



# **Reserve Bank of New Zealand Exchange Settlement Account System (ESAS)**

## **Disclosing Compliance with the FMI Standards**

Prepared by: Financial Market Infrastructures and Settlements (FMI&S) Directorate, Reserve Bank of New Zealand

March 2026

## Glossary

Account	Exchange Settlement Account
Accountholder	Exchange Settlement Accountholder and a Participant in the System
A-ORRF	Automated Overnight Reverse Repo Facility
BCP	Business Continuity Plan
BLF	Bond Lending Facility
Board	The members of RBNZ's board as defined in the Reserve Bank Act
BPS Act	Banking (Prudential Supervision) Act 1989
CCP	Central Counterparty
CLS	Continuous Linked Settlement
CSD	Central Securities Depository
CPMI	Committee on Payments and Market Infrastructures
CSP	Customer Security Programme
CVSS	Common Vulnerability Scoring System
Datacom	Datacom Systems Limited
DVP	Delivery versus Payment
ESAS	Exchange Settlement Account System
FMA	Financial Markets Authority
FMD	Financial Markets Directorate
FMI	Financial Market Infrastructure
FMI Act	Financial Markets Infrastructure Act 2021
FMI&S	Financial Market Infrastructures and Settlements
FMI Standards	Standards for designated FMIs

UNCLASSIFIED

Governor	RBNZ Governor
GCSB	Government Communications Security Bureau
GMRA	Global Master Repurchase Agreement
HVCS	High Value Clearing System
IOSCO	International Organisation of Securities Commissions
ISO	International Organisation for Standardization
ISDA	International Swaps and Derivatives Association
LFF	Lessons for the Future
NEXI	Nexi S.p.A
NZCDC	New Zealand Clearing and Depository Corporation Limited
NZCSD	New Zealand Central Securities Depository Limited
NZX	NZX Limited (New Zealand's Stock Exchange)
ORRF	Overnight Reverse Repo Facility
PFMI	Principles for Financial Market Infrastructures
PNZ	Payments New Zealand Limited
PSOC	Payments and Settlements Oversight Committee
RBNZ	Reserve Bank of New Zealand
RECS	RTGS Extreme Contingency Solution
Regulator	RBNZ Specialist Supervision
Reserve Bank Act	Reserve Bank of New Zealand Act 2021
RMF	Risk Management Framework
RTGS	Real-Time Gross Settlement

SOC	Security Operations Centre
System	Exchange Settlement Account System
System Operator	RBNZ as the System Operator of ESAS
SWIFT	Society for Worldwide Interbank Financial Telecommunication

## Contents

<b>Glossary</b>	<b>1</b>
<b>Introduction</b>	<b>5</b>
<b>1. Executive summary</b>	<b>5</b>
<b>2. Summary of major changes since last update</b>	<b>15</b>
<b>3. General background</b>	<b>16</b>
General organisation of the FMI	20
Legal and Regulatory Framework	20
System design and operations	20
<b>4. Standard by standard narrative disclosures</b>	<b>23</b>
Standard 1: Legal Basis	23
Standard 2: Governance	30
Standard 3: Framework for the Comprehensive Management of Risks	36
Standard 4: Credit Risk	40
Standard 5: Collateral	43
Standard 6: Margin	45
Standard 7: Liquidity Risk	46
Standard 8: Settlement Finality	51
FMI Standard 9: Money Settlements	52
FMI Standard 10: Physical Deliveries	54
FMI Standard 11: Central Securities Depositories	55
FMI Standard 12: Exchange-of-Value Settlement Systems	56
FMI Standard 13: Participant-Default Rules and Procedures	57
FMI Standard 14: Segregation and Portability	60
FMI Standard 15: General Business Risk	61
FMI Standard 16: Custody and Investment Risk	63
FMI Standard 17: Operational Risk	65
FMI Standard 17A: Contingency Plans	72
FMI Standard 17B: Critical Service Providers	78
FMI Standard 17C: Cyber Security Risk	82
FMI Standard 18: Access and Participation Requirements	90
FMI Standard 19: Tiered Participation Arrangements	95
FMI Standard 20: FMI Links	98
FMI Standard 21: Efficiency and Effectiveness	101
FMI Standard 22: Communication Procedures and Standards	103
<b>5. List of publicly available resources</b>	<b>104</b>

## Introduction

This document constitutes the first formal disclosure of the Exchange Settlement Account System (ESAS) in accordance with FMI Standard 23A: Disclosing Compliance with the FMI Standards, issued under the Financial Market Infrastructures Act 2021 (FMI Act).

The disclosure has been prepared by the FMI&S Directorate of the Reserve Bank of New Zealand (RBNZ), which is the operator of ESAS. As the designated FMI Operator, the RBNZ is responsible for ensuring ESAS complies with the applicable FMI Act Standards set by the regulator.

This disclosure follows the structure and content requirements set out in Annex A of FMI Standard 23A and is informed by the Financial Market Infrastructures Standards: Guidance (March 2024) issued by the regulator.

ESAS is designated and regulated under the FMI Act. Regulation, oversight, and supervision of ESAS is conducted by the RBNZ's FMI Supervision team, which operates independently of FMI&S. This disclosure represents ESAS Operator's current assessment of how ESAS complies with the relevant FMI Standards as of March 2026.

## 1. Executive summary

The Exchange Settlement Account System (ESAS) is New Zealand's principal high-value payments system and is charged with providing an efficient and safe process for the real time electronic settlement of payments between account holders. The ESAS system is owned and operated by the Reserve Bank of New Zealand - Te Pūtea Matua (RBNZ) on a cost-recovery basis and is not included in the RBNZ Five-Year Funding Agreement.

The Reserve Bank has provided ESAS as a real-time gross settlement system (RTGS) since 1998. Account holders electronically submit instructions to debit an account and credit another account using an authorised electronic submitting mechanism. Authorised submitting mechanisms include closed user groups which use the SWIFT electronic messaging system, the NZClear system and direct entry of transaction details into ESAS. The system is available for use by account holders for 23.5 hours each calendar day. Each ESAS day begins at 9:00am on a calendar day and ends at 8:30am the following calendar day.

A payment will be settled (i.e., funds are transferred from one ESAS account holder's exchange settlement account to another ESAS account holder's exchange settlement account) once a transaction instruction is authenticated, the payment instruction is authorised by the payer and the payer has sufficient funds in their exchange settlement account to effect the transaction. Once a transaction is settled it cannot be revoked.

ESAS is a systemically important payment system under the Financial Market Infrastructures Act 2021 (FMI Act). The ESAS regulator is the Specialist Supervision Directorate, part of the Reserve Bank's Financial Stability Group. Institutional arrangements ensure that dealings between the ESAS Operator and Specialist Supervision Directorate occur on an arm's length basis.

In accordance with the provisions of the Reserve Bank Act, the RBNZ Board is its governing body and is responsible for all decisions relating to the operation of the RBNZ. The Board is therefore ultimately responsible for the operation of ESAS. For practical purposes, the Board delegates the

day-to-day management authority of the Reserve Bank to the RBNZ Governor. This includes the authority to establish roles within Reserve Bank and organise the Reserve Bank to ensure it is fit for purpose.

The Governor delegates responsibility for administering the operational aspects of the System to the Reserve Bank's FMI&S Directorate, Day-to-day business support is provided by the directorate's Payment and Clearing Services Team and the Application Support and Technical Operations Team.

The FMI&S Directorate reports on the operation of ESAS to, the Reserve Bank's Assistant Governor/General Manager, Economics, Financial Markets and Banking.

Datacom supports the telecommunications network infrastructure, and related security features utilized by the system. Application support services and application development are provided by the Nexi Group. The Reserve Bank manages Datacom's and Nexi's provision of services through service contracts and related service level agreements. The management process includes assessment of performance at regular review meetings, regular performance reports, review of problem management reports, a relationship governance committee and relevant project steering committees.

The aggregate level of liquidity in the ESAS system is managed by the Reserve Bank's Financial Markets Directorate (FMD). FMD injects or withdraws liquidity from the system by undertaking transactions such as reverse repurchase agreements, foreign currency swap transactions, and issuance of Reserve Bank Bills. FMD's objective is to ensure that there is adequate aggregate liquidity in the system to ensure the efficient operation of payments, while also maintaining short-term wholesale interest rates at levels close to the Official Cash Rate.

On 6 November 2023, RBNZ as the regulator issued the Financial Markets Infrastructures Act Designation Notice (ESAS) 2023 (the ESAS Designation Notice) pursuant to section 20 of the FMI Act, under which ESAS is declared to be a designated FMI under the FMI Act, with effect from 1 March 2024.

The ESAS Rules, which form a binding contract between the RBNZ and each participant, along with the System's designation as a designated FMI (effective 1 March 2024), the Settlement Submission Mechanism, and the broader legal framework (including key statutes such as the Contracts and Commercial Law Act 2017 and the FMI Act 2021) provide strong legal certainty.

The FMI Act and associated FMI Standards (effective from 1 March 2024, with Standard 23A effective from 1 March 2025) enhance regulatory oversight, codify international best practices (PFMIs), and impose robust requirements on designated FMIs in areas such as operational risk, third-party risk, contingency planning, and disclosure.

## ESAS Accountholders

Historically, access to ESAS was deliberately limited. Account holders consisted primarily of registered banks, selected government entities, and a small number of financial market infrastructures. This conservative access model reflected a strong focus on prudential oversight, systemic risk management, and operational resilience, given the system's critical role in financial stability.

In response to structural changes in the payments ecosystem, including increased innovation, competition, and the growing role of non-bank institutions, the Reserve Bank undertook a comprehensive ESAS Access Review (EAR) between 2022 and early 2025. The review assessed whether access to ESAS could be broadened in a way that supports efficiency and competition while maintaining the safety, integrity, and resilience of the system. The EAR involved two rounds of public consultation and detailed consideration of legal, operational, and risk management implications. As ESAS is designated under the Financial Market Infrastructures Act 2021, changes to access policy required approval by the Reserve Bank Board, which was granted in March 2025.

Following the review, the access framework shifted from an institution-type based approach to a principles and risk-based model. Under the revised policy, eligibility for ESAS access is assessed through a two-step approach. First, an applicant must be engaged in business activities that align with the purpose of ESAS, namely contributing to the efficient and final settlement of payments in central bank money. Second, the applicant must demonstrate an acceptable risk profile, including appropriate governance arrangements, financial and operational resilience, compliance with anti-money-laundering and counter-financing of terrorism obligations, and the ability to meet ESAS operational and technical requirements. Applicants are responsible for providing evidence that all criteria are met and for any costs associated with preparing supporting documentation.

Access to ESAS is now open on an ongoing basis to all entities that meet the access criteria. Eligible applicants may include registered banks, licensed non-bank deposit takers, payment service providers, overseas deposit takers, market makers, and operators of designated financial market infrastructures. The revised policy removes restrictions based on historical membership categories, while ensuring that all applicants (new and existing) are subject to the same rules, risk assessments, and operational requirements.

The opening of access has been implemented in a phased manner, beginning with licensed non-bank deposit takers and subsequently extending to a broader range of institutions. Existing ESAS account holders continue under the same framework, while new entrants are assessed against the same standards to ensure a level playing field and the continued robustness of the system. ESAS operates on a cost-recovery basis, with operating costs shared across account holders through subscription and transaction fees.

## ESAS Risk Management Framework

RBNZ's Enterprise Risk Management framework (ERMF) is used across the organisation, including in support of ESAS. ERMF is defined in our Risk Management Policy (approved by the Board in 2023), as the totality of systems, structures, policies, processes and people that identify, measure, evaluate, monitor, report and control or mitigate all internal and external sources of material risk impacting across the RBNZ.

RBNZ's Risk Management Framework is designed to:

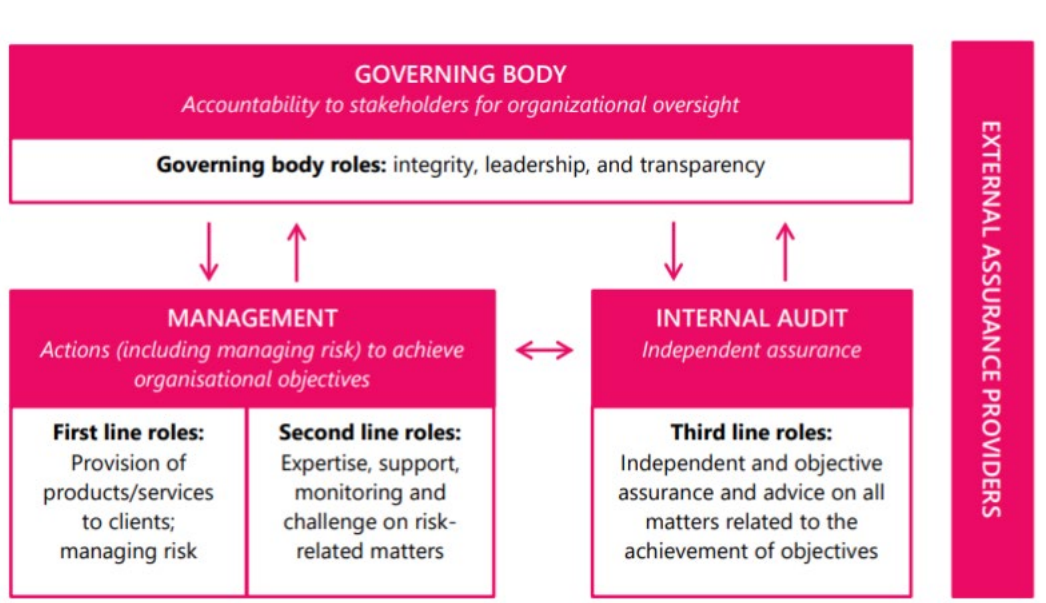
- Establish a consistent and systematic approach to identifying, assessing and managing risks within Te Pūtea Matua.
- Establish a clear and transparent process for identifying and managing risks, which improves stakeholder confidence and trust in us.
- Ensure that risks are identified and dealt within a timely and effective manner, and that potential negative impacts are minimised or avoided.
- Co-ordinate our efforts to manage risk in accordance with our Risk Appetite Statement.

- Maintain a total portfolio of risk that is appropriate for our stakeholders and employees.
- Enable risk to be taken on an informed and controlled basis within pre-determined limits.
- Protect Te Pūtea Matua from potential losses and to ensure it is able to achieve its goals and objectives.

Our Risk Management Policy is the primary policy for prescribing RBNZ’s organisation-wide principles and expectations for managing risk. The Risk Management Handbook (approved by Chief Risk Officer in 2024) describes in detail the material elements of our risk management framework. It includes a specific section relating to Financial Markets Infrastructure (FMIs), including ESAS.

### Three Lines Model

RBNZ employs a Three Lines Model to provide Enterprise Risk Management and achieve its Financial Market Infrastructures’ (FMI) objectives. This allocates accountabilities for managing risk across the First, Second and Third Lines of management (see diagram below).



Provided below is further detail of how the Three Lines model is applied at RBNZ, and the management functions delivered by the Risk, Compliance and Audit Directorate in support of ESAS.

A list of related policies and procedures captured in Appendix 3.

### First Line Risk Management

The Director of Financial Markets Infrastructures & Settlements (FMI&S) is responsible for leading their team to embed risk management practices into the daily activities of their directorate.

The AG Money Group is accountable for the overall operation and risk management of ESAS and for complying with the new FMI Act and FMI Standards. They oversee the First Line risk management responsibilities executed by the Director of FMI&S for risk identification, assessment, treatment, recording, reporting and monitoring.

The FMI&S Directorate has its own First Line risk management group known as the FMI Risk Forum (formerly Payments Risk Forum). This group meets on a quarterly basis to discuss domestic and global risk trends, and to coordinate FMI risk management activities. FMI risks are captured in risk registers specific to ESAS and NZClear, with each risk register updated quarterly and discussed at the FMI Risk Forum. Additionally, the FMI&S Directorate has a dedicated First Line group specifically for Business Continuity Management (BCM), known as the FMI Business Continuity Forum (formerly known as Payments Business Continuity Forum).

ESAS operates under a comprehensive and well-documented ESAS risk management framework that reflects the Reserve Bank of New Zealand's enterprise-wide approach to risk governance. The framework is explicitly aligned with the Financial Market Infrastructures Act 2021, the associated FMI Standards, international standards such as ISO 31000 and the CPMI-IOSCO Principles for FMIs, and the Reserve Bank's Risk Management Policy and Risk Appetite Statement (RAS). Together, these ensure that ESAS is operated safely, efficiently, and within clearly defined risk tolerances approved by the Board.

The ESAS Risk Management Framework articulates the objectives, structures, and processes that govern risk identification, assessment, mitigation, monitoring, and reporting. It is part of a hierarchy of interrelated risk management measures that include the Board-approved RAS, the Bank-wide Risk Management Policy, Enterprise Risk Management (ERM) guidelines, the ESAS Risk Assessment Framework, the ESAS Risk Register, and the system-specific rules and procedures governing settlement operations.

The Board has ultimate responsibility for risk oversight, as set out in the Board Charter, including approving the RAS, endorsing the Bank's enterprise-wide risk management approach, reviewing risk reporting, and ensuring the integrity of internal controls. The Board reviews and reapproves the RAS annually, ensuring that ESAS's risk tolerances remain appropriate in light of emerging risks, changes in technology, and industry developments.

Risk identification, assessment, and monitoring occur continuously through FMI&S's operational processes, quarterly FMI&S Risk Forums, the Risk Compliance and Audit Directorate's enterprise-level oversight, and regular reporting to PSOC and the Board. The ESAS risk management process is systematic and includes bottom-up identification, structured assessment against the RBNZ's risk appetite, evaluation of residual risks, and design and implementation of risk treatments. The ESAS Risk Register is updated quarterly, reviewed through Risk forum, and forms a key component of FMI&S's quarterly reporting to the PSOC and Board.

Key risk domains for ESAS include operational risk, cyber risk, critical service provider risk, regulatory compliance risk, credit and liquidity risk (which are limited due to real-time settlement and no overdrafts), legal risk, and participant-related risks such as AML/CFT, operational capability, and financial soundness. These risks and their mitigations are documented extensively in the ESAS Risk Management Framework and supporting procedures and artefacts.

ESAS's operational and technical risk controls, including segregation of duties, access controls, real-time monitoring, resilience design, data replication across dual sites, and business continuity arrangements, are reinforced through FMI&S's operational policies and the wider Bank's information security standards. Cyber resilience is governed by RBNZ's Information Security

Management Framework, which aligns with NZISM, ISO 27001, NIST Cybersecurity Framework, and SWIFT CSP requirements, ensuring adherence to FMI Standard 17C.

Third-party and critical service provider risks are governed by the FMI&S CSP Risk Framework, which complements the Bank's Third-Party Risk Management Framework. This includes defined SLAs, regular service reviews, risk assessments, BCP/DR requirements, control assurance (internal and external), and structured reporting and escalation mechanisms through FMI&S governance, , and the Board.

FMI&S are responsible for ESAS business continuity planning. Decision-making responsibilities captured under their BCP include:

RBNZ Director FMI&S (with AG Money as a back-up) is authorised to activate the BC response, responsible for coordination of the decision making including the decision to invoke DRP(s) outside the CLS Settlement window. During the CLS Settlement window, decisions to invoke CLS contingency arrangements will be made in conjunction with CLS.

The BCP captures triggers for BCP activation, including those scenarios where ESAS remains operable, but the directorate operations are disrupted e.g. following unexpected closure of an RBNZ building. It also captures processes for activating their BCP/DRP, with indicative timings included to guide decision making for invoking DR.

Activation of the ESAS BCP may also be cause for RBNZ to activate its Incident Response Team (IRT) to help manage the impacts to RBNZs business continuity of an ESAS outage or coordinate the response to a disruption impacting multiple directorates e.g. RBNZ building closure.

During a crisis or emergency updates to the Board would be provided via the Governor. This is aligned with the Governor's Position description which states "The Governor is responsible for ensuring that relevant and sufficient information flows to the board and to support the board and its individual members in fulfilling their collective and individual duties outlined in Part 2, Subpart 4 of the Act."

Decision-making in crises is guided by the ESAS Business Continuity arrangements, which define roles and responsibilities, communication flows, and escalation thresholds. These procedures ensure that incident response is coordinated, that settlement can continue through alternative configurations if necessary, and that all governance bodies and regulators receive timely updates. The Board is kept informed via incident briefings, periodic reporting, and updates through the ELT and PSOC as appropriate.

Crisis and incident management are supported by ESAS's Incident Management Guidelines, the Bank-wide Lessons for the Future (LFF) process, and mandatory regulator reporting for material events. The LFF policy ensures that all significant incidents are analysed, root causes identified, and improvements implemented. For material incidents, management escalates matters through FMI&S leadership, ELT, PSOC, and the Board, ensuring timely governance oversight and regulatory transparency.

ESAS's rules and procedures—including default rules, settlement finality provisions, liquidity management tools, and the prohibition of overdrafts—form part of the system's legal and operational risk mitigation. Legal certainty is ensured through the ESAS Rules and legal

assessments confirming enforceability under New Zealand law. The participant risk assessment framework (RAF) provides an internal methodology to assess new applicants and ongoing participant risks aligned with FMI Standard 18.

The ESAS Rules form the legally binding foundation of the system. They define the requirements for participation, the obligations on account holders, the Reserve Bank's responsibilities as System Operator, and the processes for managing contingencies, suspensions, and participant default. The Rules include mandatory notification obligations (clause 6), requiring all participants to immediately notify the Reserve Bank of any "Notifiable Event" such as insolvency, administration, loss of ability to meet financial obligations, appointment of receivers or statutory managers, or the commencement of liquidation or restructuring processes. The Rules also explicitly empower the Reserve Bank, acting reasonably, to suspend or terminate a participant's ESAS account at any time when necessary to protect the integrity or security of the system (clause 8.4). This authority ensures that the Reserve Bank can act decisively to isolate emerging risks, prevent the entry of invalid or unsafe transactions, and protect the wider financial system from contagion.

The Reserve Bank has supplemented the ESAS Rules with a detailed Participant Default Management Procedure, which operationalises all default-related provisions of the Rules. A participant default may be triggered by any Notifiable Event identified in the ESAS Rules, including inability to pay debts, appointment of insolvency administrators, statutory management, or regulatory suspension of licences. Default may also arise where a participant no longer satisfies the ESAS Access Criteria or where Payments NZ requests a suspension under the SBI framework. Once a default trigger event occurs, the Reserve Bank immediately suspends the participant's ability to submit or receive payments, blocks queued transactions, and initiates communication to all ESAS participants, regulators, the Reserve Bank's senior leadership, and Payments NZ (where relevant). Default actions include Suspension, Stop Pay, Stop Receive, Exclusion from ESAS, and removal from SBI participation. Close-out processes follow the ESAS Rules and involve cancellation of all queued transactions, communication of impacts to affected participants, and system reconciliation to ensure consistent records. These processes ensure that a defaulting participant cannot introduce risk to the system and that non-defaulting participants remain fully protected.

## Second Line Risk Management

The Risk, Compliance & Audit Directorate provides expertise, support, monitoring and challenge in support of ESAS, including:

### Risk Business partnering:

- Regular engagement with the FMI&S Directorate to provide support, challenge and review of First Line risk assessments, treatment, recording, monitoring and review.
- Facilitation of quarterly risk reviews with the FMI&S Directorate. These reviews include meeting with management, updating operational risk registers, and discussing material risks to the achievement of strategic objectives.
- Attendance/membership of First Line risk management groups to help business units identify, assess and manage risks effectively. This role also helps ensure risk considerations are integrated into business planning and execution.
- Providing advice on project risks within RBNZ, including those pertaining to FMI&S.

**Risk reporting:** Provides a view of the effectiveness of risk management across RBNZ, including the risk profile and the effectiveness of controls. Risk reporting also supports decision making and assists with meeting regulatory obligations. Risk reporting is provided the Board every six months.

**Lessons for the future (LFFs):** The Risk Team reviews and manages the LFFs process. LFFs are used in the reporting of incidents/near misses, documenting lessons learned, to support continuous improvement of governance, risk management and controls. The LFF information is used for risk and incident reporting to, Executive Leadership Team (ELT) or Board.

**Compliance oversight:** Oversight of RBNZs compliance with the following polices:

- AML/CFT (Director Risk, Compliance & Audit (RC&A) is the AML/CFT Compliance Officer,
- Fraud and Corruption Prevention (staffed by Risk and Compliance Team);
- Conflicts of Interest (Director RC&A appointed the Conflicts Officer);
- Gifts and Hospitality;
- Privacy (Director of RC&A is the appointed the Privacy Officer. The – temporarily covered by Director Legal and Governance/General Chief Legal Counsel is temporarily covering this role until the permanent Director RC&A starts in January 2025role is filled permanently);
- Personal Information held by RBNZ (Privacy);
- Conduct; and
- Protected Disclosures (Whistleblowing).

**Compliance advisory services:** Provides advisory services, both general and project specific. This includes:

- Targeted deep dives into areas they or Internal Audit identify. No deep dives have been conducted into specific ESAS FMI Act related matters, but one area they have been focussed on recently is sanction legislation and this included consideration of ESAS.
- Provide subject matter expertise input to First Line Compliance as necessary. This has occurred when the team drafted some specific questions in relation to financial crime (AML/CFT, sanctions and fraud) for the ESAS payment service provider application form.

**Attestations:** Coordinating and reporting of RBNZ attestations. Attestations results are reported to ELT and Board 6-monthly or annually, aligned with the frequency of information collection:

**Business continuity oversight and reporting:** The Principal Adviser Resilience member of the Resilience Team attends quarterly meetings of the FMI Business Continuity Forum. FMI&S Directorate's compliance with RBNZs Business Continuity Management (BCM) Policy is also monitored via a set of performance measures. 6-monthly reporting is provided to , AGGM Enterprise Services, ELT and Board summarising BCM policy non-compliances, including those relating to FMI such as ESAS.

**Other initiatives:** In addition to the above core activities, the directorate actively supports a range of complementary initiatives that strengthen and reinforce the Bank's overall risk management framework. These include developing and maintaining policies, risk management tools and guidance, facilitating cross-departmental collaboration on emerging risks, and providing targeted training and awareness programmes.

### Third Line Risk Management

Audit Services, provides independent assurance and advice, reporting directly to the RBNZ Board via the Audit Committee. The Senior Manager Audit Services leads the directorate team, reporting functionally to the Audit Committee Chairperson, administratively to the Director of Risk, Compliance and Audit "Chief Risk Officer", and has direct access to the Governor.

The Senior Manager Audit Services has access to the Audit Committee Chair at any time.

The Audit Services' purpose, authority, and responsibilities are defined by a board-approved Audit Services Charter which grants unrestricted access to records, facilities and personnel to carry out its internal audit activities.

Audit Services consists of five staff members, including a Senior Manager role which has recently been recruited for (start date 10 Nov 2025). The team includes a Senior Advisor dedicated to FMIs assurance, two Audit Advisors who support broader RBNZ functions and an IT Audit Advisor specialising in organisational technology. The function operates a co-sourcing model, bringing in external experts as needed for additional capacity and specialist knowledge.

Audit Services operates under an annual internal audit plan approved by the RBNZ Board, which also incorporates a three-year rolling outlook to address medium- to long-term priorities. The plan is executed through a mix of assurance, advisory, and compliance audits, alongside other related services. Additionally, Audit Services undertakes investigations as needed.

The audit approach and coverage for the FMIs have evolved with the introduction of new FMI Act 2021 and the FMI Standards which came into effect on 1 March 2024. Under this new regulatory regime, both ESAS and NZClear are designated FMIs subject to stringent oversight and assurance requirements across the Three Lines model. As such, Audit Services initiated efforts to enhance its activities, acknowledging the essential and systemic importance of the FMIs. This transformation aims to ensure that the audit approach and coverage are aligned with regulatory requirements.

In November 2024, Audit Services introduced the Senior Advisor role to strengthen assurance activities for FMIs. A comprehensive review followed, resulting in development of separate audit universes and tailored risk assessments for each FMI.

The risk assessment was aligned with the Risk Team's methodology and incorporated their data ensuring consistency and collaboration across functions. This work informed the creation of distinct FY2025/2026 audit plans for both ESAS and NZClear, with each FMI considered independently.

In addition to this, several audits relevant to both ESAS and NZClear were identified within the broader RBNZ annual audit plan, reflecting the inherent interdependencies between the designated FMI operator and other functions within RBNZ.

A high-level assurance mapping exercise was also conducted to identify coverage from various assurance providers, including external auditors, as well as Risk, Compliance, Information Security, Physical and Personnel Security, and Quality and Assurance functions.

Key external assurance activities include:

- ESAS 3402 and NZClear 3402 audits – cover a broad range of FMI controls.

- NZClear 3150 audits – focussed specifically on reconciliation controls.

Going forward, this new approach of treating ESAS and NZClear as separate and distinct entities, will become the standard practice.

## 2. Summary of major changes since last update

- This is the Reserve Bank of New Zealand's (RBNZ) first formal assessment of the Exchange Settlement Account System (ESAS)'s observance of the Standards for Financial Market Infrastructures (FMIs). The previous public disclosures relating to ESAS were made under the PFMI self-attestation framework, with the most recent PFMI-based publication issued in February 2025. Accordingly, the major changes since the last update primarily reflect the transition from the PFMI disclosure regime to the Financial Market Infrastructures Act 2021 (FMI Act) and the associated FMI Standards.
- The most significant change is the full implementation of the FMI Act and all supporting FMI Standards, including Standard 23A (Disclosure), which took effect from 1 March 2025. This marks a shift from voluntary PFMI self-attestation to a statutory disclosure and observance framework.
- ESAS was formally designated under the FMI Act through the ESAS Designation Notice issued on 6 November 2023, with effect from 1 March 2024. This designation replaced the previous legal and oversight framework under the Reserve Bank of New Zealand Act 1989 and brought ESAS fully within the scope of the FMI regulatory regime.
- In addition to the legislative transition, a few key updates across individual FMI Standards have occurred since the last PFMI self-attestation. These include updates to existing standards and the introduction of several new standards under the FMI framework, as summarised below:

Section	Change
Standard 1: Legal Basis	Update on legal opinions
Standard 2: Governance	Update on PSOC
Standard 3: Framework for the Comprehensive Management of Risks	Update on the Risk Management Framework
Standard 17: Operational Risk	Audit updates
Standard 17A: Contingency Plans	New Standard
Standard 17B: Critical Service Providers	New Standard
Standard 17C: Cyber resilience	New Standard
Standard 18: Access and Participation Requirements	Update on ESAS Access Review
Standard 21 FMI Links	New Standard

### 3. General background

#### General description of the FMI and the markets it serves

ESAS serves as New Zealand's principal high-value payment and settlement system and forms a core component of the country's financial market infrastructure. It underpins the settlement of time-critical and high-value payment obligations across wholesale financial markets and provides the primary mechanism for the transfer of central bank money between financial institutions. By enabling settlement in central bank money on a real-time gross basis, ESAS plays a critical role in reducing settlement asset risk and supporting confidence in the safety and stability of the New Zealand financial system.

Through its operation as a real-time gross settlement (RTGS) system, ESAS supports a wide range of financial market activity, including interbank liquidity management, wholesale payment flows, settlement of obligations arising from clearing and securities settlement arrangements, and the Reserve Bank of New Zealand's own monetary policy and government banking operations. ESAS operates as the foundational settlement layer beneath multiple payment and market arrangements, including linked financial market infrastructures such as NZClear, and is therefore integral to the smooth functioning of the broader payments and financial markets ecosystem.

The RBNZ has provided ESAS as a RTGS system since 1998. Accountholders electronically submit instructions to debit an account and credit another account using an authorised electronic submitting mechanism. Authorised submitting mechanisms include closed user groups which utilise the SWIFT electronic messaging system, the NZClear system, and direct entry of transaction details to ESAS. The System is available for use by Accountholders for 23.5 hours each calendar day. Each calendar day commences at 9.00am on a working day and ends at 8.30am the following working day.

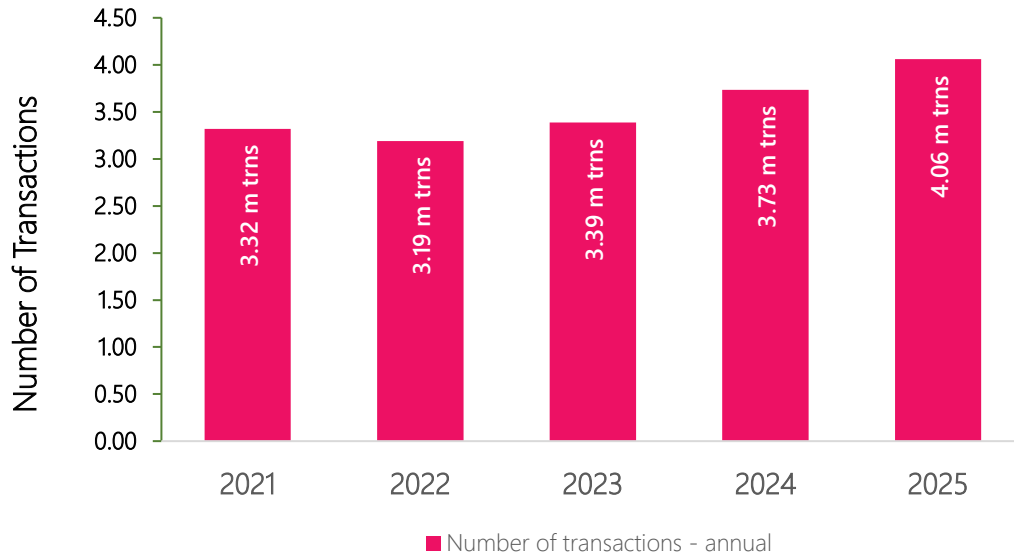
A payment will be settled (i.e. funds are transferred from one ESAS Accountholder's exchange settlement account to another ESAS Accountholder's exchange settlement account) once a transaction instruction is authenticated, the payment instruction is authorised by the payor, and the payor has sufficient funds in their exchange settlement account to affect the transaction. Once a transaction is settled it cannot be revoked.

Generally, each transaction is settled individually rather than in batches. The ESAS System allows for two or more payment instructions to be settled simultaneously, and where that occurs the ESAS Rules stipulate that each such payment instruction is settled gross and there is no netting of payment instructions. RBNZ has issued a notice to Accountholders pursuant to the ESAS Rules, which stipulates the order and method by which payment instructions are tested to determine whether the relevant Accountholder(s) has sufficient funds available to settle one or more payment instructions. The RBNZ Financial Markets Department determines the minimum balance that each Accountholder must maintain in their exchange settlement account and the interest rate(s), if any, paid on end-of-day balances.

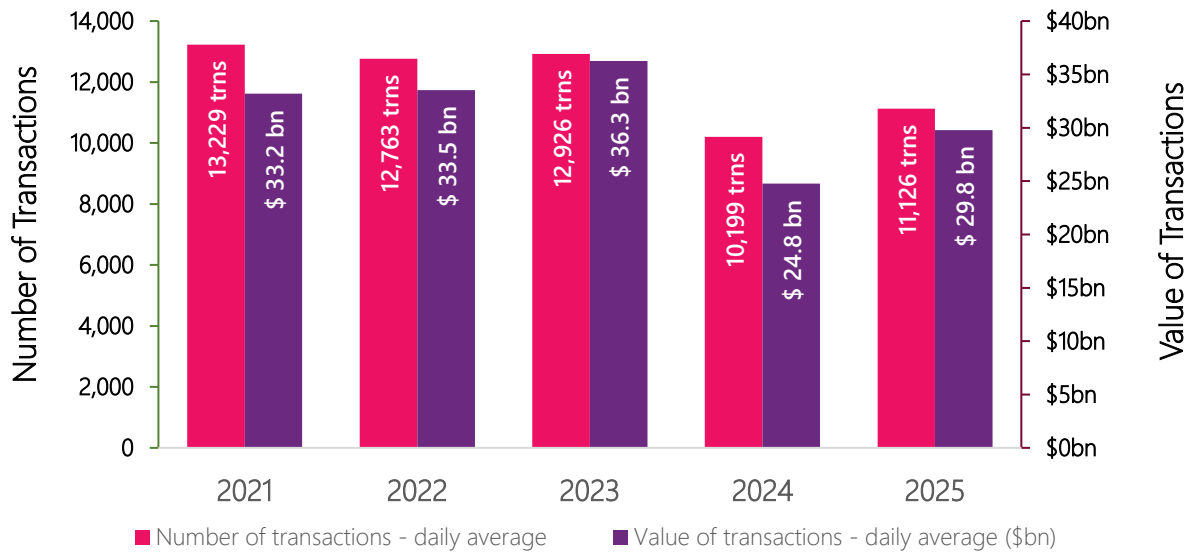
Historically, access to ESAS was largely limited to registered banks and a small number of other financial institutions. The ESAS Operator undertook a structured review of ESAS access arrangements to ensure they remain risk-based, transparent, and proportionate. As a result, ESAS access is now open, subject to meeting defined legal, operational, and risk management requirements, to a broader range of institutions, including licensed non-bank deposit takers and other non-bank payment service providers where risks can be appropriately managed. These

access arrangements are designed to support competition and innovation while maintaining ESAS’s low tolerance for risks that could undermine settlement finality, operational resilience, or financial stability.

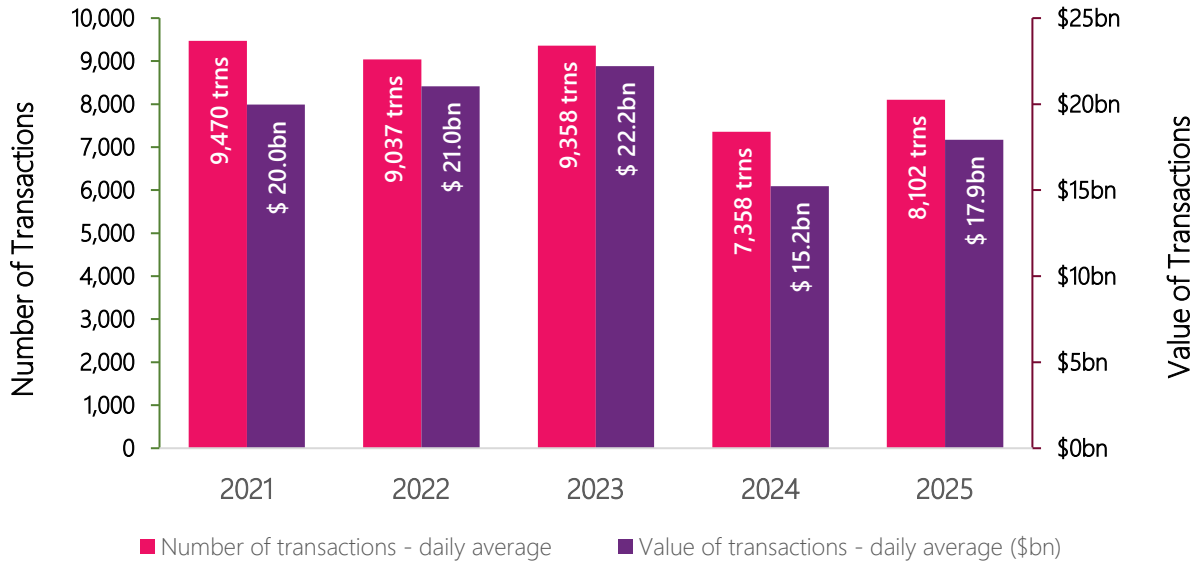
### Transaction volume per year – All



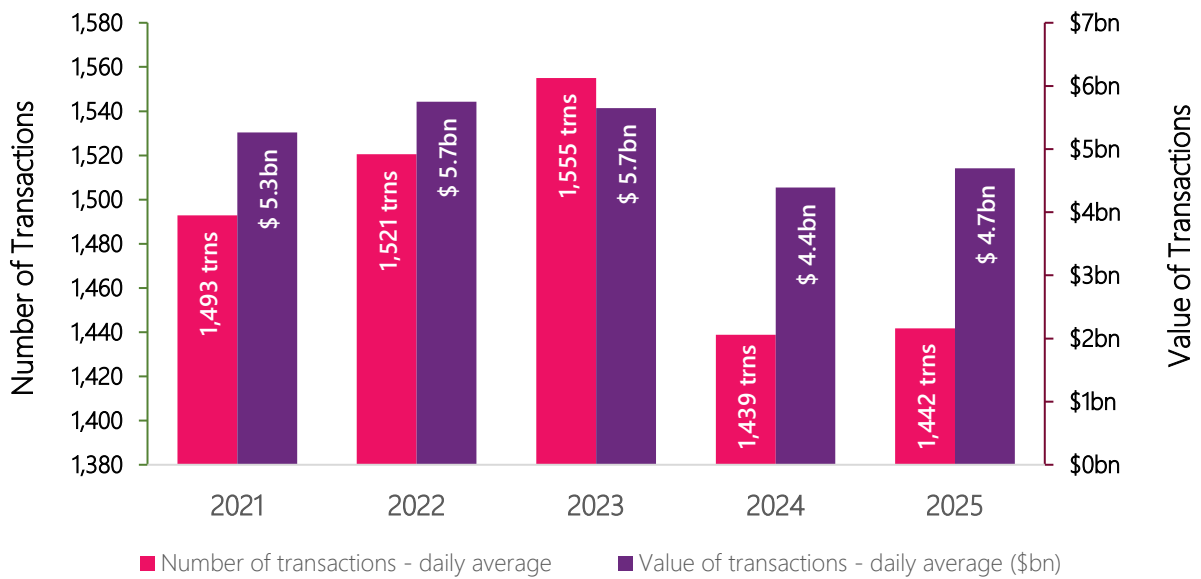
### Transactions per day – All



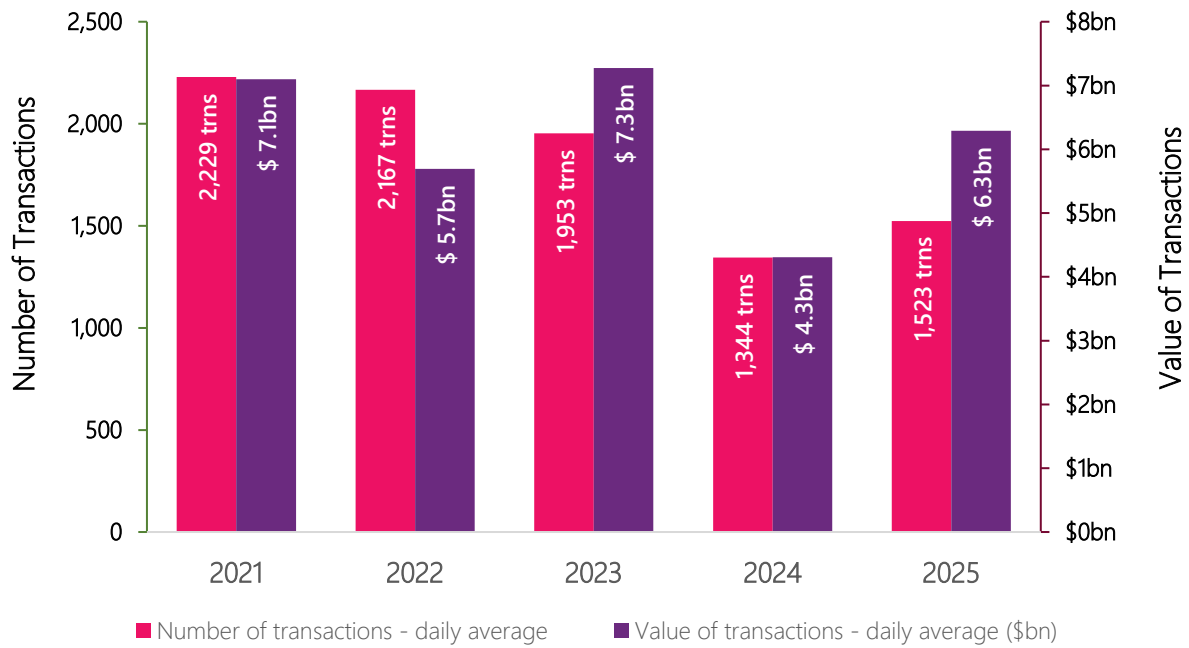
### Transactions per day – Sourced from Swift AVP



### Transactions per day – Sourced from SBI



## Transactions per day – Sourced from NZClear



## System outages year ended 30 June (hours:mins)

	2021	2022	2023	2024	2025
Outages	3:00	0:00	0:00	0:58	0:00

## Customer satisfaction

	2021	2022	2023	2024	2025
Exceed expectations	78%	92%	81%	88%	94%
Meet expectations	14%	8%	19%	12%	3%
Does not meet expectations	8%	0%	0%	0%	3%
<b>Total</b>	<b>100%</b>	<b>100%</b>	<b>100%</b>	<b>100%</b>	<b>100%</b>

## General organisation of the FMI

The Exchange Settlement Account System (ESAS) is owned and operated by the Reserve Bank of New Zealand (RBNZ) under its statutory mandate to act as New Zealand's central bank and to operate payment and settlement systems. ESAS is governed within the RBNZ's broader organisational and governance framework, which is established by the Reserve Bank Act and supported by documented governance, risk management, and accountability arrangements.

Ultimate responsibility for ESAS rests with the RBNZ Board, which provides strategic oversight and ensures that the operation of the FMI promotes safety, efficiency, financial stability, and public interest outcomes. The Board has established a dedicated governance committee, Payments and Settlements Oversight Committee, to strengthen focused oversight of ESAS and other designated FMIs.

Executive accountability for ESAS is delegated by the Governor to senior management, with day-to-day operation managed by the FMI&S Directorate within the RBNZ. Clear lines of responsibility and accountability exist between the Board, executive management, and operational teams, and are supported by documented policies, position descriptions, and performance frameworks.

Risk management and internal control functions operate with appropriate independence under a three-lines-of-defence model, ensuring effective oversight, escalation, and assurance. Governance arrangements are supported by regular engagement with participants, public disclosure through annual reporting, and ongoing consultation on material system changes.

ESAS operates within a clear, transparent, and well-defined organisational and governance structure that supports the safe and efficient operation of the FMI and the stability of the wider financial system.

## Legal and Regulatory Framework

ESAS is owned and operated by the Reserve Bank of New Zealand (RBNZ) under a comprehensive legal and regulatory framework established by the Reserve Bank Act and the Financial Market Infrastructures Act 2021. ESAS has been designated as a financial market infrastructure under the FMI Act, effective 1 March 2024, which provides statutory certainty for settlement finality, netting, and insolvency protection.

The system operates under legally binding ESAS Rules governed by New Zealand law, which establish the legal basis for all material aspects of ESAS's activities, including the submission, settlement, finality, and irrevocability of payments in central-bank money. These arrangements are supported by independent legal opinions that are regularly reviewed. ESAS is subject to ongoing regulatory oversight and compliance with FMI Standards for Financial Market Infrastructures, ensuring legal certainty, transparency, and robust supervision of the system's operation.

## System design and operations

The RBNZ is the operator of the ESAS System. RBNZ provides services to ESAS Accountholders in accordance with the ESAS Rules. The System allows:

1. Accountholders to give instructions for amounts to be transferred between exchange settlement accounts. The ESAS Rules provide that once a transaction is settled, the settlement is irrevocable.

2. Accountholders with requisite repurchase facilities with RBNZ to raise funds which are credited to their account using RBNZ's ORRF. This facility allows certain Accountholders to sell eligible securities to RBNZ under a repurchase agreement on specified terms. The required transfers of securities are effected in the NZClear system and payment for the securities is effected in ESAS.
3. Accountholders earn interest on end-of-day balances, in accordance with terms specified by RBNZ.
4. Accountholders to interrogate the ESAS System in order to report exchange settlement account balances and the status of transactions.
5. Accountholders to allocate systems access rights to their own staff in respect of the Accountholder's own exchange settlement account.

Accountholders submit instructions to the System via electronic means, primarily via the dedicated telecommunications networks, via the internet, or via the SWIFT system. In all cases the System has security features in place designed to ensure that access is authorised and instructions received are authenticated.

There are three primary interfaces or 'Accountholder Submitting Systems', which are used by ESAS Accountholders to submit payment instructions to ESAS:

- directly from the NZClear system;
- via the SWIFT system where members of the Assured Value Payment (AVP) closed user group use ESAS to pay other members of that closed user group. The RBNZ is the administrator of the AVP closed user group; and
- via the SWIFT system where members of the Settlement Before Interchange (SBI) closed user group use ESAS to pay other members of that closed user group. Payments NZ (PNZ) is the administrator of the SBI closed user group.

SBI is a retail payment system, consisting of a set of rules governing the exchange via SWIFT files of retail transactions. The net value of those files is settled in ESAS. SBI is operated by PNZ.

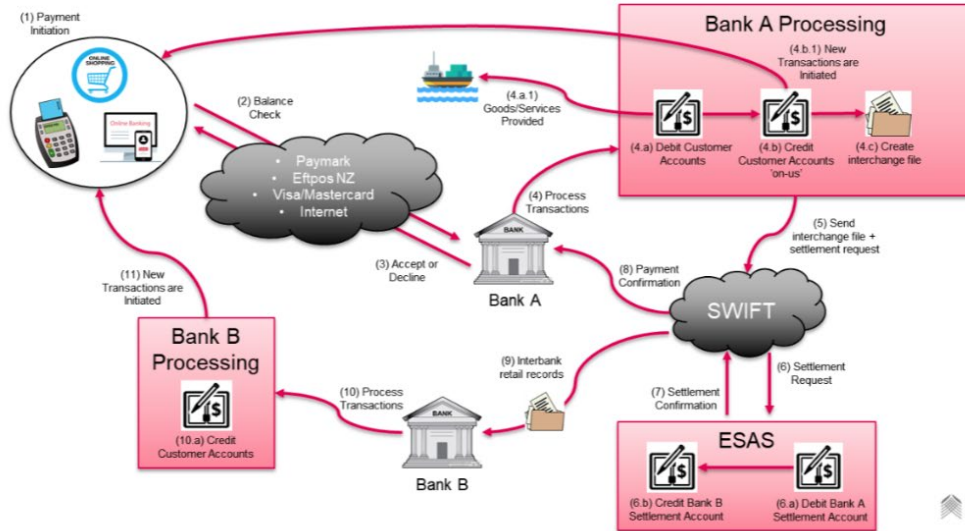
Once an SBI settlement has been effected in ESAS, a confirmation is sent to SWIFT which then allows an associated interchange file containing underlying payment details to be released to the destination bank.

High Value Clearing System (HVCS), is a company owned by eight registered banks, provides a set of rules for customer-to-customer real-time payments and for high-value payments between participating financial institutions. Settlement occurs in ESAS.

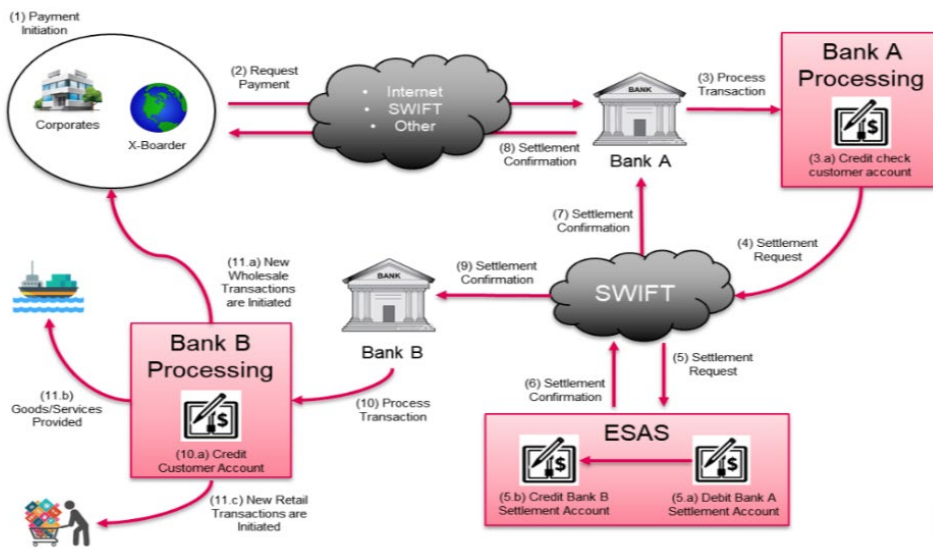
NZClear System is the securities settlement and central securities depository for a broad range of fixed-interest securities and equities that are issued in New Zealand. NZClear has been operating in New Zealand since 1990. NZClear is owned and operated by RBNZ.

NZClear works in an integrated manner with ESAS to support DVP Model 1, which is gross settlement of both funds and securities legs, whereby settlement of securities and associated cash payments occur on an irrevocable and simultaneous basis. For a transaction to be settled, both parties must enter details of the transaction into the System and relevant elements of the transaction must be 'matched' by the System. Once a transaction is settled it cannot be revoked.

## Retail Electronic Payments



## Wholesale Electronic Payments



## 4. Standard by standard narrative disclosures

This section of the report contains detailed disclosure information for each standard for FMIs. The disclosure for each standard is intended to provide sufficient detail and context to enable the reader to understand ESAS's approach for compliance with the standard.

### Standard 1: Legal Basis

#### Assessment

#### ESAS Complies with Standard 1

- 1) **An operator must ensure that the FMI has rules and contracts that are legally enforceable in respect of all material aspects of the FMI's activities in all relevant jurisdictions.**

The Reserve Bank of New Zealand (RBNZ), as Operator of the Exchange Settlement Account System (ESAS), ensures that the System's Rules and contracts are legally enforceable in respect of all material aspects of the FMI's activities in all relevant jurisdictions. ESAS operates as New Zealand's principal RTGS system, providing irrevocable and final settlement of payments between Settlement Accountholders in central-bank money.

Following written consent from all Accountholders and approval by the Regulator under section 39 of the FMI Act, the former ESAS Terms and Conditions were formally converted into the ESAS Rules effective 1 May 2025 (with minor terminology amendments approved 30 June 2025). The Rules form a binding and enforceable contract between RBNZ and each Accountholders and are governed by New Zealand law. ESAS was declared a designated FMI under the FMI Act effective 1 March 2024 through the Financial Market Infrastructures (Designation Notice — ESAS) 2023, reinforcing the statutory certainty of the Rules and settlements.

Under Sub-part 5 of Part 3 of the FMI Act, ESAS benefits from statutory certainty for settlement finality, netting, and insolvency protections (sections 54–60). This includes confirmation that settlements effected in accordance with the Rules are final and irrevocable and cannot be voided or reversed in any proceedings within New Zealand or overseas. The FMI Standards issued under the FMI Act provide ongoing regulatory requirements for ESAS governance, operational risk, and contingency arrangements, ensuring alignment with the CPMI-IOSCO PFMI framework adapted for New Zealand.

The enforceability of ESAS's activities extends across various New Zealand laws, including the Property Law Act 2007, Contracts and Commercial Law Act 2017, Companies Act 1993, Financial Markets Conduct Act 2013, and FMI Act. These laws ensure that contracts, insolvency proceedings, and settlement processes operate with a high degree of certainty, protecting the integrity of the System.

Rule amendments are subject to formal Regulator approval under sections 38–39 of the FMI Act, ensuring clarity and consistency with New Zealand law. The Rules require Accountholders to comply with RBNZ directions necessary for sound and efficient operations consistent with the FMI Act. The designation under the FMI Act and the statutory confirmations in sections 54–60 ensure

that settlement instructions, obligations, netting, and property transfers made under the Rules are valid and enforceable. Section 103A of the Personal Property Securities Act 1999 further confers a 'super-priority' on the Operator's interests in Settlement Accounts.

ESAS's legal basis provides a comprehensive and statutorily supported framework for the operation of the FMI. The combination of binding Rules, FMI Act protections, and independent legal opinions (Chapman Tripp Legal Opinion October 2025) delivers a high degree of certainty that actions taken under the Rules cannot be voided or reversed, demonstrating full compliance with FMI Standard 1 (Legal Basis).

**2) Further to the requirements in clause (1), an operator must ensure that:**

**a) In operating the FMI, it:**

**i) Provides a high degree of certainty for each of the material aspects of the FMI's activities in all relevant jurisdictions;**

ESAS is an RTGS payment system, owned and operated by the RBNZ. It is the system by which the RBNZ provides settlement account services in New Zealand to banks and other financial institutions approved by the RBNZ to have Exchange Settlement Accounts (Accountholders). The RBNZ also holds an Account within the system.

The material aspects of ESAS' activities requiring a high degree of certainty are those that support the provision of real-time irrevocable settlements of payments between Accountholders. This is achieved by:

- Accountholders submitting transactions to ESAS through authorised submitting systems, including NZClear, the ESAS–SWIFT Interface (ESI) and the SBI Interface administered by PNZ;
- the simultaneous crediting and debiting of Accounts by the System; and
- the requirement that Accounts must always be in credit.

A high degree of legal certainty for these activities is derived from:

- 1.** The ESAS Rules (effective 1 May 2025, with minor amendments 30 June 2025), which form a binding and enforceable contract between RBNZ as the System Operator and each Accountholder. The Rules were approved by the Regulator under section 39 of the Financial Market Infrastructures Act 2021 (FMI Act).
- 2.** The declaration of ESAS as a designated FMI under the FMI Act, with effect from 1 March 2024, pursuant to the Financial Market Infrastructures (Designation Notice — ESAS) 2023. This designation provides statutory certainty that settlements, netting and transfers effected under the Rules are valid, binding and irrevocable despite any contrary law or enactment (sections 54–60 FMI Act) and that the Operator's interest in Settlement Accounts has super-priority under section 103A of the Personal Property Securities Act 1999.
- 3.** The Settlement Submission Mechanism (which determines the order and combination in which Authorised Payment Instructions are queued, tested, and settled in ESAS).
- 4.** The applicable laws of New Zealand governing property, contracts, insolvency, companies, securities, trusts, banking, secured interests and liability, including the Property Law Act 2007, Contracts and Commercial Law Act 2017, Companies Act 1993, Trusts Act 2019, Financial

Markets Conduct Act 2013, Personal Property Securities Act 1999, Reserve Bank Act 2021 and the FMI Act.

5. The FMI Act substantially strengthens the regulation of FMIs in New Zealand. It provides the Regulator (RBNZ for ESAS as a pure payment system) with enhanced oversight of FMI rules, additional crisis-management powers, and imposes requirements for designated FMIs to maintain contingency plans for financial or operational failure. It also empowers the Regulator to issue legally binding minimum standards (FMI Standards) that operators must comply with.
6. The FMI Standards and guidance (operative 1 March 2024, except Standard 23A — Disclosure — 1 March 2025) are based on the CPMI–IOSCO PFMI and adapted for the New Zealand environment with enhancements for operational risk, third-party CSPs, and cyber resilience.

## ESAS Rules

The key legal basis for ESAS is provided by the ESAS Rules, which establish a complete, reliable, and enforceable contract governed by New Zealand law. The Rules incorporate by reference the Settlement Submission Mechanism Notice that determines the order and combination in which payment instructions are tested and settled. The Rules and Notice are specified in the Reserve Bank of New Zealand (Designated Settlement Systems) Order 2004 as the two documents that evidence the ESAS rules.

The Rules address:

- settlement finality and irrevocability;
- operation of the System;
- rights, obligations and powers of the RBNZ as Operator, including to act on Authorised Payment Instructions, notify Participants of errors and Notifiable Events, and suspend accounts or system operations where necessary; and
- liability provisions for both RBNZ and Participants.

Under clause 5.1 of the Rules, all settlements of Authorised Payment Instructions are final and irrevocable. Legal certainty of settlement and finality is reinforced by ESAS's designation as a Designated FMI under the FMI Act.

- ii) **is supported by a legal opinion that demonstrates the enforceability of the FMI's rules and contracts across all relevant jurisdictions;**

Following ESAS's designation as a Designated FMI on 1 March 2024 and the conversion of the Terms and Conditions into the ESAS Rules (effective 1 May 2025, with minor amendments 30 June 2025), the System Operator obtained an updated Legal Basis Opinion and NZ Law Enforceability Opinion from Chapman Tripp in October 2025. These opinions confirmed that:

1. The material aspects of ESAS's activities are:
  - a. acting upon electronically submitted payment instructions from Participants to debit one Settlement Account and credit another Settlement Account via an authorised electronic submitting mechanism; and
  - b. the gross settlement of funds once the transaction instruction is authenticated, whereby related cash payments are settled on an irrevocable and simultaneous basis.

2. The only relevant jurisdiction in which ESAS operates, and therefore the jurisdiction providing the legal basis for ESAS's activities, is New Zealand. All settlements are conducted in central-bank money held at RBNZ, and New Zealand law governs the ESAS Rules and the Settlement Submission Mechanism Notice.
3. The conclusions in the 23 October 2025 Legal Opinions support the System Operator having:
  - a high degree of certainty for each of the material aspects of ESAS's activities in New Zealand;
  - a high degree of certainty that the ESAS Rules and related contracts are clear, enforceable, and consistent with relevant New Zealand laws and regulations;
  - a reasonable basis to demonstrate the enforceability of all material aspects of ESAS's activities to the Regulator and Participants in a clear and understandable way; and
  - a high degree of certainty that actions taken by the System Operator under the ESAS Rules and the Settlement Submission Mechanism Notice cannot be voided, reversed, or subject to stays, except as qualified under section 56 of the FMI Act (24-hour insolvency rule).
  - iii) **This legal opinion should be reviewed and updated where required at least every two years or whenever there are material changes that may have an impact on the opinion;**

Legal opinions are reviewed at least every two years and updated following any material legal or operational change. The most recent Chapman Tripp opinion (October 2025) confirms that the ESAS Rules remain enforceable under the current FMI Act regime and continue to provide a high degree of legal certainty.

- b) **it has rules and contracts in relation to the FMI that are clear, enforceable, and consistent with relevant laws and regulations in all relevant jurisdictions in which the FMI operates, including New Zealand; and**

The ESAS Rules are clearly drafted and intended for ease of understanding by Accountholders familiar with the mechanics of the financial system, interchange, and settlement. The Reserve Bank of New Zealand (RBNZ), as the System Operator, seeks legal advice regarding proposed amendments to the ESAS Rules. These amendments are circulated to Settlement Accountholders for consultation and are formally submitted to the regulator to check for any regulatory concerns.

Proposed amendments must be submitted to RBNZ (as the sole regulator of pure payment systems under the FMI Act) for approval in accordance with section 39 of the FMI Act.

The process of engagement with participants on rule changes fosters understanding of the rules, procedures, and contracts governing the system. This consultation and regulatory scrutiny ensure the ESAS Rules are consistent with New Zealand laws.

ESAS Rules and additional information are publicly available on the RBNZ website. Relevant legislation, such as the RBNZ Act and FMI Act, is also publicly accessible.

The legal opinions referred to above in relation to Key Consideration 1 covered the assessment of whether ESAS Rules, procedures, and contracts are clear, understandable, and consistent with relevant laws and regulations. As mentioned above, these legal opinions examined and referred to a range of documents including the ESAS Rules, the Notice to Settlement Accountholders pursuant

to Clause 4.1 of the ESAS Rules, ESAS participation — preliminary assessment form, and application for ESAS participant.

The Legal Basis Opinion stated that the Rules:

1. should be enforceable in respect of each Participant on the basis set out in the NZ Law Enforceability Opinion; and
2. appear consistent with relevant New Zealand laws and regulations;
3. provide a comprehensive set of rules addressing ESAS's material activities by way of the provisions set out in the following clauses of the Rules:
  - a. Clause 2 setting out the rules to the opening and operation of settlement accounts;
  - b. Clauses 3 and 4 setting out the rules and processes relating to payment instructions and the relevant conditions for settlement, including the powers of the Operator to respond to System Faults. The Operator is entitled to rely on all 'Valid Instructions' and undertakes to act on all 'Valid Instructions' in accordance with the Rules. These provisions, in relation to the basis on which settlement instructions are given or received, settlement obligations are determined and calculated, and settlements are effected, are given statutory certainty by section 54 of the FMI Act;
  - c. Clause 5 addressing the finality and irrevocability of Settlement on an Authorised Payment Instruction;
  - d. Clause 6 addressing the Participant's obligations to notify the Operator in certain circumstances, including where it becomes aware of circumstances that could reasonably be expected to adversely affect its ability to comply with the Rules, its eligibility to participate in ESAS, or its ability to transact within the System;
  - e. Clause 8 setting out the rules and procedures relating to the closure of Settlement Accounts, including when the Operator may suspend (or terminate) a Participant's Settlement Account;
  - f. Clause 9 providing the Operator with the ability and powers to suspend ESAS or temporarily extend (or shorten) one or more 'ESAS Days' in certain circumstances necessary to address a 'System Fault' (both terms as defined by the Rules), widespread disruption to Participants, or any threat (or perceived threat) to the maintenance of a sound and efficient financial system;
  - g. Clause 10 setting out the rules and procedure for the Operator and Participants in the event of a System Fault;
  - h. Clauses 11 to 13 setting out the provisions relating to the operation and maintenance of ESAS, including the Operator's obligation to maintain a business continuity plan (BCP) on an ongoing basis;
  - i. Clause 14.1 addressing the rights and obligations of Participants including undertakings to:
    - i. supply such information deemed necessary by the Operator for the purpose of the Rules;
    - ii. comply with the Operator's directions relating to the ESAS where necessary or advisable for compliance with Part 5C of the BPS Act / Part 3 of the FMI Act, or to ensure the sound and efficient operation of ESAS; and

- iii. ensure all information provided to the Operator is accurate and complete in all material respects and will promptly notify the Operator if that ceases to be the case.
  - j. Clause 14.2 addressing the Operator's obligations, including to provide Participants with ancillary services (such as account statements) as agreed, ensure Participants are able to make real-time enquiries on ESAS (including status of Payment Instructions), keep accurate and secure records for a period of seven years, and have ESAS audited in accordance with the Rules); and
  - k. Clauses 17 and 18 setting out the limitations on the Operator's liability under the Rules and the remedies available to Participants;
  - l. In the remaining provisions, address other matters such as fees, confidentiality, Rules amendments, governing law, dispute resolution, and other boilerplate and operational provisions.
4. The conclusions made in this legal opinion supported the System Operator having a high degree of certainty that ESAS has rules and contracts that are clear, enforceable, and consistent with relevant laws and regulations in all relevant jurisdictions (New Zealand).
  5. The Rules and additional information relating to ESAS are publicly available on the RBNZ's website.
    - c) **it can demonstrate the enforceability of all material aspects of the FMI's activities to the regulator, participants, and, where relevant, participants' customers, in a clear and understandable way; and**

The legal basis for ESAS's activities includes its designation as a designated FMI under the FMI Act (effective from 1 March 2024). Designation under the FMI Act also provides statutory certainty with respect to settlement instructions, obligations, netting, and settlement finality.

Legal advice is sought for any changes to the ESAS Rules, and regulatory approval is required for these changes per sections 38–42 of the FMI Act.

RBNZ maintains a Markets and Payments section on its website, providing a clear explanation of the RBNZ's role as the operator of ESAS. This includes public materials that explain ESAS operations, settlement processes, business continuity arrangements, and technical documentation.

The ESAS Rules, along with assessments, annual reports, and other information for Accountholders, are published online.

A process for changing the ESAS Rules, either on a bilateral or general basis, is in place. Legal advice is obtained for all rule changes.

- d) **there is a high degree of certainty that actions taken by an operator under the rules will not be voided, reversed, or subject to stays; and**

The ESAS Rules are governed by New Zealand law.

All transactions occur within New Zealand, and the relevant assets are held in the country. Since 2012, overseas-incorporated Accountholders have been required to provide a legal opinion ensuring the ESAS Rules are valid and binding in their jurisdiction.

Section 55 of the FMI Act ensures that the finality and irrevocability of settlements apply even if foreign courts or creditors seek to challenge a settlement in insolvency proceedings.

Section 59 of the FMI Act ensures that New Zealand law prevails over the Insolvency (Cross-border) Act 2006 when conflicts arise between foreign and domestic insolvency laws.

Legal precedent: No adverse court rulings have occurred regarding the enforceability of the ESAS Rules.

- e) where the FMI operates in multiple jurisdictions, an operator identifies and mitigates the risks arising from any potential conflict of laws across those jurisdictions.

The ESAS System operates only in New Zealand and settles only New Zealand-based payments, and although a number of Accountholders are incorporated in, or operate from, a foreign jurisdiction, the ESAS Rules are governed by New Zealand law.

The principal risks in connection with overseas incorporated Accountholders are that:

- any act or thing that is required to be fulfilled or effected under a foreign law, in order to ensure the validity or effectiveness of the ESAS Rules, is not duly fulfilled or effected;
- a New Zealand court may not enforce a contractual provision which may be or become illegal under the laws of another jurisdiction in which it is to be performed; and
- proceedings may be stayed if the subject matter of the proceedings has previously been considered by, or is concurrently before, another court in another jurisdiction, or another forum, having competent jurisdiction, is the more appropriate forum for those proceedings.

The System Operator has considered these in relation to the jurisdictions in which Accountholders are incorporated and has formed the view that there are no such material risks, for the reasons elaborated in response to Key Considerations 1 to 4. In addition, as stated in response to Key Consideration 4:

- Section 55 of the FMI Act provides that the statutory confirmation of the finality and irrevocability of settlements through ESAS as a designated settlement system also applies where an application to a New Zealand court is made by a foreign court, foreign representative, or foreign creditor to reverse, repay, recover, or set aside a settlement that relates to an insolvency (in any form, whether personal or corporate) within the jurisdiction of that foreign court, foreign representative, or foreign creditor; and
- The RBNZ as System Operator requires that, before accepting an application from an overseas incorporated entity to join ESAS, a legal opinion from a law firm in the applicant's home jurisdiction must be provided confirming that the ESAS Rules will be valid and binding on the Accountholder under the laws of their home jurisdiction.

In addition, as noted above, the System Operator the NZ Law Enforceability Opinion which supported that the choice of New Zealand law as the governing law of the Rules would be recognised and enforced in any proceedings taken in New Zealand in relation to the Rules, and a New Zealand court would give effect to the provision in the Rules under which Participants irrevocably submit to the non-exclusive jurisdiction of the courts of New Zealand.

## Standard 2: Governance

### Assessment

#### ESAS Complies with Standard 2

- 1) **An operator must ensure that governance arrangements pertaining to the operation of the FMI:**
  - a) **Are clear and transparent.**

The governance arrangements for ESAS are grounded in the provisions of the Reserve Bank Act, which outlines the RBNZ's high-level objectives, functions, and governance structure. This framework ensures transparency in how ESAS operates, with defined roles and responsibilities that promote clarity for all stakeholders involved.

The RBNZ's main objectives include financial stability and otherwise acting as New Zealand's central bank in a way that furthers the purposes of the Reserve Bank Act (section 9(1)). The RBNZ's functions include acting as the central bank for New Zealand (section 10(1)), which may involve providing settlement accounts and operating payment and settlement systems (sections 116(e) and (f)).

The Reserve Bank Act confirms that operating ESAS comes within the RBNZ's public policy mandate, and the above statutory objectives and functions inform the way the RBNZ operates ESAS, ensuring that a high priority is placed on ESAS's safety and efficiency. A safe and efficient ESAS is critical to the smooth functioning of the economy, and close monitoring by the RBNZ ensures the system remains robust and resilient.

- b) **Promote the safety and efficiency of the FMI.**

The main purpose of the RBNZ Act is to promote the prosperity and wellbeing of New Zealanders and contribute to a sustainable and productive economy (section 3(b)). The RBNZ's main objectives include financial stability and otherwise acting as New Zealand's central bank in a way that furthers the purposes of the Reserve Bank Act (section 9(1)). The RBNZ's functions include acting as the central bank for New Zealand (section 10(1)), which may involve providing settlement accounts and operating payment and settlement systems (sections 116(e) and (f)).

The Reserve Bank Act confirms that operating ESAS comes within the RBNZ's public policy mandate, and the above statutory objectives and functions inform the way the RBNZ operates ESAS, ensuring that a high priority is placed on ESAS's safety and efficiency. A safe and efficient ESAS is critical to the smooth functioning of the economy, and close monitoring by the RBNZ ensures the system remains robust and resilient.

- c) **Support the stability of the broader financial system and other relevant public interest considerations, and the objectives of relevant stakeholders.**

Operating ESAS falls within the RBNZ's public policy mandate, reinforcing the commitment to financial stability. By providing a robust and efficient settlement system, ESAS enhances the stability of the financial system as a whole. The introduction of RTGS in 1998 significantly reduced settlement risk by enabling real-time transactions, thus mitigating potential chaos from bank failures. The RBNZ actively monitors ESAS to ensure its robustness and resilience, supporting not only its operational objectives but also addressing public interest concerns.

In addition, operational resilience, especially in regard to systems security and availability, and financial processing accuracy, is maintained in a manner commensurate with a low risk appetite for incident or error. ESAS's objectives, which are a combination of business as usual and project-specific targets, typically have a considerable leaning towards overall FMI integrity, governance, and meeting stakeholder needs. An ESAS Participation Group (EPG) exists and monitors progress towards achieving ESAS's objectives via regular meetings throughout the year.

An annual report for ESAS is completed at June year-end and this formally sets out ESAS's objectives for the year ahead. This report has high visibility as it is circulated to all Accountholders and is published on the RBNZ's website. The ESAS Annual Report contains considerable retrospective commentary on the year just completed, including key performance indicator (KPI) metrics, operational performance, commercial performance, financial results, and risk management activities. The report is also tabled at the RBNZ's Board Committee for review and discussion and is shared with the regulator for ESAS.

The RBNZ conducts an annual survey of Accountholders and asks Accountholders to rate the services provided and to make suggestions for change. The survey is published on the RBNZ's website. Also, Accountholders are consulted on major system changes and have the opportunity to suggest system changes.

**2) Further to the requirements in clause (1), an operator must also ensure that: There are documented objectives for the FMI that place a high priority on the safety and efficiency of the FMI, and that explicitly support financial stability and other relevant public interest considerations.**

The governance structure of the Exchange Settlement Account System (ESAS) is integrated within the Reserve Bank of New Zealand (RBNZ) framework, ensuring that its objectives prioritise safety, efficiency, and financial stability. The RBNZ operates under the mandates outlined in the Reserve Bank Act, which emphasises the promotion of the prosperity and wellbeing of New Zealanders and the sustainable functioning of the economy. These objectives include ensuring financial stability and providing effective payment and settlement systems, including ESAS.

The RBNZ's commitment to maintaining a safe and efficient ESAS aligns with its overarching goal to mitigate risks in the financial system, enhancing transaction finality and reducing settlement risks through RTGS. This is documented in the RBNZ's accountability documents, including the annual Statement of Intent, which reflects the strategic priorities and public interest considerations that guide the operation of ESAS.

**b) The FMI has documented governance arrangements that:**

**i) Provide clear and direct lines of responsibility and accountability.**

The governance of ESAS is clearly defined within the RBNZ's organisational structure. The Board of the RBNZ, which is independently appointed, holds ultimate responsibility for all decisions, including those regarding ESAS operations. Day-to-day management is delegated to the Governor, while the FMI&S Directorate oversees the operations of ESAS. The Director of FMI&S, reporting to the Assistant Governor/General Manager, is accountable for the management and ongoing development of ESAS, creating a clear line of accountability from the Board to senior management.

In 2025, the Board established the Payments and Settlements Oversight Committee (PSOC) to strengthen its oversight of the RBNZ's designated financial market infrastructures (ESAS and

NZClear). The PSOC was formed following feedback from the FMI Regulators that the Board enhance its focus on the operation and governance of these systems as stand-alone entities. The PSOC is a Board sub-committee tasked with providing focused attention on the performance, risk management, and strategic direction of ESAS and NZClear, thereby enhancing Board accountability and decision-making around the Bank's critical FMIs.

- ii) **Are disclosed in an appropriate manner to owners, the regulator, participants, and the public.**

The RBNZ ensures transparency in its governance arrangements through various accountability documents, including the annual report for ESAS, which outlines governance practices, risk management, and operational performance. These reports are published on the RBNZ's website, providing accessible information to stakeholders, including Accountholders and the public. Furthermore, the RBNZ engages with Parliament's Finance and Expenditure Select Committee, providing an additional layer of public accountability regarding its operations and decisions related to ESAS.

The RBNZ also conducts annual surveys of Accountholders to gather feedback on services and operational effectiveness, ensuring that participants have a voice in governance matters and that their perspectives are considered in decision-making processes.

- c) **The roles and responsibilities of its board of directors are clearly specified, and there must be documented procedures for its functioning, including policies and procedures to identify, address, and manage member conflicts of interest.**

The Board of the RBNZ serves as the governing body, with authority to exercise the powers and perform the functions of the RBNZ, including overseeing the operation of ESAS. The appointment process for directors is structured to ensure that individuals possess the necessary knowledge, skills, and experience to support the RBNZ's objectives. The Governor-General, on the recommendation of the Minister of Finance, appoints Board members while promoting diversity within the Board.

To manage conflicts of interest, the Reserve Bank Act includes specific sections (61–72) detailing the procedures for identifying, disclosing, and addressing interests that may conflict with the responsibilities of Board members. This framework ensures that all Board members disclose any relevant interests prior to their appointment and adhere to protocols for managing actual or perceived conflicts. The RBNZ also maintains a Conflicts of Interest policy that all employees, including those in the FMI&S, must comply with, fostering a culture of integrity and accountability within the organisation.

- d) **The board of directors consistently reviews both the board's overall performance and the performance of its individual directors in relation to the FMI.**

The Board has committed to conducting regular reviews of its overall performance, as well as the performance of individual directors and Board committees. These reviews are scheduled at least annually and are essential for maintaining high standards of governance and accountability.

Overall the RBNZ's governance structure, established through the Reserve Bank Act, outlines clear roles and responsibilities for the Board, incorporates comprehensive procedures for conflict management, and includes regular performance reviews, thereby supporting the integrity and effectiveness of ESAS operations.

- e) **The board of directors contains suitable members with the appropriate skills and incentives to fulfil its roles as operator of the FMI (including non-executive directors).**

Members of the Board are appointed through a process governed by the Reserve Bank of New Zealand Act. The Governor-General appoints Board members based on recommendations from the Minister of Finance. According to the RBNZ Act, the Minister may only recommend individuals who, in their opinion, possess the necessary knowledge, skills, and experience to assist the RBNZ in achieving its objectives and fulfilling its functions. This ensures that the Board members have the expertise required to oversee the RBNZ's roles, including its function as the operator of ESAS.

The Act also emphasises the importance of promoting diversity in the Board's membership. The Board consists of between five and nine members, with all being non-executive directors except for the Governor, who serves as an executive member. The details regarding Board members, including their other directorships and employment, are made available to the public through the RBNZ's website, ensuring transparency in its governance structure.

The Governor's appointment is subject to additional scrutiny, as the Minister may only recommend a Governor candidate who has been nominated by the Board, ensuring that the individual's skills and qualifications align with the RBNZ's broader responsibilities, including the management of ESAS operations.

- f) **In relation to the FMI's management:**

- i) **The roles and responsibilities of management are clearly set out and delineated from the roles of the board of directors, and documented; and**

Executive-level responsibility for ESAS has been delegated by the Governor to the Assistant Governor/General Manager for Economics, Financial Markets, and Banking. The Assistant Governor must possess significant experience in the financial services industry, ensuring proper leadership at the executive level. Reporting to the Assistant Governor, the Director of FMI&S manages the day-to-day business operations and overall business planning of ESAS.

The roles and responsibilities of management and staff responsible for the day-to-day operation of ESAS are clearly documented in their position descriptions. This documentation ensures a clear delineation between the responsibilities of the Board of Directors, which provides high-level oversight, and management, which handles daily operations.

- ii) **Management has the appropriate experience, a mix of skills, and the integrity necessary to discharge its responsibilities for the operation and risk management of the FMI.**

The RBNZ ensures that staff and management working in FMI&S, including those managing ESAS operations, are selected based on their relevant skills, experience, and ability to handle the associated risks. Management positions are filled with employees who have the appropriate mix of skills and experience necessary to manage the development and operation of ESAS.

The RBNZ has robust human resources policies that ensure that recruitment, selection, and management practices are aligned with maintaining the integrity and performance of the system. Employees are selected based on their suitability to perform the specific requirements of their role, which includes relevant training, qualifications, and experience. The RBNZ also has a formal performance management programme in place, ensuring expectations are communicated clearly,

and that regular feedback is provided to employees. This system supports the development of capable and accountable management for the operation of ESAS.

RBNZ staff, including those in FMI&S, are required to adhere to the RBNZ's Code of Conduct and Conflicts of Interest policies, ensuring high standards of integrity. These policies extend to all critical support functions associated with the operation of ESAS, including risk and compliance, internal audit, and digital services.

Furthermore, the RBNZ has established human resources policies to ensure that all staff, including those within the FMI&S possess the appropriate skills and incentives to perform their roles effectively. These policies are detailed in the RBNZ's human resources framework, ensuring that the organisation maintains a skilled and competent workforce.

- g) There is a clear, documented risk management framework (RMF) for the FMI that includes the FMI's risk tolerance policy, assigns responsibilities and accountability for risk decisions, and addresses decision-making in crises and emergencies.**

The RBNZ has a comprehensive RMF consisting of policies, guidance, and practices to ensure a consistent and systematic approach to identifying, assessing, and managing risks. This framework is underpinned by a Board-approved Risk Management Policy, which establishes principles for managing risks to achieve the RBNZ's objectives, including the safe and efficient operation of ESAS. The framework incorporates the RBNZ's risk tolerance policy, assigning responsibilities and accountability for risk management decisions at all levels of the organisation.

The core of the framework is based on the 'Three Lines Model' for risk management:

- 1.** First Line (Business functions): FMI&S, as the first line, is responsible for owning and managing risks related to the day-to-day operation of ESAS.
- 2.** Second Line (Enterprise Risk Management and Compliance): The RBNZ's Risk and Compliance Directorate develops and oversees the implementation of effective risk management processes.
- 3.** Third Line (Independent Assurance): Internal Audit provides independent assurance to senior management and the Board regarding the adequacy and effectiveness of risk management and control processes.

The framework also addresses crisis and emergency decision-making, ensuring that risks are managed proactively in both routine and exceptional situations. The RBNZ's risk management process is modelled on ISO 31000:2018, ensuring a structured approach to risk identification, assessment, and management.

Oversight of the risk management and assurance frameworks for ESAS now falls within the PSOC's mandate. The committee reviews risk reports, assurance plans, and audit findings pertaining to these FMIs and monitors management's implementation of risk treatments and BCPs. This additional governance layer strengthens the independence and effectiveness of risk oversight and signals to the FMI Regulators that the Board is committed to enhanced accountability for the operation of its FMIs.

- h) There are governance arrangements for the FMI that ensure the risk management and internal control functions have sufficient authority, independence, resources, and access to the board of directors.**

RBNZ's governance structure ensures that risk management and internal control functions have the necessary authority, independence, and resources to fulfil their roles effectively. The Risk and Compliance Directorate (second line) operates independently from FMI&S (first line) to ensure objective oversight of risk management activities. This independence is critical to the integrity of the risk management process.

Internal Audit (third line) is an independent assurance function that provides regular reports on the effectiveness of risk management and internal controls to senior management and the Board. This ensures that the Board has direct access to information on risk management performance and can take necessary actions where needed. The governance framework also ensures that both risk management and internal control functions are adequately resourced to perform their duties. Its board of directors takes responsibility for ensuring that:

- The design, rules, overall strategy, and major decisions appropriately reflect the legitimate interests of the FMI's direct and indirect participants, and other relevant stakeholders; and
- the RBNZ Board is responsible for ensuring that the design, rules, and overall strategy of ESAS reflect the legitimate interests of its participants and stakeholders. This is achieved through regular consultations with direct and indirect participants, regulators, and other key stakeholders. Feedback is incorporated into the design and decision-making processes to ensure that the interests of all relevant parties are considered and addressed.
- Major decisions are clearly disclosed in a reasonable timeframe after the decision is taken to relevant stakeholders and, where there is a broad market impact, the public. Under the oversight and direction of the Board, major decisions are disclosed in a timely manner to relevant stakeholders. Where decisions have a broad market impact, the information is disclosed publicly in accordance with regulatory requirements and the principles of transparency. This approach ensures that all stakeholders are kept informed of significant changes affecting ESAS and that the Board remains accountable for its decisions.

Oversight of the risk management and assurance frameworks for ESAS now falls within the PSOC's mandate. The committee reviews risk reports, assurance plans, and audit findings pertaining to these FMIs and monitors management's implementation of risk treatments and BCPs. This additional governance layer strengthens the independence and effectiveness of risk oversight and signals to the FMI Regulators that the Board is committed to enhanced accountability for the operation of its FMIs.

## Standard 3: Framework for the Comprehensive Management of Risks

### Assessment

#### ESAS Complies with Standard 3

- 1) **An operator must have a sound risk management framework pertaining to the FMI that sets out how the operator comprehensively manages legal, credit, liquidity, operational, and other relevant and material risks.**

ESAS adheres to the enterprise risk management approach defined in the RBNZ's Board-approved Risk Management Policy. This policy, which is reviewed biennially by the Board, is part of a broader risk-based framework comprising policies, guidance, and practices that support the RBNZ in achieving its objectives.

The RBNZ employs the 'Three Lines Model' for managing risk, which delineates responsibilities across three lines:

- **First Line:** The FMI&S Directorate operates as the first line, responsible for identifying, managing, and controlling business-specific risks associated with the operation of ESAS. This includes maintaining risk-management systems, reporting on the effectiveness of risk controls, and implementing necessary enhancements and remedial actions.
- **Second Line (Enterprise Risk Management and Compliance):** The Risk and Compliance Directorate operates as the second line, overseeing and developing effective risk management processes. This line is responsible for implementing and ensuring compliance with risk management guidelines (RMG) across RBNZ.
- **Third Line (Independent Assurance):** Internal Audit functions as the third line, providing independent assurance to senior management and the Board regarding the effectiveness of risk management and internal controls.

The RBNZ's RMG, based on ISO 31000:2018 standards, provide the foundation for risk management practices. FMI&S uses these guidelines to identify and prioritise risks, employing a risk taxonomy to categorise common risks, their causes, and impacts. For each identified risk, FMI&S evaluates its potential impact and likelihood, while establishing controls and mitigation strategies to reduce these risks.

ESAS has implemented a RMF specifically tailored to the unique risk profile of the ESAS. This RMF is distinct but aligned with the overarching Enterprise Risk Management Framework (ERMF) and associated guidelines, ensuring consistency in risk management across all levels. This framework incorporates procedures, policies, and governance that are in place to mitigate risks effectively, reflecting the low-risk appetite of ESAS. The ESAS RMF is designed to define all risks associated with the system, including legal, operational, third party and regulatory compliance risks.

Risk information is systematically captured in the Directorate Risk Register, reviewed quarterly by management. The Risk and Compliance Directorate compiles this information and reports it to the Board, or as needed under the 'no surprises' protocol.

Periodic audits of internal controls are conducted by PricewaterhouseCoopers (PwC) on behalf of RBNZ's external auditor, the Auditor-General. These audit reports are reviewed by the Audit Committee, which includes external auditors and RBNZ management.

FMI&S maintains dedicated roles to support the effective implementation of its enterprise risk management framework. This includes the Manager, FMI Compliance and Resilience, who is responsible for oversight of compliance with the FMI Standards, regulatory engagement, maintenance of FMI risk registers, and coordination of external assurance activities. The team also includes a Resilience Advisor, who supports the identification and management of operational and resilience risks across FMI operations, and a Membership Advisor, who is responsible for assessing and monitoring participant-related risks, including compliance with access, participation, and ongoing membership requirements. These roles are supported by a Directorate Risk Forum, which provides a structured mechanism for aligning FMI&S-specific risk management activities with the Reserve Bank's broader Risk Management Policy and for ensuring that risks relevant to FMI operations and participants are appropriately identified, assessed, and managed.

**2) Further to clause (1) an operator must ensure that:**

- a) it has, in relation to the FMI, risk management policies, procedures, and internal systems that enable the operator to identify, measure, monitor, and manage all risks that arise in, or are borne by, the FMI; and**

ESAS has implemented a RMF specifically tailored to the unique risk profile of the ESAS. This RMF is distinct but aligned with the overarching ERMF and associated guidelines, ensuring consistency in risk management across all levels.

This framework incorporates procedures, policies, and governance that are in place to mitigate risks effectively, reflecting the low-risk appetite of ESAS. The ESAS RMF is designed to define all risks associated with the system, including legal, operational, third party, and regulatory compliance risks. ESAS follows the RBNZ's enterprise risk management approach, as described in the Board-approved RBNZ Risk Management Policy. This framework includes comprehensive policies, guidelines, and practices that ensure a risk-based approach to achieving RBNZ's objectives. RBNZ manages risk through the 'Three Lines Model', which divides responsibilities as follows:

- First line: FMI&S is responsible for identifying business-specific risks, applying risk controls, maintaining risk management systems, and reporting on the effectiveness of these controls.
- Second line: The RBNZ's Risk and Compliance Directorate oversees and implements the enterprise-wide risk management processes.
- Third line: Internal Audit provides independent assurance on the effectiveness of risk management to senior management and the Board.

The RBNZ RMG are structured according to ISO 31000:2018 standards and include a methodology for identifying and prioritising risks. This methodology uses a risk taxonomy to define common risks, their causes, and impacts. Risks identified by FMI&S are assessed for their potential impact and probability, with controls and mitigation strategies established to manage them. Risk information is maintained in the Directorate Risk Register, which FMI&S reviews quarterly.

External audits of internal controls are conducted periodically by PwC, representing the RBNZ's external auditor, the Auditor-General. Audit reports are presented to the Board's Audit Committee, ensuring thorough oversight of ESAS's risk management systems.

- b) it reviews the risk management framework relating to the FMI on at least an annual basis, and whenever the risk to the FMI materially changes;**

The framework is regularly reviewed and refined to adapt to evolving challenges and stakeholder needs, particularly concerning systemic risks, cyber security measures, and regulatory requirements under the FMI Act. This alignment ensures that the risk management practices within ESAS are robust, effective, and consistent with broader risk management strategies across the organisation.

- c) it provides incentives to FMI participants and, where relevant, their customers, to manage and contain the risks they pose to the FMI;**

As an RTGS settlement system, ESAS is structured to minimise the liquidity or material credit exposures that participants (Accountholders) pose to the System Operator. The System Operator, which does not act as a guarantor or party to any transaction submitted for settlement through ESAS, ensures that participants manage and contain the risks they bring to the system. This is further detailed in the response to Standard 4 and 7: Credit and Liquidity Risk.

To incentivise participants to manage these risks, Accountholders are required to notify the System Operator of any circumstances that could potentially affect their ability to comply with ESAS Rules, their authority to make payments, or their ability to transact within the ESAS system. The System Operator actively monitors operational incidents involving Accountholders and follows up as necessary. Any material non-compliance or events that materially increase risk to the ESAS must be immediately reported to the Regulator.

The RBNZ, acting as the System Operator, may suspend or terminate an Accountholder's account for non-compliance with ESAS Rules, thereby encouraging adherence to risk management practices. Furthermore, eligibility to become an Accountholder is contingent upon meeting strict criteria that assess the applicant's operational capacity, financial condition, risk management expertise, and conformity with legal requirements. These criteria ensure that only those capable of managing and containing risks are granted access to ESAS, thereby protecting the integrity and stability of the system.

In this way, ESAS provides clear incentives for participants to effectively manage and contain the risks they pose, aligning with the broader objective of maintaining financial stability within the system.

- d) it reviews the material risks the FMI bears from and poses to other parties (such as other FMIs, settlement banks, liquidity providers, and service providers) as a result of interdependencies with other parties annually, or whenever the material risk changes, and develops appropriate risk management tools to address these risks.**

The System Operator regularly reviews the material risks it bears from and poses to other entities. This review is conducted as part of the ongoing risk assessment process, including the quarterly update of the Risk Register within the Enterprise-wide RMF. Additionally, the System Operator assesses risks associated with significant changes to the environment, such as new activities or system modifications.

To address these interdependent risks, the System Operator employs a range of risk-management tools. These include SLAs, regular reviews of service provider performance, and documented operational and contingency arrangements. Furthermore, as ESAS is a designated FMI under the FMI Act, both the System Operator and other Accountholders benefit from protections against settlement risk. This legal protection and the associated risk management practices are further discussed in Principle 1: Legal Basis.

Through these measures, the System Operator ensures that the risks arising from its interdependencies with other entities are effectively managed and mitigated, contributing to the overall stability and resilience of the ESAS system.

## Standard 4: Credit Risk

### Assessment

#### ESAS Complies with Standard 4

- 1) **An operator must effectively measure, monitor, and manage the FMI's credit exposures to participants, and those arising from the FMI's payment, clearing, and settlement processes. The operator must maintain sufficient financial resources to cover the FMI's credit exposure to each participant fully and with a high degree of confidence.**

The nature of RTGS settlement in ESAS eliminates credit risk between Accountholders. As settlement occurs in real time, there are no intraday exposures built up between Accountholders through use of the System. There has to be sufficient liquidity in the Accountholders' ESAS Accounts before the settlement can take place. Payment messages are exchanged between Accountholders simultaneously with the transfer of funds across accounts.

The System Operator does not grant overdrafts to Accountholders and therefore the RBNZ is not exposed to credit risk in its role as System Operator. Payments in ESAS are settled in Accountholders' ESAS accounts, which cannot be overdrawn, and the System Operator does not guarantee any transaction submitted for settlement in ESAS. Accordingly, in the event of an Accountholder default the System Operator would not be exposed to a loss.

The RBNZ provides additional facilities to support the efficient functioning of the payment system. The RBNZ can make credit available to Accountholders (as well as to institutions which do not have ESAS accounts) as part of its monetary policy and financial stability functions. The RBNZ may enter FX swap and/or repurchase transactions, including the provision of an A-ORRF for emergency liquidity. The liquidity facilities offered by the RBNZ are structured as monetary policy instruments and are managed and operated by the Financial Markets Department of the RBNZ.

These operations are effected through direct dealing arrangements (supported by internationally recognised agreements — GMRA and ISDA). Participation in ESAS and the associated ESAS Rules does not of itself guarantee an Accountholder access to any liquidity facilities provided by the RBNZ. Any credit risk associated with these facilities is borne by the RBNZ and not the ESAS System.

In addition, settlement risk is mitigated through the use of DVP protocols — this applies to all domestic and most FX trades (the RBNZ encourages the use of Continuous Linked Settlement (CLS) to settle wholesale FX trades).

- 2) **An operator must ensure that:**
  - a) **the FMI has a robust framework to manage its credit exposures to its participants, and the credit risks arising from its payment, clearing, and settlement processes. This includes credit exposures arising from both current exposures and potential future exposures; and**

The nature of RTGS settlement in ESAS eliminates credit risk between Accountholders. As settlement occurs in real time, there are no intraday exposures built up between Accountholders through use of the System. There has to be sufficient liquidity in the Accountholders' ESAS accounts before the settlement can take place. Payment messages are exchanged between Accountholders simultaneously with the transfer of funds across accounts. The System Operator

does not grant overdrafts to Accountholders and therefore RBNZ is not exposed to credit risk in its role as System Operator. Payments in ESAS are settled in Accountholders' ESAS accounts which cannot be overdrawn, and the System Operator does not guarantee any transaction submitted for settlement in ESAS. Accordingly, in the event of an Accountholder default the System Operator would not be exposed to a loss.

- b) in relation to the FMI, it identifies sources of credit risk, routinely measures and monitors credit exposures, and that it uses appropriate risk management tools to control these risks.

The System Operator does not grant overdrafts to Accountholders and therefore RBNZ is not exposed to credit risk in its role as System Operator. Payments in ESAS are settled in Accountholders' ESAS Accounts which cannot be overdrawn, and the System Operator does not guarantee any transaction submitted for settlement in ESAS. Accordingly, in the event of an Accountholder default the System Operator would not be exposed to a loss.

- 3) Further to the requirements in clauses (1) and (2) and in accordance with the requirement to have contingency plans in section 47 of the Act and Standard 17A 'Contingency plans', an operator (where it bears credit risk) must establish explicit rules, policies, and procedures that fully address any credit losses it may face as a result of any individual or combined default among participants, with respect to any of their obligations under the rules of the FMI. These rules, policies, and procedures must:
  - a) address how potentially uncovered credit losses would be allocated, including the repayment of any funds that an operator or FMI may borrow from liquidity providers; and

Payments in ESAS are settled in Accountholders' ESAS Accounts which cannot be overdrawn, and the System Operator does not guarantee any transaction submitted for settlement in ESAS. Accordingly, in the event of an Accountholder default the System Operator would not be exposed to a loss.

- b) indicate the process to replenish any financial resources that it may employ during a stress event, so that the FMI can continue to operate in a safe and sound manner.

Loan accounts, as mentioned in the ESAS Rules, are currently inactive. While the functionality for these accounts exists for financial market and monetary policy purposes, it is not in use at present. Consequently, the potential for uncovered credit losses associated with borrowed funds is minimised.

Moreover, the fees charged to Accountholders for the use of ESAS are collected on a cost-recovery basis. If the RBNZ is unable to collect these fees, it would not result in material losses for the Reserve Bank, further reducing the risk of uncovered credit losses.

- 4) Further to the requirements in clauses (1) and (2), either an operator of a pure payment system or an operator of a securities settlement system must ensure that: a) it covers current and, where they exist, potential future exposures to each participant fully with a high degree of confidence using collateral and other equivalent financial resources (see Standard 5: 'Collateral'); and b) the FMI maintains sufficient resources to cover the exposures of the two participants and their affiliates, who create the largest aggregate credit exposure in the system.

ESAS is a real-time gross settlement (RTGS) system that settles payment instructions individually and irrevocably in central bank money. As a result of its design and operating rules, ESAS does not extend credit to participants and does not create credit exposures between participants or between the system and its participants. Settlement occurs only when the paying Accountholder has sufficient available funds in its exchange settlement account to meet the full value of the payment instruction. Payment instructions that cannot be funded are not settled and remain pending until sufficient funds are available or are cancelled by the Accountholder.

Because ESAS does not permit settlement on a deferred net basis and does not provide intraday credit, overdrafts, or prefunding guarantees, the system does not generate credit exposures that would require coverage through collateral or other equivalent financial resources. Consequently, ESAS is not exposed to the risk of participant default following settlement, and there is no requirement for the system to maintain collateral to cover participant exposures.

**5) Clause (4) applies in a situation where the FMI operates with deferred net settlement in which there is no settlement guarantee, but where the FMI participants face credit exposures arising from its payment, clearing, and settlement processes.**

Clauses (4) and (5) are not applicable to ESAS because they apply only to FMIs that operate on a deferred net settlement basis without a settlement guarantee, where participants face credit exposures between clearing and final settlement.

ESAS operates as a pure payment system using RTGS in central bank money, where each payment is settled individually, immediately, and irrevocably. ESAS does not provide credit, does not net obligations, and does not accumulate exposures between participants. Participants must have sufficient balances in their Exchange Settlement Accounts before a payment can settle.

Because ESAS does not create current or potential future participant credit exposures, the requirements to hold collateral or financial resources to cover such exposures — including the exposures of the two participants creating the largest aggregate credit exposure — do not apply.

**Central counterparties**

Not applicable as ESAS is not a CSP

## Standard 5: Collateral

### Assessment

#### ESAS Complies with Standard 5

- 1) **An operator that requires collateral for the purposes of operating the FMI, to manage the FMI's or its participants' credit exposure, must ensure it only accepts collateral with low credit, liquidity, and market risks. An operator must also set, and enforce appropriately, conservative haircuts and concentration limits.**

The RBNZ provides additional facilities to support the efficient functioning of the payment system.

The RBNZ can make liquidity available to institutions that are Accountholders as part of its monetary policy and financial stability functions. In providing credit liquidity the RBNZ does so in its capacity as a central bank to support monetary policy implementation and financial stability functions, and not in its capacity as System Operator of ESAS.

When providing liquidity, the RBNZ does so on a collateralised basis. It does this through the use of repurchase agreements or FX swaps. Any outright trades are settled on a delivery-versus-payment (DVP) basis.

This policy applies to all of the domestic operations. The Operating Rules and Guidelines for RBNZ domestic market facilities are made available on the RBNZ website and are regularly reviewed. Eligible securities for use as collateral are generally restricted to highly rated liquid securities.

- 2) **Further to the requirements in clause (1) an operator must ensure that:**
  - a) **it establishes prudent valuation practices and develops haircuts that are tested at least annually, and that take into account stressed market conditions; and**

The RBNZ values collateral based on market pricing and applies haircuts that are tested and set to cover anticipated declines in value over a conservative liquidation horizon. Inputs such as credit rating, security maturity, and market conditions are used in these calculations. These practices are continuously monitored to reflect both normal and stressed market conditions.

- b) **stable and conservative haircuts for collateral are established, and that these haircuts are calibrated to include periods of stressed market conditions, to the extent practicable and prudent, to reduce the need for procyclical adjustments; and**

Haircuts applied by the RBNZ are calibrated to ensure the minimisation of loss in value during both normal and stressed conditions. The RBNZ's approach ensures stability in the financial system, reducing the need for procyclical adjustments.

- c) **it avoids concentrated holdings of any assets where this would significantly impair its ability to liquidate such assets quickly without significant adverse price effects; and**

The RBNZ continuously monitors its security holdings, specifically evaluating its position relative to the total amount of securities issued. This helps avoid concentrated holdings and ensures the timely liquidation of assets without adversely impacting market prices.

- d) where an operator accepts cross-border collateral for the FMI, it mitigates the risks associated with the use of that collateral, and ensures the collateral can be used in a timely manner; and

The RBNZ accepts New Zealand dollar-denominated securities issued or guaranteed by foreign governments or supranational agencies. These securities meet strict criteria, such as appropriate credit ratings and lodging requirements in NZClear, which mitigate the risks associated with cross-border collateral and ensure timely usage.

- e) it uses an internal system that is well-designed and operationally flexible for managing collateral.

The RBNZ employs a widely used treasury system designed for central banks, which covers all aspects of collateral management, including daily revaluation, security transactions, margining, and reporting. This system provides operational flexibility and supports the effective management of credit exposures and collateral.

## Standard 6: Margin

### Assessment

**Standard 6 is not applicable to ESAS.**

- 1) An operator of a central counterparty must cover credit exposures to the central counterparty's participants for all products through an effective margin system that is risk-based and regularly reviewed.

## Standard 7: Liquidity Risk

### Assessment

#### ESAS Complies with Standard 7

#### Requirement 1

- 1) **An operator must measure, monitor, and manage the FMI's liquidity risk. An operator must ensure there are sufficient liquid resources available in all relevant currencies to effect same day and, where appropriate, intraday and multiday settlement of payment obligations with a high degree of confidence under a wide range of potential stress scenarios.**

The System Operator is not exposed to any liquidity risk as the ESAS is structured as an RTGS system, and there are no overdrafts allowed. However as Accountholders may face some potential liquidity risks, ESAS provides Accountholders liquidity assistance through its liquidity-efficient design, including incentives for redistribution of Account balances, the provision of liquidity using automated ORRF (A-ORRF) for eligible securities through NZClear, the provision of real-time information on transactions and ESAS balances, and the provision of tools to manage their payments and liquidity. These tools are described below.

Accountholders have access to their payments queue and can prioritise transfer orders and adjust the order as needed for queued transactions. ESAS provides Accountholders with a number of liquidity management features, including; settlement prioritisation, authorisation (Payer to Activate), releasing instructions for settlement at a specific date/time, and configuring a bilateral limit.

In addition, ESAS provides a 'gridlock buster' function. The process involves identifying all eligible and queued settlements that, if settled, would leave Accountholders in a positive position. The process is configured to run every five minutes in ESAS.

The A-ORRF is a facility provided by the RBNZ to approved Accountholders in order to generate additional liquidity if required. The RBNZ can enter into these overnight agreements with any counterparty that has signed the 2011 GMRA (and associated ORRF annex). The facility works on the basis of the RBNZ accepting approved collateral, at a price set by the RBNZ, in return for additional liquidity in ESAS. A-ORRF is typically called upon when an Accountholder wishes to effect a payment but does not have enough cash. This facility can also be invoked on demand. The A-ORRF transaction is settled using the repurchase functionality provided in NZClear. Legal ownership of the securities is transferred into the RBNZ's name. Under the current A-ORRF conditions, the repurchase agreement must be fulfilled overnight (i.e., the Accountholder must repurchase the collateral from the RBNZ the next business day).

These features collectively enhance the liquidity efficiency of the system, allowing Accountholders to navigate potential liquidity risks while ensuring the smooth operation of payment obligations under various stress scenarios.

- 2) **An operator's qualifying liquid resources for the purposes of clause (1) include the following liquid resources:**

Not applicable.

These provisions are not applicable because ESAS, as a central-bank-operated RTGS, does not take on liquidity obligations or maintain a pool of qualifying liquid resources. ESAS settles only in central bank money and only when participants have sufficient balances. The system therefore does not rely on credit lines, FX swaps, repos, commercial bank liquidity, or collateral pools to meet settlement obligations.

**a) cash at the central bank of issue and at creditworthy commercial banks.**

All ESAS operational accounts are held directly with the RBNZ. ESAS therefore has access to central bank money to meet operational liquidity needs.

ESAS does not rely on commercial bank balances.

**b) committed lines of credit.**

ESAS does not rely on external committed credit lines.

As a system operated by the central bank, liquidity — if required — is managed through the RBNZ's own liquidity facilities within its operating framework.

**c) committed foreign exchange swaps.**

Not applicable.

ESAS settles only in New Zealand dollars and does not require foreign exchange swaps to support system operations.

**d) repos.**

ESAS itself does not enter into repo transactions to finance settlement. Any liquidity provided by the RBNZ to participants is governed by the Bank's broader liquidity and collateral policies, not by ESAS holding repo positions.

**e) highly marketable collateral held in custody and investments that are readily available and convertible into cash with prearranged and highly reliable funding arrangements, even in extreme but reasonably foreseeable market conditions.**

ESAS does not hold collateral or investments for liquidity purposes. Participants may access the RBNZ's liquidity facilities using eligible collateral under the Bank's published collateral policy. This ensures liquidity can be generated without ESAS maintaining its own pool of marketable assets.

**f) access to routine credit at a central bank of issue to the extent that the relevant FMI has collateral that is eligible for pledging to (or for conducting other appropriate forms of transactions with) the central bank.**

ESAS, as a system operated by the central bank, has access to central bank liquidity arrangements within the RBNZ's operating framework. Participants may obtain liquidity from the RBNZ using eligible collateral, supporting smooth settlement without ESAS needing to hold qualifying collateral itself.

**3) Further to requirements in clause (1), an operator must:**

**a) not assume the availability of emergency central bank credit as a part of the FMI's liquidity plan; and**

ESAS does not assume the availability of emergency central bank credit as part of its liquidity planning. Payments settle strictly on a real-time gross basis using available balances. Any liquidity

facilities offered by the RBNZ to participants are part of the Bank's wider operating framework and are not considered emergency support for ESAS.

- b) **have a robust framework to manage liquidity risks for the FMI from its participants, settlement banks, nostro agents, custodian, liquidity providers, and other entities; and**

ESAS does not face liquidity risks arising from participants or third parties because it does not rely on them to meet settlement obligations. However, to ensure smooth settlement flows, ESAS maintains a RMF that includes real-time monitoring of liquidity distribution, participant balances, and payment queues. Operational controls support the timely detection of disruptions in liquidity flows (e.g., due to a participant operational outage), and the System Operator actively engages with affected participants to mitigate impacts.

- c) **have effective operational and analytical tools to identify, measure, and monitor the FMI's settlement and funding flows on an ongoing and timely basis, including its use of intraday liquidity.**

ESAS provides real-time visibility of participant balances, queued payments, and settlement activity. The System Operator monitors liquidity movement at system and participant levels to identify any anomalies or disruptions. Since ESAS does not assume liquidity risk, it does not maintain funding flows of its own. Nonetheless, operational monitoring ensures timely identification of issues affecting liquidity circulation among participants.

- 4) **Further to the requirements in clauses (1) and (3), an operator must obtain a high degree of confidence, through rigorous due diligence, that each provider of the FMI's minimum required qualifying liquid resources, whether a participant of the FMI or an external party, has sufficient information to understand and to manage the provider's associated liquidity risks, and that the provider has the capacity to perform its commitment as required. If relevant to assessing a provider's performance reliability with respect to a particular currency, a provider's potential access to credit from the central bank of issue may be taken into account.**

ESAS does not use external liquidity providers or maintain a pool of qualifying liquid resources. Therefore, due diligence on liquidity providers is not required.

#### Liquidity providers

- 5) **An operator must annually test the procedures for accessing liquid resources from the provider.**

Not applicable

ESAS does not access external liquid resources and therefore no testing is required.

- 6) **Stress testing**

Not applicable

ESAS does not maintain liquid resources to cover participant obligations and thus does not conduct liquidity stress testing.

### Procedures for settlement following participant default

- 7) Further to the requirements in clause (1)), an operator must establish explicit rules and have clear policies and procedures that enable the FMI to effect same-day and, where reasonable, intraday and multiday settlement of payment obligations on time, following any individual or combined default among its participants. These rules and procedures must:
- a) address unforeseen and potentially uncovered liquidity shortfalls and must aim to avoid unwinding, revoking, or delaying the same-day settlement of payment obligations; and
  - b) indicate the process to replenish any liquidity resources an operator may employ during a stress event, so that the FMI can continue to operate in a safe manner.

The requirement is not applicable to ESAS.

### Pure payment systems and securities settlement systems

- 8) An operator of a pure payment system or securities settlement system, including one employing a deferred net settlement mechanism, must maintain sufficient liquid resources for the FMI in all relevant currencies to effect same-day settlement, and where appropriate intraday or multiday settlement, of payment obligations with a high degree of confidence under a wide range of potential stress scenarios.

As ESAS does not assume liquidity risk as principal, the System Operator does not maintain liquid resources to cover payment obligations in stressed scenarios.

- 9) The scenarios in clause (8) must include, but not be limited to, the default of the participant and its affiliates that would generate the largest aggregate payment obligation in extreme, but reasonably foreseeable, market conditions.

As ESAS does not assume liquidity risk as principal, the System Operator does not maintain liquid resources to cover payment obligations in stressed scenarios.

### Central counterparties

- 10) Further to the requirements in clause (1), an operator of a central counterparty must maintain sufficient liquid resources in all relevant currencies for the central counterparty to:
- a) settle securities-related payments; and b) make required variation margin payments as per Standard 6; and c) meet other payment obligations on time with a high degree of confidence under a wide range of potential stress scenarios that must include, but not be limited to:
    - i) where the operator is an operator of an FMI engaging in simple central counterparty activities, and the FMI is not systemically important in multiple jurisdictions (including New Zealand), the default of the largest participant and its affiliates that would generate the largest aggregate payment obligation to the FMI in extreme, but reasonably foreseeable, market conditions; or

- ii) where the operator is an operator of an FMI engaging in complex central counterparty activities, or where the FMI is systemically important in multiple jurisdictions (including New Zealand), the default of the two largest participants and their affiliates that would generate the largest aggregate payment obligation to the FMI in extreme, but reasonably foreseeable, market conditions.

The requirement is not applicable. ESAS is not a CSP.

## Standard 8: Settlement Finality

### Assessment

#### ESAS Complies with Standard 8

- 1) **An operator must ensure that the FMI provides clear and certain final settlement, at a minimum by the end of the value date.**

The operator ensures that the ESAS provides clear and certain final settlement by defining that the settlement of a payment is final and irrevocable when the accounts of the paying and receiving Accountholders are simultaneously debited and credited. This process is clearly outlined in the ESAS Rules, specifically clause 5.

- 2) **Further to clause (1), an operator must ensure that:**
  - a) **The rules and procedures for ESAS explicitly state that settled payments made pursuant to Authorised Payment Instructions are irrevocable and may not be reversed once completed.**

ESAS is structured as an RTGS system. Payments are therefore settled individually on a real-time basis. Although settlements occur in real time, a payment submitted to the ESAS queue may remain there if the payer chooses not to settle the transaction (e.g. if the payer has set the status of the transaction to 'unauthorised') or has insufficient funds. Any payments that are not settled at the end of the relevant session are automatically cancelled from ESAS.) In ESAS, it is possible for an Accountholder to cancel payment instructions at any time before they are settled.

Under the ESAS Rules, an Accountholder is able to unilaterally revoke its outgoing RTGS payments at any time prior to settlement. ESAS cash transfers and payments sent via a feeder system can be revoked prior to settlement via the ESAS User Interface. However, a settled transaction cannot be cancelled or revoked.

An explanation has been added to the notice to settlement accountholders pursuant to clause 4.1 of ESAS Rules for clarity regarding revoking authorised payment instructions during and after gridlock buster operation. The Amendment to Settlement Submission Mechanism Notice had become effective on 9 May 2024.

## FMI Standard 9: Money Settlements

### Assessment

#### ESAS Complies with Standard 9

- 1) **An operator must conduct the FMI's money settlements in central bank money where reasonable and available, to avoid credit and liquidity risks. If central bank money is not available, or cannot be reasonably used, the operator must minimise and strictly control the credit and liquidity risk arising from the use of commercial bank money.**

Money settlements in ESAS are conducted in central bank money on a RTGS basis. The RBNZ, as the operator of ESAS, does not permit Accountholders' balances in ESAS to be overdrawn and, because ESAS is a designated FMI under the FMI Act, finality of settlement of ESAS transactions has statutory backing.

- 2) **Further to the requirements in clause (1) an operator must:**
  - a) **if central bank money is not used, ensure that the FMI conducts money settlements using a settlement asset with little or no credit or liquidity risk; and**

ESAS does not need to rely on commercial bank money, as all cash transactions are settled in central bank money. This eliminates any concern about credit or liquidity risk from commercial banks.

- b) **if an FMI settles in commercial bank money, it must monitor, manage, and limit the credit and liquidity risks for the FMI arising from the commercial settlement banks; and**

As all cash transactions in ESAS are settled in central bank money, there is no need to monitor or manage risks associated with commercial settlement banks.

- c) **establish and monitor adherence to strict criteria for commercial settlement banks that take account of, among other things, their regulation and supervision, creditworthiness, capitalisation, access to liquidity, and operational reliability; and**

Since ESAS uses central bank money there is no reliance on commercial banks for money settlements, meaning that criteria for commercial settlement banks are not required.

- d) **monitor and manage the concentration of credit and liquidity exposures to the FMI's commercial settlement banks; and**

Since ESAS uses central bank money, there are no credit and liquidity exposures to commercial settlement banks.

- e) **if an FMI conducts money settlements on the operator's or FMI's books, minimise and control credit and liquidity risks in the FMI; and**

Since ESAS settles transactions in central bank money, there are no additional credit or liquidity risks to be managed in the FMI itself. The System Operator does not take on any credit risk from the settlement of transactions between participants using ESAS.

- f) **ensure that contracts with settlement banks clearly state when transfers on the books of individual settlement banks are expected to occur, that transfers are**

final when effected, and that funds received are transferable as soon as possible, to enable the operator and the participants to manage credit and liquidity risks.

RBNZ does not use commercial bank money settlement agents in the operation of ESAS.

## FMI Standard 10: Physical Deliveries

### Assessment

Standard 10 is not applicable to ESAS

## FMI Standard 11: Central Securities Depositories

### Assessment

Standard 11 is not applicable to ESAS

## FMI Standard 12: Exchange-of-Value Settlement Systems

### Assessment

Standard 12 is not applicable to ESAS

## FMI Standard 13: Participant-Default Rules and Procedures

### Assessment

#### ESAS Complies with Standard 13

- 1) **An operator must have effective and clearly defined rules, policies, and procedures to manage a participant default. The rules, policies, and procedures must ensure that the operator can take timely action which will enable the FMI to continue to meet its obligations when facing potential losses and liquidity pressures.**

The RBNZ has the right, acting reasonably, to suspend or terminate the operation of the Accountholder's Settlement Account at any time, on notification to the Accountholder or as soon as practicable following such suspension or termination (clause 8.4).

Accountholders are obligated to notify the System Operator immediately upon the occurrence, or threatened occurrence, of a 'notifiable event' such as an inability to pay its debts or appointment of receiver or liquidator (clause 6). In addition, Accountholders must inform the System Operator of the steps (if any) the Accountholder is taking to ensure that it continues to have authority to issue Payment Instructions.

The default of an Accountholder in ESAS does not require the System Operator to meet obligations on its behalf; nor does it create additional obligations for non-defaulting Accountholders. Steps taken by the System Operator to manage an Accountholder's default are therefore largely procedural in nature.

The System Operator has established comprehensive rules, policies, and procedures designed to effectively manage Accountholder defaults within the ESAS framework. These rules and procedures enable the System Operator to take timely actions, ensuring the FMI can continue to meet its obligations even in the face of potential losses or liquidity pressures.

- 2) **Further to the requirements in clause (1), an operator must have default rules, policies, and procedures for the FMI that:**
  - a) **Enable the FMI to continue to meet the FMI and/or operator's obligations in the event of a participant default.**

The ESAS Rules specify that the default of an Accountholder does not create additional obligations for non-defaulting Accountholders. In the event of a default, the System Operator is equipped to implement decisive actions, such as suspending the Accountholder's Settlement Account, ensuring compliance with FMI obligations.

- b) **Address the replenishment of resources following a default where the FMI is exposed to credit or liquidity risk.**

The default of an Accountholder in ESAS does not require the System Operator to meet obligations on its behalf; nor does it create additional obligations for non-defaulting Accountholders. Steps taken by the System Operator to manage an Accountholder's default are therefore largely procedural in nature.

Accountholder default may result from insolvency events or a failure to comply with the requirements of the ESAS Rules. The System Operator has a documented process that sets out actions required to be taken by the RBNZ to manage Accountholder default.

Those actions are:

- Suspension: All debits and credits against the Accountholder are rejected.
- Stop Pay: All debits against the Accountholder are rejected.
- Stop Receive: All credits against the Accountholder are rejected.
- Exclusion: Removing the participant from ESAS.
- Remove from SBI agreement: All SBI transactions for the Accountholder are rejected.

The above actions would only be invoked in consultation with the RBNZ Supervision Department and PNZ. PNZ will be consulted, but the ultimate decision to take one of the actions set out above sits with the RBNZ. All the above actions require system-enforced second-level approval within ESAS. The four-eyes principle requires that the payment is processed by one privileged enabled user and then approved by different enabled privileged user.

- c) Be prepared to implement the FMI's rules, policies, and procedures for default, including any appropriate discretionary procedures provided for in the FMI rules.**

The System Operator is ready to execute the actions outlined in the ESAS Rules, including suspending all debits and credits against the Accountholder, stopping payments and receipts, and potentially excluding the participant from ESAS, ensuring adherence to established protocols.

- d) Publicly disclose key aspects of the FMI's rules, policies, and procedures for default.**

The ESAS Rules, including the rights of the System Operator and the obligations of Accountholders in the event of a default, are publicly accessible on the RBNZ's ESAS webpage, providing transparency and clarity for all stakeholders.

- e) Include participants and other stakeholders in the testing and review of the FMI's default rules, policies, and procedures, including any rules, policies, and procedures relating to close-out rights.**

The System Operator has enhanced its testing framework to incorporate structured stakeholder engagement. From 2026, default management testing will include scenario-based exercises involving relevant internal and external stakeholders, as appropriate, to test the operational readiness, clarity, and effectiveness of the procedures. These exercises will be conducted on a regular basis and are intended to ensure that default management arrangements remain robust, practical, and well understood by parties with a role in their execution.

- f) Conduct the testing and review referred to in clause (2)(e), following material changes to the rules, policies, and procedures, and on an annual basis ensure that the rules, policies, and procedures for participant default are practical and effective.**

The System Operator has documented processes for managing Accountholder defaults, including actions such as:

- Suspension: All debits and credits against the Accountholder are rejected.
- Stop Pay: All debits against the Accountholder are rejected.
- Stop Receive: All credits against the Accountholder are rejected.

- Exclusion: The participant is removed from ESAS.
- Remove from SBI Agreement: All SBI transactions for the Accountholder are rejected.

These actions will be implemented in consultation with the RBNZ Supervision Department and PNZ, with the ultimate decision-making authority resting with the RBNZ. Each action requires system-enforced second-level approval, adhering to the four-eyes principle, ensuring that all processes are conducted with diligence and care.

The processes are tested annually.

## FMI Standard 14: Segregation and Portability

### Assessment

Standard 14 is not applicable to ESAS.

## FMI Standard 15: General Business Risk

### Assessment

#### ESAS Complies with Standard 15

- 1) An operator must identify, monitor, and manage general business risk, including losses from poor execution of business strategy, negative cash flows, or unexpected and excessively large operating expenses.

The System Operator adopts a coordinated approach to identifying, assessing, and managing general business risks at both the enterprise and business levels. A critical part of this framework involves robust budgeting and accounting processes that enable continuous monitoring and control of operating expenses, including those incurred from the operation of ESAS.

- 2) An operator must hold sufficient liquid net assets funded by equity, such as common stock, disclosed reserves, and/or retained earnings, to cover potential general business losses so that the FMI can continue operations and essential services if those losses materialise.

ESAS is operated by the central bank, which means it benefits from a significant balance sheet that provides a robust financial foundation. Additionally, the business is self-funded, with all costs fully recovered from the Accountholders. This structure ensures that sufficient liquid net assets are available to cover potential general business losses, enabling the FMI to maintain operations and essential services even if those losses occur.

- 3) An operator (except where it is a central bank) must ensure that liquid net assets funded by equity are at all times sufficient to ensure a recovery or orderly wind-down of the FMI's operations and essential services. For the purposes of this clause, an operator may include equity held under international risk-based capital standards, where relevant and appropriate.

The System Operator is a central bank.

- 4) An operator must ensure that it maintains a viable recovery or orderly wind-down plan for the FMI (see Standard 17A: 'Contingency plans'), and ensure (except where the operator is a central bank) that it holds sufficient liquid net assets funded by equity to implement this plan.

The System Operator is a central bank.

- 5) An operator (except where it is a central bank) must hold liquid net assets funded by equity equal to at least six months of current operating expenses (see also requirement in Standard 17A: 'Contingency plans'). These assets must be held in addition to resources held to cover participant defaults or other risks covered under Standard 4: 'Credit Risk' and Standard 7: 'Liquidity Risk'.

The System Operator is a central bank.

- 6) An operator must ensure that a) assets held to cover general business risk are of high quality and sufficiently liquid so that the operator can meet the FMI's current and projected operating expenses under a range of scenarios, including in adverse market conditions; and

ESAS is operated by the central bank, which means it benefits from a significant balance sheet that provides a robust financial foundation. Additionally, the business is self-funded, with all costs fully recovered from the Accountholders. This structure ensures that sufficient liquid net assets are available to cover potential general business losses, enabling the FMI to maintain operations and essential services even if those losses occur; and

- c) it maintains a viable plan for raising additional equity should the operator's equity fall close to, or below, the amount needed, except where the operator is a central bank.

The System Operator is a central bank.

- 7) In relation to the plan referred to in clause (6)(b), an operator must: a) review the plan annually; and b) ensure that the outcome of the review is approved by the operator's board of directors.

The System Operator is a central bank.

## FMI Standard 16: Custody and Investment Risk

### Assessment

#### ESAS Complies with Standard 16

- 1) **An operator must safeguard assets held for FMI operations, including participant assets held for this purpose, and minimise the risk of loss on, and delay in access to, these assets. These assets must be invested in instruments with minimal credit, market, and liquidity risks.**

Securities provided to the RBNZ as collateral under repo are held within the NZClear system, which is a designated FMI regulated jointly by the RBNZ and the FMA. New Zealand Central Securities Depository (NZCSD), as a wholly owned subsidiary of the RBNZ, acts as the nominee to hold custody of NZClear Participants' securities. The governance structure ensures that these assets are safeguarded effectively, minimising risks of loss and delays in access. However, it is important to note that the ESAS does not engage in investment activities, so the specific investment strategy requirement is not applicable in this context.

- 2) **Further to the requirements in clause (1), an operator must:**
  - a) **Ensure that assets described in clause (1) are held by custodians with robust accounting practices, safekeeping procedures, and internal systems that fully protect these assets, and who comply with all legal and regulatory obligations.**

The RBNZ and NZCSD do not utilise third-party custodians; instead, they directly hold the securities deposited by NZClear Participants. As a statutory body governed by the Reserve Bank Act, NZCSD adheres to stringent legal and regulatory obligations, and its operations are subject to regular audits, including quarterly external audits and annual audits of internal controls conducted by PwC.

- b) **Have prompt access to the assets described in clause (1).**

As the System Operator is owned by the central bank, it has immediate access to the assets held within the NZClear system whenever necessary, ensuring that any operational requirements can be met without delay.

- c) **Evaluate its exposures to its custodians, considering the full scope of its relationships with each custodian.**

Given that the RBNZ and NZCSD do not engage third-party custodians for asset holding, this evaluation is not applicable. The direct management of securities allows for a comprehensive understanding of the exposures without intermediary custodial relationships.

- d) **Have an investment strategy that is consistent with its overall risk management strategy and fully disclosed to the FMI's participants.**

Since the ESAS does not invest funds, the requirement for an investment strategy is not relevant in this context. However, the operations of NZClear and the safeguarding of assets are aligned with a broader risk management strategy that prioritises the security and accessibility of participant assets.

- 3) For the purposes of clause 2(d), the investments must be secured by, or be claims on, high-quality debtors. These investments must allow for quick liquidation with minimal adverse price effect.

Since the ESAS does not engage in investment activities, this clause is not applicable. However, the collateral management practices in place ensure that the securities held are of high quality, maintaining the integrity of the FMI's operations.

## FMI Standard 17: Operational Risk

### Assessment

#### ESAS Complies with Standard 17

- 1) **An operator must:**
  - a) **Identify the reasonably foreseeable sources of operational risk for the FMI, both internal and external.**

The RBNZ has established a comprehensive RMF that outlines policies, guidance, and practices aimed at systematically identifying, assessing, and managing operational risks. As the System Operator of ESAS, the FMI&S Directorate focuses primarily on operational risks, which are identified through a thorough assessment of system processes to uncover potential vulnerabilities. This includes evaluating both internal processes and external threats that could impact the functioning of ESAS.

The FMI&S Directorate identifies operational risks by considering various factors, such as system performance, security vulnerabilities, and external risks from market disruptions or technological failures. This proactive approach ensures that the RBNZ remains aware of potential operational risk sources and can respond effectively.

- b) **Mitigate their impact through the use of appropriate policies, procedures, and internal systems on an ongoing basis.**

To mitigate identified operational risks, FMI&S has developed and continuously improves its internal controls, systems, and procedures in alignment with the RMF. Key elements of operational risk management for ESAS include:

- **Daily Reconciliations:** Regular completion and review of reconciliations to ensure accurate and timely processing of transactions.
- **Compliance with Policies:** Adherence to RBNZ policies governing segregation of duties, security measures, and technology risk, including change control processes.
- **SLAs:** Monitoring third-party SLAs to ensure compliance with agreed-upon contractual requirements.
- **BCPs:** Maintenance and testing of robust BCPs to ensure resilience against disruptions, including natural disasters.

The RBNZ also employs an LFF policy, which mandates the escalation of incidents and near misses, analysis of root causes, and implementation of remedial actions to prevent recurrence.

Specific control objectives are documented in the 3402 Report on Controls over the ESAS System, covering key areas such as:

- **Security Management:** Ensuring that security management procedures are robust, including controls for managing internal and external network security risks and access privileges.
- **Change Control:** Establishing procedures for testing and approving changes before migrating them into production, with emergency changes being appropriately authorised.

- Problem Management: Timely identification and resolution of operational problems to minimise disruptions.
- Backup and Recovery: Implementing processes for ensuring data integrity and enabling timely recovery of business operations across primary and secondary sites.

The System Operator maintains multiple versions of the ESAS application and associated infrastructure, synchronised in real-time, to ensure continuous service in case of system failure or other emergencies. With staff located in both Auckland and Wellington, the RBNZ is well prepared to provide ongoing business support, ensuring operational continuity regardless of potential disruptions.

**2) The RBNZ has implemented a robust framework to ensure that the internal systems supporting ESAS are designed with a high degree of security and operational reliability. Key elements of this framework include:**

The RBNZ has established comprehensive security management procedures that are designed to protect against both internal and external threats. This includes stringent access controls to ensure that only authorised users have the necessary privileges within the system, and the implementation of environmental and physical security measures over computing equipment.

The FMI&S Directorate is committed to maintaining operational reliability through regular reviews and updates of its internal systems. Daily reconciliations and adherence to RBNZ policies on segregation of duties and technology risk help to minimise operational errors and enhance system integrity.

To ensure the continuity of essential services, the System Operator maintains multiple versions of the ESAS application and its associated infrastructure. This architecture allows for real-time data synchronisation, enabling uninterrupted service even in the event of a system failure, natural disaster, or other emergencies.

A comprehensive BCP is in place, which includes regular testing and updates to ensure readiness in the face of disruptions. The RBNZ has protocols for backup and recovery that guarantee data integrity across primary and secondary sites, facilitating timely recovery of operations.

The RBNZ employs a LFF policy that mandates thorough analysis of incidents and 'near misses'. This process ensures that root causes are identified, and necessary remedial actions are implemented to enhance system resilience and prevent recurrence.

**3) Further to the requirements in clauses (1) and (2), an operator must: a) Implement and maintain a robust operational risk management framework for the FMI, with appropriate policies, procedures, and internal systems to identify and manage operational risks.**

The RBNZ has established a RMF designed to effectively identify and manage operational risks associated with ESAS. The FMI&S Directorate is responsible for the management of operational risk, employing risk matrices to assess the system and processes for potential vulnerabilities. These matrices are reviewed quarterly to ensure that any emerging risks are promptly addressed. To mitigate material risks, FMI&S continuously develops and enhances internal controls, systems, and procedures.

- a) **Ensure that the operational RMF, as well as compliance with such framework, is assessed by way of an external assurance engagement, undertaken in accordance with applicable auditing and assurance standards, by a qualified auditor:**
  - i) **at least every two years; and**
  - ii) **subject to clause (4), whenever a material incident or material outage occurs.**

The RBNZ's operational RMF is subject to independent assessments through 3150 engagements conducted by PwC, who act as the external auditors on behalf of the Auditor General. PwC conducts audits of the internal controls related to ESAS, and their findings are reported to the Governor. The Audit Committee of the Board oversees these audits, ensuring that both internal and external audit functions are appropriately managed. Audit reports from PwC are available upon request to all participants, ensuring transparency and accountability.

Through these structured processes, the RBNZ maintains a robust operational RMF that is regularly assessed and continuously improved to safeguard the integrity and reliability of ESAS.

- c) **Provide any report from an external assurance engagement to the regulator at the regulator's request; and**

The System Operator will provide any external assurance engagement reports to the regulator upon request, ensuring compliance with regulatory requirements.

- d) **Ensure the board of directors of the operator clearly defines the roles and responsibilities for addressing the FMI's operational risk and endorses the FMI's operational risk management framework.**

The RBNZ's Board of Directors plays a crucial role in overseeing the management of operational risk for ESAS. The Board is responsible for clearly defining roles and responsibilities related to operational risk, ensuring that these are well-documented and communicated across the organisation. The Board endorses the operational RMF, which is implemented and managed by the FMI&S. This framework is designed to effectively identify and manage operational risks, ensuring that the RBNZ can achieve its objectives while maintaining the integrity of ESAS.

- e) **Ensure that policies, procedures, and internal systems are reviewed and tested annually and after substantive changes to those policies, procedures, or internal systems.**

The RBNZ is committed to maintaining robust internal controls and policies for ESAS. To ensure their effectiveness, these policies, procedures, and internal systems are reviewed and tested on an annual basis at a minimum. Additionally, any substantive changes to these policies or internal systems trigger a review process to assess their adequacy and effectiveness. The Risk Compliance and Audit Directorate is responsible for monitoring compliance with the operational RMF, while internal audits conducted by the RBNZ's Risk Compliance and Audit Department further ensure that the framework remains effective and aligned with best practices.

Internal controls related to ESAS are audited by PwC, who provide independent assurance regarding their adequacy. PwC's audit reports are addressed to the Governor and reviewed by the Board's Audit Committee, which includes external auditors, RBNZ governors, and management. These reports are made available to all participants upon request, ensuring transparency and accountability in the operational risk management processes.

**f) Have clearly defined operational reliability objectives for the FMI, with policies and procedures in place that are designed to achieve those objectives.**

ESAS is designed to achieve high availability and resiliency, with its infrastructure and applications housed in two geographically separate data centres. This setup supports the system's operational reliability objectives, which are clearly defined and monitored through a set of KPIs.

The primary operational reliability objective for ESAS is to maintain a targeted system availability of 99.9 percent. Performance against this benchmark is regularly reported and monitored, with actual availability statistics included in both the RBNZ Annual Report and the ESAS Annual Report, which are accessible on the RBNZ's website.

To support this primary KPI, several additional KPIs are in place to ensure that the underlying systems can collectively meet operational objectives. For example, fault-handling regimes are established with the two key service providers, NEXI and Datacom, to address faults, outages, and issues in line with contractual obligations. This proactive management minimises downtime, thereby safeguarding the 99.9 percent availability target. Fault-handling performance is reviewed both individually, upon occurrence, and collectively in monthly performance reports.

In addition to availability KPIs, performance and throughput metrics are validated during the software release process to ensure the system can process the required volumes within specified timeframes. Continuous monitoring is conducted throughout the day, supported by a help desk to assist users with inquiries. Any problems, incidents, or near misses are reported to senior management for timely decision-making and action.

To further enhance operational reliability, the following measures and KPIs are implemented as early warning mechanisms for operational deficiencies:

- Continuous monitoring of the system during operational hours, alongside an incident management regime.
- Monthly assessments of network reliability and service-level compliance.
- Ongoing external audits of key operational processes, change control processes, and network access changes.
- Regular forums with key service providers to monitor and manage their performance effectively.

These structured policies and procedures collectively contribute to achieving and maintaining the operational reliability objectives of ESAS.

**g) Ensure that the FMI has the capacity adequate to handle increasing stress volumes and to achieve its service-level objectives.**

The infrastructure and applications of ESAS, and supporting systems are governed by two key contracts: the Master Services Agreement with Datacom for infrastructure services, and the Software Licensing and Services Agreement with NEXI for application software. Both agreements establish clear obligations related to contract performance and governance, ensuring effective management of all operational aspects.

To maintain adequate capacity and meet service-level objectives, the System Operator engages in a structured management approach with both vendors:

For the infrastructure service provider (Datacom):

- Regular meetings are held to manage the work program and address any issues that arise.
- System performance, including capacity assessments, is reviewed in these meetings to ensure alignment with operational goals.
- Ongoing reviews of contract performance and system roadmaps are conducted to anticipate future needs and developments.
- Weekly and monthly meetings involve collaboration with the Security Operations Centre (SOC) team and infrastructure support provider architects to discuss cyber security and vulnerability management.

For the application software provider (NEXI):

Regular meetings are scheduled to review software developments and releases, prioritising application performance and addressing any active issues.

- NEXI's performance against the contract is assessed, along with discussions on the development roadmap and any key outages.
- Strategic initiatives and developments are reviewed regularly to ensure alignment with operational requirements.

Both contracts and their governance obligations are audited under the 3402 Audit Report and are also aligned with the SWIFT CSP control framework.

In the event that monitoring systems indicate potential capacity issues, the System Operator proactively engages with Datacom and NEXI to analyse the situation and develop an appropriate response plan. This ensures that any emerging challenges are addressed swiftly, maintaining the predetermined buffers of the system and enabling the FMI to continue meeting its service-level objectives even under increasing stress volumes.

**h) Ensure that the FMI has comprehensive physical and information security policies that address all potential vulnerabilities and threats.**

The RBNZ has established a comprehensive suite of policies that govern both physical and information security for its Financial Market Infrastructures (FMIs). These policies encompass several critical areas, including:

- Information disclosure
- Records management
- Access restrictions (both records and physical)
- Information systems security
- Building security
- Incident reporting management

The architecture and operation of the payment systems prioritise security, aligning with SWIFT's CSP and the Government Communications Security Bureau's (GCSB) New Zealand Information Security Manual (NZISM), which adheres closely to ISO standards. This approach is consistent with the guidelines set forth by the Bank for International Settlements (BIS) and the International Organization of Securities Commissions (IOSCO), as well as the RBNZ's draft Guidance on Cyber Resilience.

A comprehensive cyber support program is in place, utilising a SOC that operates 24/7 to monitor and manage security within the payments domain. The SOC actively manages all systems and access activities, overseeing security monitoring, vulnerability management, and scanning of the payments systems.

Collaboration is a key element of the security strategy, with the SOC working closely with Datacom support staff, the RBNZ payments technical team, the RBNZ Cyber Team, and national cyber agencies. Weekly meetings are convened to address current security issues and to manage vulnerabilities based on an agreed RMF, which evaluates risks according to asset value and the Common Vulnerability Scoring System (CVSS) risk rating applicable in the payments context. Any identified risks are managed within the RBNZ ERMF. Additionally, a monthly SOC review assesses the overall security posture of ESAS and the broader cyber risk landscape.

The RBNZ has also implemented a comprehensive incident management and recovery plan for cyber incidents, covering both ESAS and its supporting infrastructure. This plan integrates with the corporate incident management strategy where appropriate. Regular penetration testing is conducted on the systems, coordinated by the RBNZ Cyber Team and executed by an external third party. Furthermore, a SWIFT CSP assessment is performed at least annually, with independent audits initiated from 2021 onward.

- i) **Identify and manage the risks that key participants, other FMIs, and service and utility providers might pose to the FMI's operations. In addition, an operator must identify and manage the risks the operations of the FMI might pose to other FMIs.**

The System Operator acknowledges system failure as a critical enterprise risk and has designed the ESAS for high availability and resiliency. This design includes multiple physical computer systems, with two instances located in each of two geographically separate locations, aimed at mitigating the risk of processing disruptions.

ESAS operates in an integrated manner with the RBNZ's NZClear System, facilitating DVP Model 1 gross settlement of both funds and securities. The simultaneous and irrevocable settlement of securities and associated cash payments underscores the importance of a holistic approach to risk management, which the RBNZ applies, given that both ESAS and NZClear are operated by the same entity. This integration allows for comprehensive oversight of interdependencies and risk considerations between the two systems.

Settlement instructions to and from ESAS may be sent over the SWIFT network, which involves some administration by the System Operator while largely relying on the SWIFT organisation for overall system operation. The telecommunications network infrastructure supporting ESAS is managed by Datacom, which also provides software support and operational services. The System Operator ensures effective management of third-party services through service contracts and related SLAs, conducting monthly risk assessments and performance reviews, monitoring problem management reports, and overseeing relevant project steering committees.

The telecommunications infrastructure on which ESAS operates is provided by Spark New Zealand Limited, supplemented by a backup network service from a second provider to ensure operational continuity.

Major ESAS Accountholders, primarily registered banks, are required to attest to the RBNZ regarding the suitability of their BCPs. Accountholders must notify the System Operator of any

processing issues impacting ESAS, and conversely, the Bank promptly informs accountholders if its systems are not functioning as required.

Additionally, we monitor systemically important participants based on their transaction volumes and values, analysing trends for any emerging risks. With the new ESAS Access Policy, we will implement an ongoing compliance plan, which will include regular due diligence and annual attestations. We also oversee how systemically important participants manage risks arising from their clients. For further details, please refer to Standard 19 regarding tiered participation and its risk management approach.

To manage the risks that ESAS operations may pose to other FMIs, the System Operator actively manages the resilience of ESAS and its interfaces. This includes ongoing monitoring of all interfaces, robust fault management processes, and alternative backup processing options, ensuring that potential negative impacts are effectively mitigated.

- 4) **Clause (3)(b)(ii) does not apply if, in the opinion of the operator, it is not reasonably practicable to seek an external assessment following the material incident or material outage.**

The requirement will be applied on an ad hoc basis depending on the incident,

- 5) **If clause (4) applies, the operator must provide reasons for its opinion to the regulator as soon as possible following a material**

The requirement will be applied on an ad hoc basis depending on the incident,

## FMI Standard 17A: Contingency Plans

### Assessment

#### ESAS Complies with Standard 17A

- 1) **An operator must ensure that the FMI contingency plans for the designated FMI: a) Identify the FMI's essential services.**

The BCP for ESAS clearly identifies the essential services provided by the FMI. ESAS is tasked with facilitating real-time irrevocable settlements on a gross basis, ensuring the safe and efficient electronic settlement of payments between Accountholders. These settlements are critical to the functioning of the financial system, as they provide the backbone for high-value and time-sensitive transactions.

Furthermore, the BCP acknowledges the role of PNZ, which administers the HVCS, CLS, and SBI processes. These services are essential for maintaining liquidity, minimising settlement risk, and ensuring the smooth operation of New Zealand's financial markets.

The contingency plans ensure that all essential services, including the integration with PNZ, CLS, and SBI, are protected and can continue to operate or be restored promptly in the event of a disruption. The identification of these core services allows the operator to prioritise recovery efforts and maintain the integrity of critical financial operations during emergencies.

- b) Identify scenarios that pose a significant risk of disrupting the FMI's activities, including events that could cause widespread or major disruption.**

The contingency plans for ESAS identify several scenarios that could significantly disrupt its activities. Operational failures, including those resulting from natural disasters, are specifically addressed in the BCP. These disruptions could stem from events like earthquakes, flooding, or other natural disasters that may affect the infrastructure or data centres supporting the ESAS system. To mitigate these risks, ESAS has a robust infrastructure with geographically separated data centres to ensure resilience and continuity of operations.

Non-financial risks, such as technological failures or cyber security threats, are also recognised as significant. These risks, which may cause widespread disruption, are mitigated through continuous monitoring, regular audits, and backup systems designed to maintain real-time settlements even during adverse conditions.

The BCP captures potential failures of CSPs such as Datacom, NEXI, and SWIFT, which are vital to the operational continuity of ESAS. These providers are considered integral to the system's functionality, and any disruption in their services is managed within the BCP. However, since ESAS is owned by the RBNZ, it has the ability to provide liquidity support in case of disruptions, ensuring continuous operations without posing liquidity risks to the central bank.

Credit losses are also not a concern since ESAS ensures adequate credit availability before any transfer occurs, and no overdrafts are allowed. This means that settlement activity does not expose ESAS to liquidity risks.

Additionally, the BCP identifies PNZ as the administrator of critical linked FMIs, including HVCS, SBI, and CLS. However, the failure of PNZ is considered extremely unlikely, given that it is owned by eight registered banks. Therefore, its failure does not pose a direct risk to the operation of ESAS, and it is not included as a scenario in the BCP.

The BCP also captures other foreseeable scenarios, including operational disruptions such as an office building becoming unsuitable for work or an IT outage. In addition, the ESAS BCP outlines the application of the loss allocation FMI rule in the event of a participant default, ensuring continuity of operations under stress.

Internal and external threats have been carefully considered in developing the BCP scenarios. Furthermore, linked FMIs, such as PNZ, which administers the HVCS, SBI, and CLS, are monitored. However, the failure of PNZ is considered extremely unlikely, as it is owned by eight registered banks. Consequently, this scenario is not included in the BCP, as its failure would not directly impact the operation of ESAS.

- c) Identify scenarios that have a significant risk of placing the operator under financial stress and could affect the ability of the FMI to continue to provide essential services.**

For ESAS, financial stress due to insolvency is not applicable since the operator is a central bank, the RBNZ. As a central bank, the RBNZ has an inherent ability to supply liquidity as needed to support the continuity of operations. This ensures that scenarios where financial stress impacts essential services are highly unlikely.

- d) Set out the interaction between the FMI contingency plans and the FMI's rules.**

While the contingency plans should be standalone documents, they must also be operationalised through specific provisions in the FMI's rules where necessary. For instance, in cases where a participant default creates losses, the FMI's rules should provide for the allocation of those losses among participants. However, this is not currently required for ESAS.

'In the event of an Accountholder default, the System Operator would not be exposed to a loss.' This is because payments in ESAS are settled using the Accountholder's ESAS accounts, which cannot be overdrawn. Furthermore, the System Operator does not guarantee any transactions submitted for settlement in ESAS. Therefore, the system rules do not currently necessitate loss allocation provisions in the event of a participant default, as ESAS's design ensures there is no risk of financial loss to the System Operator.

This structure ensures that ESAS remains resilient and risk-free from participant defaults, aligning with both the contingency plans and the system's rules.

- e) Set out what constitutes an acceptable degree of recovery following a scenario described in (b) and within what timeframes, and if recovery within two hours is not possible, the reasons why.**

The BCP defines the acceptable degree of recovery as:

- All ESAS settlements are being completed by the end of the day.
- All high-priority helpdesk queries are being responded to within two hours.

The BCP provides procedures to ensure recovery within the two-hour time frame. This includes real-time monitoring of system activity and the activation of the contingency plan for missing

transaction references via SWIFT audit steps. If a significant disruption occurs, the secondary sites (Hamilton and Auckland data centres) are designed to restore services within two hours.

However, in cases such as a major cyber incident or a failure of both New Zealand data centres, recovery within two hours may not be possible. The BCP acknowledges this scenario and highlights the activation of the RTGS Extreme Contingency Solution (RECS) in Milan as a backup measure.

**f) Set out how the FMI, following a scenario described in (b), will complete settlement by the end of the day.**

The BCP outlines that all ESAS settlement processes are structured to ensure completion by the end of the day. Key steps include:

- Data backup and reconciliation through RECS, which allows for the restoration of transaction data within the two-hour window.
- Use of geographically separate Tier 3 data centres in Hamilton and Auckland to provide robust infrastructure redundancy.
- RBNZ staff are based across Auckland and Wellington and can work remotely to ensure continued operations in the event of an office disruption.

If both data centres were to fail, the RECS can be activated to ensure continuity of services. However, the BCP notes that it cannot fully guarantee settlement completion by the end of the day in cases of major cyber incidents or a dual data centre failure.

This structured approach minimises downtime while ensuring critical settlement functions are prioritised for rapid recovery.

**g) Set out policies and procedures, including management procedures, designed to respond to identified operational and financial risk events.**

ESAS maintains a comprehensive BCP that sets out the policies, procedures, and management arrangements required to respond effectively to operational and financial risk events. The BCP forms a core component of the ESAS operational resilience framework and establishes clear expectations for restoring critical services following a disruption. It defines a recovery time objective (RTO) that specifies the maximum acceptable outage period and guides the operator's approach to continuity planning. In most scenarios, the objective is to restore critical settlement services within two hours, ensuring that key payment flows remain uninterrupted.

The BCP also defines the acceptable degree of recovery following an incident. This includes completing all ESAS settlements by the end of day and responding to high-priority service requests within required timeframes. These thresholds help ensure continuity of essential functions and maintain confidence in the system's reliability.

Operational risk procedures are documented for a wide range of scenarios, including IT system failures, data centre outages, network disruptions, and cyber incidents. ESAS supports these procedures through geographically diverse infrastructure, with secondary operational sites located in Hamilton and Auckland and an RECS hosted offshore in Milan to safeguard the system in severe or extreme situations.

Financial-risk considerations are incorporated into the BCP, although they are limited due to the central-bank nature of ESAS. As the operator, the RBNZ does not face credit or liquidity exposure

from settlement activity and, therefore, does not rely on loss-allocation procedures. The ability of the central bank to provide liquidity in times of stress further reduces financial-risk vulnerability.

The BCP also sets out clear management and governance procedures for incident response, including escalation routes, decision-making responsibilities, and communication expectations. Regular testing exercises, scenario walkthroughs, and audits validate the effectiveness of these arrangements and support continuous improvement. Collectively, these policies and procedures ensure ESAS is able to respond promptly and effectively to operational and financial risk events.

- h) **Include a set of financial recovery tools that are reliable, timely, effective, legally robust, and enforceable, taking into account the nature of the FMI's operations.**

The financial recovery framework of ESAS is structured around its central bank ownership and robust operational design, minimising credit and liquidity risks. Key aspects include:

**Credit Risk Mitigation:** Credit losses are avoided in ESAS as no overdrafts are permitted. Settlement activities ensure that all transactions are fully funded before transfer occurs, eliminating exposure to credit risks.

**Liquidity Support:** As ESAS is owned by the RBNZ, the system has an inherent ability to supply liquidity to maintain operations, ensuring the continuity of services in the event of financial stress or disruptions. This includes providing liquidity to cover any potential shortfalls.

**Participant Default** In the event of a participant default, the BCP specifies that the defaulting participant can be either expelled or suspended. These measures are legally enforceable under ESAS rules, ensuring timely and effective resolution of financial risk scenarios.

**Legally Robust and Enforceable Tools:** The recovery tools in place are supported by legally binding agreements with participants, ensuring that measures like participant suspension or expulsion can be executed without delay. The system's rules and frameworks are regularly reviewed to ensure they remain legally robust and enforceable.

These financial recovery tools are designed to be reliable, timely, and effective, ensuring ESAS remains resilient in the face of financial risks while maintaining essential service continuity.

- i) **Include procedures to allow for a change to the operator of the relevant FMI (except where the operator is a central bank).**

The requirement is not applicable to ESAS as it is operated by the central bank.

- j) **Set out how an FMI would be wound down in an orderly manner if essential services cannot be provided on an ongoing basis and an alternative operator is not available (except where the operator is a central bank).**

The requirement is not applicable to ESAS as it is operated by the central bank.

- k) **Set out arrangements for testing and reviewing the contingency plans on at least an annual basis.**

The system's contingency plans are still subjected to regular and rigorous review and testing:

- Annual Testing: The ESAS contingency plans are tested at least once a year to ensure they remain effective in addressing potential disruptions. These tests assess the system's operational resilience, identify gaps, and confirm that recovery objectives, such as the RTO, are achievable.

- **Joined-Up Testing with NZClear:** Given the close operational link between ESAS and NZClear, joint testing is conducted to ensure that both systems can continue to function seamlessly under stress scenarios. This ensures that DVP settlement processes are preserved, and the contingency plans for both FMI are aligned.

This annual review process ensures that any emerging risks or operational changes are accounted for, keeping the contingency plans up to date and reliable.

**l) Set out the persons responsible for maintaining, activating, and implementing the plans.**

For the ESAS BCP, the Director of FMI&S holds the responsibility for ensuring that the plan is regularly assessed and updated. In the event that activation is necessary, the plan can be initiated by either the Director of FMI&S or the Assistant Governor of Economics, Financial Markets, and Banking.

The Incident Response Plan outlines that regular assessments and updates are crucial, with the individual responsible yet to be specified. However, the activation of this plan falls under the purview of the Incident Response Team (IRT) Chair.

Should a situation arise requiring activation, the Major Incident Manager will initiate the IT Major Incident Management process. The Major Incident Plan was updated in April 2023.

The Security Incident Management Playbook also designates responsibilities for maintaining and activating the plan. The Manager of Cyber Security Operations is responsible for maintaining this Playbook, and the Chief Information Security Officer (CISO) is the accountable party.

Review processes are integral to the BCP framework. The ESAS BCP is reviewed twice a year, while the Incident Response Plan is assessed at least annually by the Principal Resilience Adviser.

Testing protocols are also established, particularly for the ESAS BCP, which includes regular testing of data centres and failover procedures.

The Incident Response Protocol (IRP) was last updated in October 2024, and the Principal Resilience Adviser, Risk & Compliance is responsible for updating it. Meanwhile, the IT Major Incident Management Plan is tested approximately three times a year, including elements of the Security Incident Management Playbook.

Training initiatives play a vital role in ensuring that personnel are equipped for their responsibilities. Primarily, training is delivered through participation in exercises, with ongoing efforts to ensure all involved individuals receive adequate training and support throughout their roles.

**m) Set out the procedure for activating the FMI contingency plans.**

Firstly, the ESAS BCP outlines the steps for activating contingency measures specifically tailored to events that disrupt ESAS operations. This plan includes comprehensive communication strategies to ensure that all relevant stakeholders are informed and engaged throughout the activation process.

In addition to the ESAS BCP, the RBNZ IRP is critical for addressing physical attacks and natural disasters that could impact RBNZ operations. This protocol is informed by Security Alert Levels and an Escalation Plan, providing a framework for assessing the severity of incidents and guiding the appropriate response.

For incidents related to disaster recovery (DR) and cyber security events, the Major Incident Response Plan (MARP) is implemented. This plan serves as a crucial mechanism for managing incidents that could jeopardise the integrity of the FMI's operations.

The ESAS BCP also includes provisions for notifying relevant regulators, such as the RBNZ Prudential Supervision Regulators and the Financial Markets Authority Regulators, ensuring compliance with oversight requirements during an incident.

## FMI Standard 17B: Critical Service Providers

### Assessment

#### ESAS Complies with Standard 17B

- 1) **An operator must take all reasonable steps to ensure the continued provision of critical services by managing the relationship with its critical service providers).**

ESAS relies on three key CSPs to support its operations:

1. **NEXI:** Responsible for software development, ensuring the system's functionality and regular updates.
2. **Datacom:** Provides hardware support, ensuring the reliability of our physical infrastructure and technical equipment.
3. **SWIFT:** Manages messaging and network services, ensuring secure communication between ESAS participants.

As the System Operator, we implement several critical measures to manage our relationships with CSPs effectively, ensuring the uninterrupted provision of essential services:

1. **Clear Contractual Framework:** We establish comprehensive MSAs and SLAs that outline the obligations and performance expectations of our CSPs. These agreements serve as the foundation for our collaborative relationships, ensuring clarity and accountability.
2. **Structured Governance and Oversight:** The System Operator conducts regular governance meetings with our CSPs to facilitate open dialogue and collaboration. These meetings are designed to review performance, address any emerging issues, and align on operational reliability and strategic objectives.
3. **Performance Monitoring and Reporting:** The System Operator actively monitors the performance of CSPs against established KPIs. They generate monthly performance reports to evaluate compliance with the agreed-upon service levels, allowing us to identify any deviations early and take corrective action as needed.
4. **Proactive Risk Management:** The System Operator adopts a proactive approach to risk management by identifying potential risks associated with service delivery. This includes developing contingency plans that outline the actions required to maintain critical services during disruptions, thereby enhancing our operational resilience.
5. **Continuous Improvement and Feedback:** The System Operator have implemented a feedback mechanism that facilitates ongoing assessment of service provider performance. By gathering input from stakeholders and conducting regular reviews, we ensure that our CSPs remain aligned with our operational needs and strategic goals.
6. **Stakeholder Engagement and Communication:** The System Operator prioritises building strong relationships with all relevant stakeholders. By keeping stakeholders informed and engaged through regular updates and discussions, we foster a collaborative environment that enhances the overall effectiveness of our service delivery.

Through these comprehensive strategies, we ensure that our relationships with CSPs are effectively managed, thereby safeguarding the continuity and reliability of the critical services we provide.

2) Further to the requirements in clause (1), an operator must take reasonable steps to ensure that a FMI's critical service provider: a) identifies and manages relevant operational and financial risks to the provider's ability to provide critical services to the FMI. This includes ensuring that:

i) the provider implements and maintains appropriate policies and procedures for the continued provision of critical services;

Each CSP implements and maintains policies and procedures designed to ensure the uninterrupted delivery of critical services to ESAS. These policies are regularly reviewed and updated to align with best practices such as ISO 27001 (Information Security) and ISO 22301 (Business Continuity). By adhering to internationally recognised standards, CSPs ensure their processes for access control, data protection, incident response, and DR remain robust and capable of sustaining ongoing operations.

ii) the provider has effective risk management processes;

CSPs have comprehensive RMFs in place that guide the identification, assessment, and mitigation of risks. These frameworks are aligned with industry standards such as ISO 31000 (Risk Management) and include processes for regular risk reviews. High-risk areas are prioritised, with monthly reviews conducted where necessary. RMFs are designed to address not only operational risks but also financial risks, ensuring the CSPs' ability to meet their obligations even under adverse conditions.

FMI&S documents all CSP risks in dedicated CSP risk registers using the enterprise risk methodology. Each risk is linked to mapped controls and assessed for residual exposure based on likelihood and impact. These registers are reviewed quarterly at the FMI&S Risk Forum, where second-line functions challenge the completeness of risk identification, the strength of controls, and the validity of risk ratings.

Where CSP risk profiles change — such as through technology upgrades, resource constraints, market events, or assurance findings — FMI&S updates CSP assessments and adjusts monitoring intensity. This ensures a continuous and forward-looking view of CSP risk.

iii) the provider's critical services are available, reliable, and resilient;

The CSPs ensure that their services remain highly available, reliable, and resilient by continuously improving their infrastructure and systems. They have comprehensive BCPs and disaster recovery plans (DRPs), which are regularly tested and updated to ensure readiness for any disruption. By aligning their continuity and recovery frameworks with standards like ISO 22301:2019, CSPs ensure they can promptly resume critical services in the event of system outages, safeguarding the operational stability of ESAS.

FMI&S receives monthly SLA performance reports and incident summaries, conducts structured RCA discussions, and reviews performance metrics across availability, reliability, and response times. Resilience issues identified during incidents, assurance reviews, or due diligence are incorporated into CSP risk mitigation plans.

iv) the provider has robust business continuity management plans and disaster recovery plans to support the timely resumption of its critical services in the event of an outage, so that the provider fulfils the terms of its agreement with the operator or FMI, as appropriate;

All CSPs maintain comprehensive BCPs and DRPs that are rigorously tested to ensure minimal downtime and quick recovery in the event of an incident. These plans detail procedures for restoring services, with pre-defined RTOs and recovery point objectives (RPOs) that align with the agreed service levels in their contracts with ESAS. By regularly reviewing and enhancing these plans, CSPs ensure that they are well-prepared to handle outages and maintain service continuity.

All CSPs supporting ESAS are required to maintain documented and tested business continuity and disaster-recovery plans that align with the recovery time targets specified in ESAS contracts and operational requirements. Datacom conducts annual DR failover testing, resilience rehearsals, and data centre readiness reviews. NEXI executes application-level recovery testing tied to ESAS's release cycles. SWIFT maintains a continuity model that is tested globally and that covers multiple regions and data centres.

**b) devotes sufficient resources to ensuring the confidentiality and integrity of information relating to the operator and the FMI;**

CSPs devote substantial resources to maintaining the confidentiality and integrity of information related to ESAS and its operations. They implement stringent data protection measures such as encryption, access control, and incident monitoring in line with ISO 27001 standards. Additionally, they regularly train personnel on data security protocols and conduct penetration testing to ensure their defences remain effective. These efforts are supported by continuous investments in cyber security infrastructure to protect against emerging threats.

**c) has in place robust methods to plan for the entire lifecycle of the use of its technologies and the selection of technological standards;**

CSPs apply rigorous technology lifecycle management processes to ensure that the systems supporting ESAS remain current and capable of meeting operational demands. This includes regular technology assessments and updates to align with evolving standards and industry innovations. Each CSP follows a structured approach to technology planning, ensuring that both current and future operational needs are addressed, minimising the risk of obsolescence and maintaining service reliability. Strategic governance structures, like roadmap planning and monthly reviews, help CSPs manage the selection and implementation of technological standards.

**d) provides the operator with sufficient information to enable the operator to clearly understand the provider's roles and responsibilities in managing risks related to the FMI's use of the provider.**

CSPs ensure transparency in their roles and responsibilities through detailed documentation such as MSAs, SLAs, and operational manuals. These documents clarify the scope of services, risk management expectations, and incident management procedures. In addition, CSPs maintain open lines of communication through regular governance meetings, monthly reporting, and performance reviews, ensuring that ESAS has a clear understanding of how risks are being managed and what steps are being taken to mitigate them.

**3) An operator must identify the FMI's critical service providers and disclose the FMI's dependency on those providers to the regulator and, where appropriate, its participants.**

The operator identifies and discloses its dependencies on CSPs to the regulator, ensuring full transparency regarding these relationships. This disclosure includes detailed information about how the operator relies on its CSPs — such as NEXI for software development, Datacom for

hardware support, and SWIFT for messaging and network services — to maintain key operational functions. Reports and updates are shared with the regulator when necessary, highlighting the critical nature of these dependencies and any associated risks.

Where appropriate, the operator also informs participants, ensuring they are aware of the essential role these providers play in supporting the reliability and continuity of the FMI. This proactive disclosure process helps ensure that both the regulator and participants understand the potential risks related to the operator's reliance on CSPs, fostering trust and enabling informed decision-making.

## FMI Standard 17C: Cyber Security Risk

### Assessment

#### ESAS Complies with Standard 17C

- 1) **An operator must ensure that the FMI maintains cyber resilience in a manner that is commensurate with the FMI's exposure to cyber risk and enables the FMI to remain sound and efficient.**

The operator ensures that the FMI's cyber resilience strategy aligns with the FMI's exposure to cyber risks and supports the continued soundness and efficiency of the system. This is achieved by adopting a multilayered approach:

The RBNZ maintains a comprehensive Information Security Management Policy supported by a suite of detailed sub-policies. These are aligned with national and international frameworks — including the NZISM, ISO 27001, the NCSC Cyber Security Framework, and the SWIFT CSP — ensuring that cyber security controls remain robust and appropriate for the environment in which the FMI operates. This governance foundation provides the structure within which cyber risks are managed and mitigated.

Day-to-day cyber resilience is maintained through well-defined information security standards and standard operating procedures (SOPs). These procedural documents guide operational teams in executing security activities consistently and systematically, helping to safeguard the FMI from emerging cyber threats. The RBNZ's Certification and Accreditation (C&A) process, which is fully aligned with NZISM requirements, provides another key layer of assurance. It ensures that all new and existing systems supporting the FMI undergo appropriate security assessment before being placed into operation, confirming that the security posture remains fit for purpose.

Clear accountability is a central feature of the cyber resilience framework. Roles and responsibilities are formally defined across the organisation — including specific responsibilities for the CISO and Chief Security Officer (CSO). Senior management oversees the cyber risk environment and ensures alignment with the broader cyber resilience strategy. Regular reporting to the Board ensures visibility of vulnerabilities, threats, and major developments. The RBNZ's Protective Security Requirements policy on the Vault further sets out organisational accountabilities for protective security, including cyber security.

Given the FMI's reliance on external service providers, vendor and third-party risk management forms an integral part of cyber resilience. The RBNZ's vendor management processes require third-party providers, including CSPs, to meet defined cyber security expectations. This includes embedding non-functional security requirements into RFPs and ensuring that all relevant systems and services undergo C&A by the RBNZ Cyber Security Team. These controls help to mitigate risks introduced through external technology providers.

Regular testing further strengthens the FMI's resilience posture. Failover exercises, data centre swaps, and contingency tests are conducted routinely to validate the effectiveness of business continuity arrangements. These activities ensure that the FMI can continue operating in the event of a cyber-related disruption, with annual reviews providing assurance that continuity measures remain robust.

In the event of a cyber incident, established incident reporting procedures ensure that it is escalated and managed appropriately. Any cyber incident affecting financial market infrastructures is treated as an operational or material incident and reported through the RBNZ's formal incident management processes. Additionally, new requirements under the FMI Act provide for 6-monthly reporting to regulators, ensuring transparency and regulatory oversight.

Through these combined measures — robust governance, well-defined procedures, strong assurance mechanisms, clear accountability, third-party oversight, rigorous testing, and structured incident reporting — the operator ensures that the FMI's cyber resilience remains aligned with its exposure to cyber risks, enabling the system to remain secure, sound, and efficient.

## 2) Cyber resilience strategy and framework.

**Further to the requirements in clause (1), an operator must ensure that the FMI has a cyber resilience strategy and cyber resilience framework that is comprehensive, adequate, and credible. The operator must ensure that the cyber resilience strategy and cyber resilience framework:**

- a) **are based on internationally and nationally recognised frameworks and guidelines;**

To address the requirements under clause (2) relating to the cyber resilience strategy and framework for an FMI Operator, and particularly for ESAS, which is operated by the RBNZ, we can confirm that the RBNZ meets these expectations through a comprehensive, adequate, and credible set of cyber resilience arrangements grounded in both national and international frameworks and guidelines. As part of this approach, the RBNZ complies with key national frameworks, including the NZISM and the Protective Security Requirements, demonstrating its adherence to nationally recognised standards for information security.

In addition to these national obligations, the RBNZ also aligns with international expectations. As a member of the SWIFT network, the System Operator of ESAS is obligated to comply with the SWIFT CSP, ensuring that ESAS aligns with the internationally mandated security practices applied to global financial messaging. The RBNZ has also adopted elements from several internationally recognised frameworks, including ISO/IEC 27001:2022, which establishes the information security management system (ISMS) principles that guide how sensitive information relevant to ESAS is managed. Complementing this, the NIST Cyber Security Framework provides further guidelines for managing and reducing cyber security risks, strengthening the overall cyber security posture for ESAS.

The comprehensiveness and adequacy of the RBNZ's cyber resilience strategy is supported through the RBNZ's Digital and Security Strategy, which sets out the approach for investing in and prioritising cyber security capabilities for both the RBNZ and ESAS. This strategy outlines how the organisation prepares for and responds to emerging cyber threats and reinforces the importance of continued capability uplift. This is further supported by the RBNZ Information Security Policies & Standards documents, which specify the expected processes and acceptable use of IT systems, ensuring that the cyber resilience framework remains adequate for ESAS.

The credibility of the cyber resilience framework is further strengthened through the adoption of recognised governance frameworks such as the NCSC Cyber Security Framework, which helps reinforce the integrity and reliability of the RBNZ's cyber resilience initiatives for ESAS. Continuous updating of security policies and frameworks within the RBNZ Policy Portal ensures that staff,

including those supporting ESAS, remain aware of current expectations and adhere to the latest security practices, contributing to a credible and effective cyber resilience framework.

Finally, as a financial sector regulator, the RBNZ is committed to demonstrating leadership as a cyber security exemplar, and this commitment naturally extends to ESAS. This aligns with the organisation's strategic theme of 'promoting understanding and trust', which emphasises transparency, accountability, and strong cyber security governance.

In summary, ESAS, as operated by the RBNZ, follows a comprehensive, adequate, and credible cyber resilience strategy and framework that is firmly grounded in national and international guidelines. The integration of these recognised frameworks and the RBNZ's ongoing investment in cyber security capabilities ensure that ESAS effectively manages its cyber resilience obligations and positions itself as a leader in this domain.

**b) align with the FMI's business objectives, stakeholder requirements, corporate strategy, risk management framework, and other related strategies and frameworks; and**

ESAS's cyber resilience strategy is designed to ensure that cyber security measures not only protect against threats but are fully aligned with the FMI's business objectives, stakeholder requirements, corporate strategy, RMF, and related strategies and frameworks. This alignment begins with ESAS's core business objectives, particularly its target of achieving 99.95 percent system availability. Because high availability is essential for maintaining trust and credibility across the financial system, the cyber resilience strategy is structured to support this objective through robust incident response planning, system redundancy, and proactive monitoring to safeguard uptime and continuity.

The strategy also reflects the requirements and expectations of key stakeholders, including ESAS participants, supervisors, and the wider financial sector. By demonstrating a clear commitment to strong cyber security practices and consistent system availability, ESAS reinforces confidence among stakeholders and supports the organisation's broader strategic theme of 'promoting understanding and trust'. This focus on stakeholder expectations ensures that cyber resilience is not treated simply as a technical function but as a core enabler of ESAS's reputation and reliability.

Alignment with the RBNZ's corporate strategy is also a fundamental part of the framework. The cyber resilience strategy supports the organisation's ambition to demonstrate leadership as a cyber security exemplar by adopting internationally recognised frameworks such as the NIST Cyber Security Framework, ISO/IEC 27001:2022, and the SWIFT CSP. By aligning with these standards, ESAS ensures its cyber security practices are consistent with global best practices and meet the expectations of both national and international stakeholders.

ESAS's cyber resilience strategy is further integrated with its broader RMF, ensuring cyber security risks are assessed alongside operational, technological, and resilience-related risks. This integration enables the identification of threats to system availability and prioritises investment in cyber security capabilities where they are most needed to reduce risk exposure.

The strategy also aligns with related organisational frameworks, including the RBNZ Digital & Security Strategy, the RBNZ Information Security Policies & Standards, and the Protective Security Requirements. Consistency with these frameworks ensures that ESAS's cyber security initiatives reflect the organisation's overall security architecture, strategic direction, and governance

expectations. This alignment reinforces ESAS's commitment to comprehensive and coherent security oversight.

Performance monitoring and reporting play an important role in maintaining alignment with business objectives. KPIs relating to cyber security and system availability enable ESAS to measure the effectiveness of its resilience efforts and ensure that these remain responsive to emerging risks. Regular reporting and review processes allow for timely recalibration of the strategy where necessary.

Finally, ESAS's cyber resilience strategy incorporates mechanisms for continuous improvement, ensuring that it remains adaptive to evolving cyber threats and stakeholder needs. Regular reviews of the framework and updates informed by stakeholder feedback ensure that ESAS continues to meet its organisational objectives while maintaining a strong and future-focused cyber-resilience posture.

- c) **are commensurate with the FMI's cyber risk tolerance, cyber risk appetite, and the operational reliability objectives required under Standard 17: 'Operational risk'; and**

ESAS's cyber resilience approach is closely aligned with the organisation's broader risk appetite and risk management expectations. ESAS operates within the boundaries defined by the RBNZ's Risk Appetite Statement, which articulates the level of risk the organisation is willing to accept to achieve its objectives. This statement serves as the foundation for determining the extent of cyber security measures required to protect the system from potential threats, and it ensures that cyber resilience remains consistent with the FMI's overall RMF.

Cyber security risk management at the RBNZ is integrated directly into the enterprise risk management model. This ensures that cyber security risks are identified, assessed, and managed in a manner that reflects organisational objectives and supports system resilience. Regular assessments undertaken by the RBNZ Cyber Security Team help identify how cyber risks may manifest and guide the development and implementation of appropriate controls. In addition, quarterly updates are provided by Cyber Security in partnership with the Risk business partner to inform of current and emerging cyber risks.

The cyber risk assessment process is supported through tools such as the Cyber Security Risk Assessment template, where the DSS Security Team uses a 5x5 risk matrix to evaluate both the likelihood and impact of cyber security risks. This structured methodology provides consistency and transparency in how cyber risks are assessed and prioritised.

The cyber resilience approach is also closely tied to ESAS's operational reliability objectives. The goal of maintaining 99.90 percent system availability — outlined under Standard 17 — depends on a cyber resilience strategy that prioritises high availability and ensures that operational capabilities are protected against cyber threats. By embedding this objective into the cyber resilience strategy, ESAS strengthens its ability to maintain continuity and performance standards.

Risk visibility is further enhanced through enterprise-wide risk profiles maintained by the RBNZ's Risk Management Team. These profiles include business departments such as the FMI&S Directorate, which operates ESAS, and help provide insight into the organisation's current risk levels. This visibility supports proactive management of cyber security risks and ensures that these risks remain aligned with the organisation's stated risk appetite.

ESAS's alignment with risk management expectations is also supported by participation in key forums, including the FMI&S Risk Management Forum, which facilitates ongoing dialogue around identifying and assessing risks relevant to ESAS. These discussions help ensure that cyber risks are addressed in a manner consistent with operational priorities and risk tolerance, allowing for the establishment of targeted controls and appropriate mitigation strategies.

Awareness of emerging risks is another key component of this alignment. Through initiatives such as the External or Emerging Risks Forums, the RBNZ actively monitors potential external threats that may affect the organisation. This proactive approach ensures that cyber security strategies remain relevant and responsive to changes in the risk environment, and that ESAS continues to adapt to emerging challenges.

Finally, ESAS supports continuous improvement through regular reporting on cyber security posture and risk assessment outcomes. These reports provide leadership with clear visibility of the organisation's security landscape and support informed decision-making. This regular flow of information enables timely adjustments to strategies and controls, ensuring ongoing alignment with ESAS's risk tolerance and operational reliability objectives.

- d) identify and assess the cyber risk associated with the use of third-party service providers, and outline how this risk will be managed, including through compliance with the requirements in Standard 17B: 'Critical service providers'; and**

The RBNZ implements a comprehensive Vendor Management process that emphasises the importance of securing a resilient IT supply chain. As part of this process, the RBNZ Cyber Security Team carries out C&A of both new and existing third-party technology service providers. This includes evaluating the security measures and controls in place to protect sensitive data and ensuring that these providers are capable of safeguarding against cyber threats. The C&A process provides assurance regarding the security of the information systems and services used to store, process, and access data. Accreditation formally authorises the operation of any new IT system, application, or tool within the RBNZ environment, mandating that each undergoes a rigorous C&A process on a regular cycle to ensure they continue to meet security standards.

To effectively manage identified cyber risks, the RBNZ ensures that contractual obligations regarding cyber security are clearly articulated and understood by all parties involved. This includes incorporating specific requirements into contracts with third-party service providers, mandating compliance with industry standards and best practices related to cyber security.

The RBNZ is committed to complying with the requirements set forth in Standard 17B, which pertains to CSPs. This involves implementing a framework that includes:

- 1.** Regular Risk Assessments: Periodic assessments of third-party providers to evaluate their cyber risk profiles are carried out through the C&A process.
- 2.** Monitoring and Reporting: Ongoing monitoring of third-party service providers' cyber security practices and incident reporting mechanisms to ensure timely communication of potential risks.
- 3.** CSPs develop and maintain incident response plans to respond effectively to any cyber security incidents that may impact the services provided to the FMI.

Through these measures, the RBNZ aims to mitigate cyber risks associated with third-party service providers while maintaining compliance with the necessary regulatory standards, thereby ensuring the security and reliability of its IT supply chain.

- e) **set out how information on cyber incidents and threats will be securely shared with relevant external stakeholders, including the regulator and participants; and**

Cyber incidents that affect the integrity, availability, or reliability of payment and clearing services will be treated as material incidents. Such incidents will be reported through the established incident management reporting framework. This ensures that all relevant parties are promptly informed and can take appropriate actions to mitigate any potential risks arising from the incident.

In accordance with the new requirements under the FMI Act, RBNZ adheres to the mandated 6-month reporting framework concerning cyber incidents and threats. This includes providing comprehensive updates on the status of cyber security practices, incidents that have occurred, and the responses undertaken to address those incidents.

- f) **provide for cyber resilience training to staff members (the content of which will depend on the nature of the role) during the entire employment lifecycle; and**

Cyber resilience training is provided to all staff members throughout their employment lifecycle, with content tailored to the nature of each role. Training includes foundational security practices during onboarding, regular role-specific sessions (for example, phishing awareness for finance teams and advanced threat management for IT/security teams), and ongoing refreshers to ensure all employees remain informed on current threats. Please see the attached Cyber Security Awareness training page — [It's Cyber Smart Week 2024 – The Vault](#).

- g) **are reviewed annually, and updated when required, to ensure that any changes in the cyber risk environment are adequately managed.**

Cyber resilience training content is reviewed and updated annually, and necessary adjustments are made whenever significant changes in the cyber risk environment arise. This ensures our staff training remains aligned with evolving cyber threats and best practices.

- 3) **Further to the requirements in clause (1), the operator must ensure that its board of directors is ultimately responsible for the cyber resilience of the FMI. An operator must take reasonable steps to ensure that its board of directors understands the cyber risk environment that the FMI operates in, including ensuring that its board of directors:**
  - a) **Appoints a senior manager with the appropriate skills, knowledge, and experience to be accountable for the FMI's cyber resilience strategy and cyber resilience framework.**

The RBNZ has appointed a CISO who is responsible for the information security strategy and policy, governance of cyber security risks, and the delivery of cyber security initiatives. The CISO is tasked with overseeing the implementation of the FMI's cyber resilience strategy and ensuring that appropriate skills, knowledge, and experience are applied to manage cyber resilience effectively.

- b) **Ensures that senior management updates the board of directors on any significant changes to the FMI's vulnerabilities or the wider cyber risk environment.**

The RBNZ Security Advisors, along with the CISO, play a crucial role in communicating significant changes in the FMI's vulnerabilities and the wider cyber risk environment to the board of directors. Regular updates and reports are facilitated through established channels to ensure that the board is informed and can make informed decisions regarding cyber resilience.

- c) **Reviews and approves the FMI's cyber resilience strategy and cyber resilience framework and monitors the implementation of such strategy and framework, including any policies, procedures, and internal systems that support this implementation.**

The Governor of the RBNZ holds ultimate accountability for security, including the approval of the FMI's cyber resilience strategy and framework. The board of directors, alongside the CISO, regularly reviews and monitors the implementation of the cyber resilience strategy, policies, procedures, and internal systems to ensure effective governance and compliance with security practices.

- d) **Takes responsibility for determining the FMI's cyber risk tolerance and cyber risk appetite.**

The Risk Compliance and Audit Directorate, alongside senior leadership, is responsible for determining the FMI's cyber risk tolerance and appetite. This involves assessing the potential impact of cyber risks on the organisation and establishing a framework that aligns with the RBNZ's overall risk management strategy, ensuring that the organisation can operate within its defined risk boundaries.

By assigning these roles and responsibilities across various levels of management, RBNZ ensures that cyber resilience is integrated into its governance framework, promoting a comprehensive approach to managing cyber risks.

- 4) **An operator must ensure that the cyber resilience strategy and the cyber resilience framework, and the subsequent compliance with them, are assessed by way of an external assurance engagement by a qualified auditor in accordance with applicable auditing and assurance standards:**

- a) at least every two years; and
- b) subject to clause (6), whenever a cyber incident occurs that materially impacts, or could materially impact, the FMI's continuing operations.

The System Operator has engaged a qualified auditor to perform an external assurance review of the cyber resilience strategy and framework. This review will follow all relevant auditing and assurance standards and will take place at least every two years. This work is underway currently.

In the event of a cyber incident that materially impacts or has the potential to impact the FMI's ongoing operations, the operator will initiate an external assurance engagement to assess the incident's impact and the system's response.

- 5) **An operator must provide any report from an external assurance engagement to the regulator at the regulator's request.**

The System Operator will comply with this requirement by providing any report from an external assurance engagement to the regulator upon request.

- 6) **Clause 4(b) does not apply if, in the opinion of the operator, it is not reasonably practicable to seek an external assessment following a cyber incident that materially impacts, or could materially impact, the FMI's continuing operation**

The System Operator will comply with this requirement by providing any report from an external assurance engagement to the regulator upon request.

- 7) **If clause (6) applies, the operator must provide reasons for its opinion to the regulator as soon as possible following the cyber incident.**

The System Operator will comply with this requirement by providing any report from an external assurance engagement to the regulator upon request.

## FMI Standard 18: Access and Participation Requirements

### Assessment

#### ESAS Complies with Standard 18

- 1) **An operator must have objective, risk-based, and publicly disclosed criteria for participation in the FMI, which permit fair and open access to the FMI.**

The ESAS Operator maintains objective, risk-based, and publicly disclosed criteria for participation in ESAS that permit fair and open access to the system, consistent with the requirements of FMI Standard 18.

The access criteria are formally set out in the ESAS Access Criteria (April 2025), which are published on the RBNZ's website as part of the public information on payments and settlement systems. These criteria describe the eligible business activities that are eligible to hold Exchange Settlement Accounts and the documentation required to demonstrate that each criterion has been met. The access criteria are designed to ensure that only entities with the necessary financial soundness, governance capability, operational capacity, and legal standing may access ESAS, thereby protecting the integrity and stability of the system.

The criteria are designed to be objective. Each criterion is clearly defined and supported by guidance describing how an applicant can demonstrate compliance. The guidance specifies the types of documentation and policies that the ESAS Operator may consider in its assessment, such as evidence of incorporation and licensing, risk management policies, operational risk frameworks, board charters, or external assurance reports.

The criteria are risk-based and are underpinned by the ESAS Risk Assessment Framework (RAF). The RAF was developed as part of the ESAS Access Review Project and was the subject of public consultation in 2023. Feedback from that consultation was used to refine the framework and ensure its alignment with the ESAS Operator's low-risk appetite. The RAF identifies the types of risks a participant may introduce to ESAS — including credit, liquidity, operational, legal, and compliance risks — and provides a structure for determining whether these risks can be mitigated to a level that is acceptable for ESAS operations.

Access to ESAS involves confirming that the applicant's business activities fall within the pre-defined activities that support the purposes and functions of ESAS, ensuring that participation contributes to the effective operation of the New Zealand payments system. A detailed risk assessment is then applied against the published risk-based criteria, which include requirements for anti-money laundering (AML) and countering financing of terrorism (CFT) compliance, prudential oversight, governance, and operational resilience. These assessments ensure that prospective participants do not expose the system to risks inconsistent with the ESAS Operator's responsibilities under the FMI Act or with the overall risk appetite established for ESAS.

Opening ESAS to applications under the ESAS Access Criteria (April 2025) has been implemented in phases to expand access in an orderly and risk-controlled manner. Phase One, completed in April 2025, extended eligibility to licensed non-bank deposit takers (NBDTs) in New Zealand. Phase Two, completed in September 2025, further extended eligibility to payment service providers

(PSPs) and other institutions that satisfy the published access criteria and can meet the operational, governance, and legal requirements applicable to ESAS Accountholders. Each phase of the ESAS opening has been accompanied by appropriate risk-assessment procedures and legal and operational safeguards to maintain the safety and resilience of the system.

The ESAS Operator ensures that access criteria and related information are publicly disclosed. The full access criteria document and guidance on the application process and documentation requirements are published on the RBNZ's website. The website includes a 'How to apply for ESAS access' section that provides application information specific to the five applicant categories defined in the access criteria: licensed deposit takers, PSPs, overseas deposit takers, market makers and designated FMIs.

By publishing this information, the ESAS Operator provides transparency regarding the access criteria and documentation needed to meet the criteria. This approach ensures that all potential participants have access to the same information and that the process of applying for access is fair, open, and transparent.

In summary, the ESAS Operator has established and implemented access criteria that are objective, risk-based, and publicly disclosed. These criteria and the supporting guidance ensure that access to ESAS is open to eligible institutions on a fair basis, while maintaining the safety, integrity, and efficiency of the system in accordance with the requirements of the FMI Act and FMI Standard 18.

**2) Further to the requirements in clause (1), an operator must:**

- a) Allow fair and open access to the FMI's services, including by direct and, where relevant, indirect participants and other FMIs.**

The ESAS Operator ensures fair and open access to ESAS through transparent, risk-based access criteria that went into full effect on 23 September 2025 (Access to ESAS is granted on an objective, criteria-driven basis that assesses both (i) the alignment of an applicant's business activity with the purposes of ESAS, and (ii) the applicant's risk profile in accordance with the ESAS Access Criteria April 2025 and the supporting RAF.

The published access criteria specify five categories of eligible business activities (licensed deposit takers, PSPs, overseas deposit takers, market makers and designated FMIs); as well as AML compliance, prudential and governance, operational, and legal enforceability (for overseas applicants) requirements. These objective and transparent criteria make it clear to any interested entity whether they are eligible to apply and how they can demonstrate they have met the risk requirements.

- b) Ensure that access requirements are:**
- i) based on reasonable risk-related participation requirements; and**
  - ii) justified in terms of the safety and efficiency of the FMI and the markets that it serves; and**
  - iii) tailored to, and commensurate with, the FMI's specific risks; and**
  - iv) publicly disclosed.**

The access criteria are grounded in the ESAS Participant Risk Assessment Framework, which identifies and evaluates the potential risks an applicant may pose to the system: credit, liquidity, operational, legal, and compliance. The framework ensures that only entities with sound governance, financial capacity, and robust risk management are admitted.

Each criterion within the Access Criteria is directly linked to a risk dimension within the RAF. For instance, AML compliance requirements mitigate financial crime risk, prudential and governance criteria address credit and legal risks, and operational criteria manage resilience and technology risks. The ESAS access and participation requirements are specifically designed to uphold both the safety and efficiency of the system and the markets it serves.

As a systemically important FMI, ESAS must ensure that all participants can meet their settlement obligations reliably, without introducing undue credit, liquidity, operational, technological, or legal risks. The access criteria, therefore, require applicants to demonstrate strong governance, adequate financial capacity, resilient operational arrangements, and robust risk management practices. These requirements protect the system from participant failures, operational disruptions, and compliance breaches, thereby supporting the safe functioning of the broader financial system.

At the same time, the criteria promote efficiency by ensuring that access is open to a broad range of qualified institutions, without imposing unnecessary barriers. The requirements are risk-based and proportionate, enabling entities with appropriate capability to participate while avoiding overly restrictive or burdensome obligations.

All requirements are published on the RBNZ website, along with application guidance and supporting documentation. This transparency enables potential applicants to assess their eligibility and align their submissions with the operator's risk tolerance and system objectives.

- c) Set requirements that have the least restrictive impact on access to the FMI that circumstances permit, subject to the maintenance of acceptable risk standards.**

The access criteria are designed to facilitate broad, proportionate participation consistent with ESAS's statutory purposes under the FMI Act. The operator adopts a least-restrictive approach by calibrating risk thresholds according to the nature of the applicant's business activities and its business model.

Applicants that are already subject to prudential supervision in New Zealand (for example, licensed deposit takers and designated FMIs) are deemed to satisfy certain criteria automatically, while non-regulated entities such as New Zealand-based PSPs are assessed against tailored financial, operational, and governance requirements. This approach balances open access with the need to maintain acceptable risk standards to ensure the safety and efficiency of ESAS and the markets it serves.

- d) Monitor compliance with participation requirements for the FMI on an ongoing basis and have clearly defined and publicly disclosed procedures for facilitating the suspension and orderly exit of a participant that breaches, or no longer meets, the participation requirements.**

The ESAS Operator has established a structured, risk-based monitoring framework to ensure that all participants will continue to meet the access and participation requirements set out in the ESAS Rules and the ESAS Access Criteria (April 2025). The compliance framework includes both continuous and periodic monitoring to verify compliance, detect emerging risks, and safeguard the operational integrity and stability of ESAS.

### Monthly monitoring NBDTs

NBDTs who join ESAS for the purposes of holding reserves to meet prudential liquidity requirements will be subject to monthly monitoring. Under the proposed arrangements, the ESAS Operator will conduct monthly monitoring of payments to and from each NBDT's ESAS account to confirm that all transactions are limited to those made through the NBDT's nominated settlement bank. Payments made to, or received from, any other ESAS Accountholder would constitute a high-value payment and breach the conditions of access. Where such activity occurs, the Accountholder will be required to regularise its settlement arrangements, including, where applicable, joining the HVCS.

Monthly monitoring will also include the review of month-end balances against forecast information submitted during the application process. Where material deviations or sustained increases are identified, the ESAS Operator will consult with the Financial Markets Department and other relevant functions to assess whether the changes are significant or may indicate a prudential or liquidity concern.

### Annual monitoring

An annual compliance review programme is being enhanced and will apply to all ESAS Accountholders following the full implementation of the updated access criteria. This programme will be scheduled around the anniversary of each Accountholder's admission to ESAS and will include:

- verification of tax reporting obligations
- self-attestations on financial crime compliance
- confirmation from AML/CFT supervisors of continued compliance
- checks of SWIFT CSP attestations, and
- validation of current credit rating information.

Accountholders will also be required to reconfirm legal and governance attestations, demonstrating that contractual enforceability and risk management arrangements remain sound.

In addition, Accountholders will provide attestations that their business continuity and DR frameworks are maintained and tested, and that they remain compliant with all domestic and international sanctions requirements. Conditions or caveats applied during the application process will be monitored to confirm ongoing adherence, and authorised signatory registers will be confirmed to preserve their integrity.

### Ad hoc and event-driven monitoring

Ad hoc and event-driven monitoring will supplement periodic monitoring. This will include reviews triggered by supervisory feedback, material adverse developments reported in trade publications,

or international regulatory actions concerning an overseas participant. Such event-based reviews will enable the ESAS Operator to detect and address emerging risks in a timely manner.

### Addressing non-compliance or emerging risk

Where monitoring identifies non-compliance or emerging risk, the ESAS Operator can apply graduated escalation measures in line with the ESAS Rules, ranging from remedial requirements and conditional participation to temporary suspension or, if necessary, orderly exit.

All compliance monitoring, escalation, and exit procedures will be formally documented in the updated ESAS Rules and publicly disclosed on the RBNZ's website following their approval under section 39 of the FMI Act.

This monitoring framework is designed to ensure that ESAS maintains effective and proportionate.

## FMI Standard 19: Tiered Participation Arrangements

### Assessment

#### ESAS Complies with Standard 19

- 1) **The operator must identify, monitor, and manage the material risks to the FMI arising from tiered participation arrangements.**

The ESAS Operator identifies, monitors, and manages any material risks to the FMI arising from tiered participation arrangements. Tiered participation refers to arrangements in which entities that are not direct ESAS Accountholders ('indirect participants') access ESAS services through direct participants. ESAS has only direct participants (Accountholders). These participants may, in the normal course of their business, process transactions on behalf of their own clients. While such client activity may resemble tiered participation arrangements in practice, access to ESAS is not provided directly to third parties, and all settlement activity occurs solely through ESAS Accountholders.

ESAS is designed as an RTGS system operating in central-bank money. This design significantly limits the potential for systemic risk from tiered participation. Transactions settle individually and irrevocably in real time, with no provision of overdraft facilities or credit exposure between participants. This structure confines any potential disruption to the bilateral relationship between the direct participant and its customer, rather than to the system as a whole.

Since 2022, the ESAS Operator has periodically collected information on indirect participation through targeted surveys of systemically important participants. The 2022 and 2024 and again in 2025 surveys confirmed that indirect participation in ESAS was limited and did not present a material risk to the FMI.

Following completion of Phase Two of the ESAS Access Review on 23 September 2025, the ESAS Operator formalised these monitoring arrangements, embedding them within its broader participant-compliance and risk-assessment framework. This ensures that indirect participation is now reviewed on a systematic and ongoing basis as part of the ESAS Operator's core compliance programme.

- 2) **Further to the requirements in clause (1), the operator must: a) ensure that the FMI's rules, procedures, and contracts allow the operator to gather basic information about indirect participation in order to identify, monitor, and manage any material risks to the FMI arising from such tiered participation arrangements; and**

The ESAS Rules empower the Operator to obtain information relevant to the operation of each Account. Clause 14.1 of the ESAS Rules requires Accountholders to provide the Operator with any information reasonably requested, enabling the Operator to collect data necessary to identify, monitor, and manage risks from indirect participation.

Building on this authority, the Operator now maintains a formalised compliance process that includes an annual tiered-participation questionnaire and targeted information requests for high-volume participants. The responses are assessed and used to update the Operator's understanding of tiered structures and associated risk exposures.

- b) **identify material dependencies between direct and indirect participants that might affect the FMI; and**

Analysis from the 2025 compliance cycle confirmed that indirect participation continues to represent a very small proportion of overall ESAS transactions and is not significant relative to the operational or financial capacity of the sponsoring direct participants.

The ESAS Operator, therefore, has not identified any material dependencies between Accountholders and their clients that could affect the safe or efficient operation of ESAS.

Under the new compliance framework, these dependencies are reviewed annually, with data from the tiered-participation questionnaire and transaction analysis providing early indicators of any emerging concentration or reliance on a single direct participant.

- c) identify: i) indirect participants responsible for a significant proportion of transactions processed by the relevant FMI; and ii) indirect participants whose transaction volumes or values are large relative to the operational and financial capacity of the direct participants through which they access the FMI; and**

The design of ESAS as an RTGS system plays a pivotal role in minimising risk. ESAS operates without providing overdrafts and settles transactions on an irrevocable basis using central bank funds. This design significantly reduces the risk of loss to the System Operator and other Accountholders in the event of an Accountholder's failure.

Accountholders are responsible for managing risks generated by their customers. They must ensure that they have sufficient controls in place to mitigate the risk that their customers' activities will disrupt their ability to meet their settlement obligations in ESAS. The Accountholders that account for the highest volumes and values processed through ESAS are typically registered banks. These banks are required to prepare quarterly attestations regarding their management of key risks, ensuring a high level of oversight and risk management.

In 2022, the System Operator implemented a process change to monitor the extent of activities conducted on behalf of indirect participants by systemically important participants. Surveys conducted in 2022 and 2024 and 2025 provided information about the tiered dynamics within the New Zealand financial markets.

The surveys conducted in 2022, 2024, and 2025 assessed whether any clients were responsible for a significant proportion of transactions processed through ESAS or whether client activity was large relative to the capacity of the sponsoring Accountholders. The results confirmed that, while some participants exhibit higher client concentration than others, these concentrations are well understood, actively managed, and not material to ESAS.

Given the robust design of ESAS as an RTGS system and the effective risk management practices enforced by Accountholders, the System Operator has concluded that the risks arising from tiered participation are minimal. The monitoring process and the findings from the recent surveys affirm that the current level of indirect participation does not warrant additional actions by the System Operator.

- d) review risks arising from tiered participation arrangements on at least an annual basis and taking action to mitigate all material risks following this review.**

The System Operator has implemented an annual process to monitor and review risks associated with tiered participation arrangements. This process includes periodic assessments designed to identify and evaluate the materiality of risks arising from the interactions between direct participants and their clients.

The outcomes of the 2022, 2024, and 2025 reviews consistently indicate that client activity does not represent a material risk to the FMI. Concentration levels observed across major participants are managed within robust risk management frameworks that cover financial, credit, AML/CFT, operational, and cyber-security risks. These frameworks ensure that client-related risks are identified, monitored, and mitigated at the participant level in a manner consistent with Principle 19.

Given the design of ESAS as an RTGS system, which operates without providing overdrafts and settles transactions on an irrevocable basis in central bank funds, the risk of loss to the System Operator and other Accountholders due to the failure of an Accountholder is minimised. Accountholders are required to manage the risks generated by their customers and to have sufficient controls in place to mitigate any potential disruptions to their ability to meet their obligations in ESAS.

Based on the findings from the risk assessment surveys and the System Operator's understanding of the tiered participation dynamics, it has been determined that the risks posed by clients of Accountholders are not material.

## FMI Standard 20: FMI Links

### Assessment

#### ESAS Complies with Standard 20

- 1) **An operator of an FMI that establishes a link with one or more FMIs must identify, monitor, and manage link-related risks.**

FMI&S Directorate has confirmed that PNZ, CLS, and NZClear are recognised as FMI links for ESAS. These links are integrated into the RMFs and processes that are deployed across the FMI. As part of this framework, link-related risks are identified, monitored, and managed through regular assessments and ongoing reviews.

In addition to the RMF, these FMI links are also incorporated into BCP scenarios, ensuring that contingency plans account for disruptions related to these links. Furthermore, incident management procedures are in place, specifically designed to coordinate with the FMIs during operational incidents, ensuring the timely and effective resolution of any issues that arise within these linked infrastructures.

The link between NZClear and ESAS is characterised by their shared ownership and operation by FMI&S Directorate. As both systems are managed under the same operator, they operate within a unified RMF that facilitates the effective identification, monitoring, and management of risks.

The fact that both NZClear and ESAS are operated by the same entity (FMI&S) means that risk management practices are consistent across both systems. This synergy allows for comprehensive oversight and streamlined communication regarding operational, legal, and financial risks.

The shared RMF ensures that any risks associated with one system are understood in the context of the other. This integration enhances the overall resilience of both systems, allowing for effective responses to operational incidents and compliance with regulatory standards.

### Requirement 2

- 2) **An operator must ensure that before entering into a link, and on an ongoing basis once the link is established, the operator identifies, monitors, and manages all potential sources of risk arising from the link.**

RMFs are regularly reviewed to ensure they remain effective in addressing any emerging risks. Additionally, link-related risks are integrated into the BCP scenarios to ensure that disruptions in linked FMIs such as PNZ, CLS, and NZClear are accounted for. Incident management procedures are also established and regularly tested with these FMIs, ensuring that coordinated responses are in place to mitigate potential disruptions and ensure system integrity.

- 3) **Further to the requirements in clause (1), an operator must:**
  - a) **design links such that each FMI is able to observe the other FMI's compliance with the applicable FMI Standards or relevant overseas standards; and**

When establishing links between ESAS and other FMIs, such as NZClear and CLS, the system is designed to ensure that each FMI can effectively observe the other's compliance with the relevant

standards. This involves a mutual understanding of the operational requirements, risk management processes, and compliance obligations, either under domestic FMI Standards or overseas equivalents. Regular reviews and assessments are conducted, enabling ESAS to verify that linked FMIs continue to meet their regulatory and operational requirements. This fosters transparency and trust between the systems, ensuring that compliance with applicable standards is actively monitored and maintained.

- b) **Ensure that the link has a well-founded legal basis, in all relevant jurisdictions, that supports the link's design and manages operational, legal, and financial risk to the FMIs involved in the link**

Each link established between ESAS and other FMIs is governed by a strong legal foundation. For PNZ, the PNZ Rules explicitly cover RBNZ's participation, and the RBNZ's own terms and conditions acknowledge PNZ as a settlement submission mechanism, ensuring clarity around roles and responsibilities and legal alignment between the two. For CLS, a signed terms and conditions agreement is in place, and a detailed legal protocol governs the interaction between RBNZ and CLS, ensuring that legal risks are adequately addressed across jurisdictions.

In the case of NZClear, both NZClear and ESAS are operated by the RBNZ, which simplifies the legal framework. As both systems are under the same operator, they are subject to the same legal and operational controls, reducing potential legal complexities and ensuring consistency in managing operational, legal, and financial risks.

These legal arrangements ensure that the links have a solid foundation that supports their design and ongoing operations. The legal basis helps manage risks and provides a mechanism for addressing issues such as dispute resolution, enforcement of obligations, and compliance with relevant FMI standards in all applicable jurisdictions.

### Central securities depositories

- 4) **Further to the requirements in clause (1), an operator of a central securities depository that is part of a link must:**
  - a) **measure and manage the credit and liquidity risks arising from other linked central securities depositories; and**
  - b) **ensure that any credit extensions between the central securities depository and another central securities depository are covered fully with high-quality collateral, and are subject to size limits.**

The requirement is not applicable. ESAS is not a CSD.

- 5) **Further to the requirements in clause (1), an operator of a central securities depository must prohibit provisional transfers of securities between the central securities depository and any linked central securities depository.**

The requirement is not applicable. ESAS is not a CSD.

### Investor central securities depositories

- 6) **Further to the requirements in clause (1), an operator of an investor central securities depository must:**

- a) only establish a link between the investor central securities depository and an issuer central securities depository if the arrangement provides a high level of protection for the rights of participants; and
- b) if the operator uses an intermediary to operate a link with an issuer central securities depository, measure and manage the additional risks (including custody, credit, legal, and operational risks) arising from the use of the intermediary.

The requirement is not applicable. ESAS is not a CSD

#### Central counterparties

- 7) Further to the requirements in clause (1), an operator of a central counterparty must:
  - a) identify and manage the potential spill-over effects on the other central counterparty, participants of the central counterparties, and the wider financial system from the default of the linked central counterparty; and
  - b) ensure that the FMI can fully cover, on a daily basis, its current and potential future exposures to the linked central counterparty and any participants, without reducing the ability to fulfil its obligations to its own FMI participants at any time.

The requirement is not applicable. ESAS is not a CCSP.

## FMI Standard 21: Efficiency and Effectiveness

### Assessment

#### ESAS Complies with Standard 21

- 1) 1) An operator of an FMI must ensure that the FMI is operated efficiently and effectively in meeting the requirements of the FMI's participants and the markets the FMI serves.

The System Operator engages closely with the industry through the ESAS Participation Group, ensuring that the FMI evolves in line with the needs of participants and markets. The RBNZ regularly updates Accountholders on planned fee changes and developments every six months. This allows participants to provide input on improvements and gives the RBNZ a platform to consult on any planned upgrades.

Through structured engagement, consultation processes, and regular communication channels, the System Operator ensures that ESAS continues to meet market expectations while maintaining high standards of safety, reliability, and service performance.

- 2) Further to the requirements in clause (1), an operator must: a) ensure that the FMI is designed to meet the needs of the FMI's participants and the markets the FMI serves, including: i) the choice of a clearing and settlement arrangement; and ii) the operating structure; and iii) the scope of products cleared, settled, or recorded; and iv) the use of technology and procedures; and

The System Operator communicates with participants on clearing and settlement arrangements through biannual updates. This allows participants to suggest improvements and provides transparency around any changes or upgrades to settlement arrangements.

The System Operator works with participants via the ESAS Participation Group and provides an open communication channel through the Help Desk, allowing participants to ask questions and track progress on their requests. This ensures that the operating structure is continuously aligned with the needs of participants.

The scope of products provided by ESAS is regularly reviewed in consultation with participants. Each year, a participant satisfaction survey is conducted, focusing on processing, system performance, and development. The results of the survey are made public and inform future adjustments.

The System Operator ensures that participants' needs for technology and procedures are met by regularly reviewing feedback from the annual participant satisfaction survey. In addition, the FMI's technology and procedures are subject to continuous improvement, with regular updates to meet evolving industry standards.

Further strengthening the efficiency and effectiveness of ESAS, the ESAS Access Review has ensured that participation in the system evolves in a structured, objective, and risk-based manner. By expanding eligibility in phases; first to licensed non-bank deposit takers (NBDTs) in April 2025 and subsequently to payment service providers (PSPs) and other qualifying institutions in September 2025 the System Operator has enabled broader direct access to central bank settlement. This reduces reliance on indirect or correspondent arrangements, enhances transparency, and improves overall settlement efficiency within the New Zealand payments ecosystem.

The phased and risk-controlled implementation of the revised ESAS Access Criteria ensures that expanded participation does not compromise system integrity. Access decisions are aligned with the ESAS Risk Assessment Framework and the Operator's low risk appetite, balancing efficiency, innovation, and competition with financial stability, operational resilience, and legal robustness. Through this approach, the design and operating structure of ESAS continue to adapt to evolving market needs while maintaining safety and confidence in central bank money settlement.

- b) have clearly defined goals and objectives for the FMI that are measurable and achievable, including in the areas of minimum service levels, risk management expectations, and business priorities.**

The System Operator sets clear goals and objectives for ESAS annually, focusing on system availability, customer satisfaction, and external audit outcomes. Accountholders are invited to comment on the proposed plan before it is finalised, ensuring that their needs are reflected in the objectives. The System Operator's main goal is to manage and maintain payment and settlement systems with high trust and confidence while maintaining flexibility for future adaptations.

## FMI Standard 22: Communication Procedures and Standards

### Assessment

#### ESAS Complies with Standard 22

- 1) **The operator must ensure that the FMI uses relevant internationally accepted communication procedures and standards.**

The operator ensures that the FMI uses internationally accepted communication procedures and standards by integrating SWIFT protocols and implementing the ISO 20022 messaging standard, which enhances payment processing and settlement efficiency. Payment instructions are primarily fed into ESAS via feeder systems such as NZClear, ESI, and SBI, or entered manually through the ESAS User Interface.

The majority of ESAS transactions, by volume and value, are transmitted via ESI using the Y-Copy service, ensuring that settlement occurs within ESAS before the payment instruction is released to the counterparty. This secure system uses internationally recognised communication protocols set by SWIFT and operates within a closed user group administered by the RBNZ.

To further enhance efficiency and compliance, ESI will be upgraded in early 2025 to support the new ISO 20022 standard, as mandated by SWIFT. This upgrade will ensure the same or better functionality for Accountholders compared to the existing SWIFT messaging standard. Similarly, the SBI operates using the FileAct Y-Copy service, ensuring net obligations for batched retail payments are settled in ESAS before being processed by the counterparty. Both proprietary and ISO 20022 XML messaging are supported by SBI, with access controlled by PNZ.

Manual entry of payment instructions into ESAS through the user interface follows the same stringent message standards as SWIFT, ensuring consistency across all communication channels. The System Operator has robust procedures in place to accommodate changes in connectivity protocols, whether standardised or commercial, and established processes ensure that downstream users and dependent applications are notified promptly of any changes.

This comprehensive approach ensures that ESAS maintains a high level of reliability, security, and compliance with internationally accepted communication procedures and standards, positioning it to meet evolving regulatory and market demands.

## 5. List of publicly available resources

Document	Reference
ESAS Rules	<a href="https://www.rbnz.govt.nz/-/media/project/sites/rbnz/files/payments/esas/esas-rules.pdf">https://www.rbnz.govt.nz/-/media/project/sites/rbnz/files/payments/esas/esas-rules.pdf</a>
Overview of ESAS	<a href="https://www.rbnz.govt.nz/payments-and-settlement-systems/exchange-settlements-account-system/esas-overview">https://www.rbnz.govt.nz/payments-and-settlement-systems/exchange-settlements-account-system/esas-overview</a>
Annual Report for ESAS - 2025	<a href="https://www.rbnz.govt.nz/payments-and-settlement-systems/exchange-settlements-account-system/esas-members#bAQJLm3vi0OFFu0XIGGtjg">https://www.rbnz.govt.nz/payments-and-settlement-systems/exchange-settlements-account-system/esas-members#bAQJLm3vi0OFFu0XIGGtjg</a>
Financial Markets Infrastructures Act Designation Notice (ESAS) 2023 (the ESAS Designation Notice)	<a href="https://www.rbnz.govt.nz/-/media/project/sites/rbnz/files/regulation-and-supervision/financial-market-infrastructure-oversight/esas-fmia-designation-notice-signed.pdf">https://www.rbnz.govt.nz/-/media/project/sites/rbnz/files/regulation-and-supervision/financial-market-infrastructure-oversight/esas-fmia-designation-notice-signed.pdf</a>
ESAS Access Criteria	<a href="https://www.rbnz.govt.nz/payments-and-settlement-systems/exchange-settlements-account-system/esas-overview">https://www.rbnz.govt.nz/payments-and-settlement-systems/exchange-settlements-account-system/esas-overview</a>