed level of data loss after a disaster or significant outage event. We test disaster recovery capabilities of our critical applications and systems annually.
- We minimise risk to our production IT assets associated with change through the operation of a comprehensive change management process.
- We govern technology change across Te Pūtea Matua to ensure alignment with our digital strategy and architecture target states.

7. Operational management

We use industry best practice to ensure the services provided by our technology meets the performance, availability, resilience, and reliability requirements of Te Pūtea Matua.

- We design and implement disaster recovery capabilities appropriate to the criticality of IT assets. Disaster recovery capabilities for critical IT assets are tested annually to ensure that they are still effective and so our teams maintain operational readiness.
- Appropriate backup capabilities are implemented to meet recovery point objectives (RPO) and recovery time objectives (RTO) for our IT assets and associated data.
- We patch our IT assets, prioritising critical systems and vulnerabilities. We take a risk-based approach to patch prioritisation to ensure that our assets are protected from new vulnerabilities in a timely manner.
- We proactively monitor our IT assets to measure their availability and performance. Where IT assets cross pre-defined thresholds our monitoring capabilities generate alerts which support our teams to identify and resolve problems in a timely manner.
- We proactively monitor and manage IT asset capacity, allowing us to manage resource consumption within budgetary constraints, and to provide accurate forecasts for resource consumption and associated costs. We monitor IT asset usage, and proactively lower costs by hibernating and decommissioning workloads when they are not being used.
- We maintain an accurate IT asset register that allows us to map applications, infrastructure, and cloud services to business owners.
- We use a quarterly prioritisation and planning cycle to understand, prioritise and plan work to meet the demand for IT changes.

8. Commercial management

We make extensive use of commercial arrangements for the delivery of our technology services. We ensure these commercial arrangements deliver the desired outcomes for the RBNZ with the greatest value.

- We follow government mandates and best practice for commercial and contractual management of our IT assets and services.
- We proactively manage our strategic suppliers and contractual agreements through regular reporting, supplier meetings and benchmarking.

9. Lifecycle management

Effective IT asset management includes a lifecycle view of technology as technology components making up an IT solution are likely to change multiple times throughout the life of an IT asset.

- We proactively manage our IT assets, maximising use and value, mitigating risks, ensuring support and consumption costs are monitored and reasonable, and actively plan for end-of-life.
- We proactively manage end-of-life and end-of-support components in IT assets, remediating or replacing components before they become unsupportable or at risk of introducing vulnerabilities.
- We take a structured approach to safely decommission information technology.
- We ensure software, system logic and data are properly transitioned to new systems or archived in accordance with legal requirements.

10. Capacity and capability management

- We have the right mix of skills and experience, sufficient capacity for change, and the right operating models to be efficient.
- We maintain a plan that identifies the skills and experience required to support future technologies RBNZ is likely to use.
- We invest in our staff, providing good opportunities to learn through a mixture of on-the-job, coached, and external learning.
- We maintain a balance of workforce types to meet the demands of day-to-day operations and project-driven change. This mix includes permanent, contingent and partner capacity.

11. Accountabilities and responsibilities

Accountabilities and responsibilities for technology management are set out in this table.

Role	Responsibilities
Chief Technology Officer (CTO)	Sets the strategic direction and policy for technology, governance of technology risks and delivery of technology programmes.
Chief Information Security Officer (CISO)	Sets the information security strategy and policy, governance of cyber security risks and delivery of cyber security initiatives. The CISO is the delegated certification authority for all IT systems.
System owners	Responsible for the technological aspects for a system, including ensuring its availability and currency, maintaining vendor relationships, and providing assurance for backups and recovery.
Business owners	Responsible for the business strategy and user operation of the system within approved parameters. If a system is used by multiple groups within RBNZ, the CTO is the business owner.