

Dr Alan Bollard  
The Governor  
Reserve Bank of New Zealand  
PO Box 2498  
WELLINGTON

9 October 2009

Dear Dr Bollard

**Auditors' Report to the Reserve Bank of New Zealand**

**Scope**

We have audited the internal controls in relation to the Austraclear system (Austraclear) for the quarter ended 30 September 2009, in order to express an opinion about their effectiveness. The Reserve Bank of New Zealand (RBNZ) is responsible for maintaining an effective internal control structure including controls in relation to the Austraclear system.

In accordance with Rule 19 of Austraclear Rules, our audit included:

- Reviewing the integrity of Austraclear, including the maintenance of security and confidentiality over the data of individual members
- Assessing the integrity of systems-generated information, including controls over the input, processing, accounting and reporting of all transaction data
- Reviewing reconciliation of securities recorded in the respective registry records
- Reviewing and evaluating internal controls and accounting procedures of the Austraclear New Zealand System.

**Basis of Opinion**

An audit includes examining on a test basis, evidence relevant to making an assessment of the internal control environment of Austraclear and securities held in that system in accordance with Rule 19.

Our examination includes the following procedures designed to account for securities lodged with RBNZ:

- Conducted at least once per quarter:
  - sample confirmation of member balances

- Conducted periodically:
  - review and evaluation of the system control and accounting procedures of Austraclear
  - audit examination of specific transactions processed by Austraclear
  - review of IT security and recoverability of Austraclear computer systems.

We have conducted our audit in accordance with New Zealand Auditing Standard No. 404 *Audit Considerations Relating to Entities Using Service Organisations* and with reference to Australian Auditing Guidance Statement No. 1042 *Reporting on Control Procedures at Outsourcing Entities* (AGS 1042). We planned and performed our audit so as to obtain all the information and explanations we considered necessary to provide us with sufficient evidence to give reasonable assurance that the assessment of the internal control environment of Austraclear and securities held within that system, are free from material misstatement whether caused by fraud or error.

#### **Inherent limitations**

Because of inherent limitations in any internal control structure, fraud, error, or non-compliance with laws and regulations may occur and not be detected. Also, projections of any evaluation of the internal controls to future periods are subject to the risk that the internal controls may become inadequate because of changes in conditions, or that the degree of compliance with the control procedures may deteriorate.

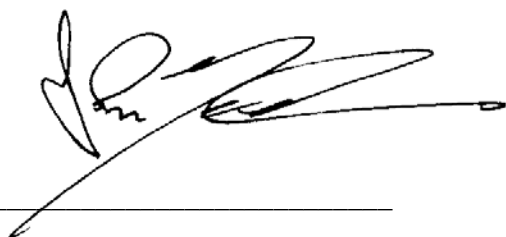
The audit opinion expressed in this report has been formed on the above basis.

#### **Unqualified opinion**

We have obtained all the information and explanations we have required.

In our opinion, RBNZ maintained, in all material respects, the control procedures identified in the accompanying description, which were suitably designed to provide reasonable, but not absolute, assurance that the internal control objectives were achieved and the control procedures operated effectively and continuously for the period 1 July 2009 to 30 September 2009.

Our audit was completed on 2 October 2009 and our unqualified opinion is expressed as at that date.



John Meehan  
PricewaterhouseCoopers  
On behalf of the Auditor-General  
Wellington, New Zealand

**Austraclear Description of Risks, Control Objectives, Policies and Procedures**

System Risks	Control Objectives	Key Controls
<b>Security</b>		
<p>Security is insufficient to prevent unauthorised or inappropriate activity that may compromise the integrity, availability or confidentiality of the systems.</p>	<p>Security management procedures and policies are adequate.</p>	<ul style="list-style-type: none"> <li>• Information Security Guidelines are in place</li> <li>• IT roles and responsibilities are defined in formal position descriptions</li> <li>• A System Requirements form must be approved by the Payment and Settlement Services Team Leader, Manager - Payment and Settlement Services or another senior team member for setting up new users</li> <li>• Procedures are in place to authorise all changes to security parameters</li> <li>• All new Reserve Bank employees are involved in an induction process informing the new staff member about information technology and security in the business and their responsibilities</li> <li>• Austraclear audit trails are reviewed on a reactive basis as required.</li> </ul>

System Risks	Control Objectives	Key Controls
	RBNZ internal and external network is adequately secured.	<ul style="list-style-type: none"> <li>• Before a router is installed at an account holder and before access is granted to the Austraclear / ESAS network, the account holder must complete and agree to the Austraclear Rules in the New Member application pack</li> <li>• Network addressing and access control lists on the routers ensure that account holders can only gain limited access to the Bank systems</li> <li>• Host based Intrusion Detection System and guards capture and analyse traffic across the Austraclear network</li> <li>• Account holders are unable to change the configuration of routers as the consoles are password protected</li> <li>• Network activity is reviewed on a daily basis using Site Protector Console</li> <li>• Network security is reviewed regularly</li> <li>• Internet access is restricted using firewalls, routers and secure tokens.</li> </ul>
	Access to system privileges within the underlying operating system is adequately secured.	<ul style="list-style-type: none"> <li>• Access to system privileges at the operating system level requires manager approval</li> <li>• Operating system access is commensurate with the users' role</li> <li>• Administrative access is appropriately restricted.</li> </ul>
	Adequate data integrity controls are in place to prevent compromise at the database level.	<ul style="list-style-type: none"> <li>• Access to system privileges at the database level requires manager approval</li> <li>• Access is commensurate with the role of each user</li> <li>• Administrative access is appropriately restricted.</li> </ul>

System Risks	Control Objectives	Key Controls
	<p>Austraclear functionality is only available to appropriate users at appropriate levels.</p>	<ul style="list-style-type: none"> <li>• Group profiles are used to restrict users to specific roles. Roles are aligned to users' requirements</li> <li>• User access rights within the Bank (outside the Financial Services Group) are reviewed regularly to ensure that these are appropriate</li> <li>• Dormant user accounts are removed on a regular basis</li> <li>• User access rights available to members is restricted to accessing their own information.</li> </ul>
	<p>Austraclear application security controls are adequate.</p>	<p>The following Austraclear system controls are in place:</p> <ul style="list-style-type: none"> <li>• Minimum password length</li> <li>• Passwords complexity</li> <li>• Lock out from the system once the number of incorrect login attempts have been reached. Only system administrators are able to reactivate the user accounts</li> <li>• Password expiration intervals</li> <li>• Use of previous passwords is restricted</li> <li>• Concurrent logins are restricted.</li> </ul>
<p>Inadequate environmental and physical security controls are in place to prevent system outages.</p>	<p>Adequate environmental and physical security controls are in place over computing equipment.</p>	<ul style="list-style-type: none"> <li>• Access to the server room is restricted to authorised personnel</li> <li>• Environmental controls are in place in the server room, including: <ul style="list-style-type: none"> <li>◦ dual air conditioning units</li> <li>◦ raised floor</li> <li>◦ dry pipe sprinkler system</li> <li>◦ fire extinguisher just outside server room door</li> <li>◦ fire alarms</li> <li>◦ racks for all equipment</li> <li>◦ all servers and computer facilities in the server room are supported by dual UPS in the event of a power disruption.</li> </ul> </li> </ul>

System Risks	Control Objectives	Key Controls
<b>Application Controls</b>		
Additions, changes and deletions to member details are performed incorrectly.	Authorisation is obtained for all additions, changes and deletions to member details.	<ul style="list-style-type: none"> <li>• All potential new members are assessed for eligibility prior to being accepted as an Austraclear member</li> <li>• Approval for new members is required from the Manager Austraclear New Zealand and Chief Financial Officer</li> <li>• If a change is to a member's bank account number, RBNZ Austraclear personnel will only act if a deposit slip or confirmation from the member is received</li> <li>• A request for deletion must be authorised by the member.</li> </ul>
	Additions, changes and deletions to member details are correctly input into the system.	<ul style="list-style-type: none"> <li>• A documentation checklist is completed to confirm that all of the required forms have been received</li> <li>• A new or change member checklist is completed for all new members and changes in membership details</li> <li>• Access is updated as part of additions and changes to member details.</li> </ul>
	Errors in recording member details are identified and corrected in a timely manner.	<ul style="list-style-type: none"> <li>• Additions, deletions and changes to member details in the Austraclear system are subject to a peer review process.</li> </ul>
Lodgements and uplifts of securities are not performed in accordance with authorised instructions received.	All lodgements and uplifts from the various registries into Austraclear are authorised.	<ul style="list-style-type: none"> <li>• Processes and procedures are documented</li> <li>• Security transfer forms must be authorised before a lodge or uplift can be executed.</li> </ul>
	Lodgements and uplifts are reconciled back to instructions received.	<ul style="list-style-type: none"> <li>• Staff are required to sign-off lodgements and uplifts once they are processed</li> <li>• A daily report is checked for all lodges and uplifts.</li> </ul>
	Errors in performing lodgements and uplifts are identified and corrected in a timely manner.	<ul style="list-style-type: none"> <li>• All reconciliations are independently reviewed</li> <li>• All reconciliation issues are followed up immediately.</li> </ul>

System Risks	Control Objectives	Key Controls
Corporate actions are not performed in accordance with authorised instructions received.	All corporate actions are appropriately authorised.	<ul style="list-style-type: none"> <li>Processes and procedures are documented</li> <li>All corporate actions are independently reviewed.</li> </ul>
	Corporate actions are reconciled back to instructions received.	<ul style="list-style-type: none"> <li>Check-sheets are completed for all corporate actions</li> <li>A second person is responsible for checking the diary of actions and corporate action files</li> <li>Documentation is scanned and retained in Documentum.</li> </ul>
	Errors in performing corporate actions are identified and corrected in a timely manner.	<ul style="list-style-type: none"> <li>All corporate actions are independently reviewed.</li> </ul>
The registry details of securities held in Austraclear are incorrect.	Member account balances reconcile with the Austraclear system.	<ul style="list-style-type: none"> <li>Quarterly confirmation of a sample of member holdings.</li> </ul>
	Austraclear is reconciled with holdings in various registries under NZCSD.	<ul style="list-style-type: none"> <li>Daily (or weekly for a small number of securities) reconciliation between the number of securities in the Austraclear system and those held in various registries under the name of NZCSD</li> <li>Reconciliations are checked by an Austraclear team member and discrepancies are dealt with immediately</li> <li>Reconciliations are reviewed by senior management on a weekly basis to review completion and nature of any occurring problems.</li> </ul>
<b>Change Control</b>		
Unauthorised, unreliable or untested changes are migrated into the production environment, resulting in system performance issues.	All changes migrated into production are authorised.	<ul style="list-style-type: none"> <li>Documented change control procedures are in place that require authorisation by multiple persons for all changes</li> <li>System logs capture changes to the production environment</li> <li>A central database is in place to record all change requests</li> <li>Initial authorisation and implementation authorisation include assessment of priority, impact and risk.</li> </ul>
	All changes migrated into production are reliable and tested.	<ul style="list-style-type: none"> <li>All changes are tested and authorised prior to implementation</li> <li>Separate development, test and production environments are used</li> <li>A segregation of duties exists, a user with access to the development or test environment cannot make changes to production</li> <li>All emergency changes are tested before implementation,</li> </ul>

System Risks	Control Objectives	Key Controls
		<ul style="list-style-type: none"> <li>unless approved by senior management</li> <li>• Back-out plans are prepared for all changes prior to migration.</li> </ul>
	All changes are appropriately reviewed prior to implementation.	<ul style="list-style-type: none"> <li>• Changes are peer reviewed and authorised by multiple parties before implementation</li> <li>• Processes are in place to detect failed and unauthorised changes on a timely basis</li> <li>• Third party vendors are monitored to ensure they have procedures in place, and that the procedures are followed.</li> </ul>
	Emergency changes are authorised prior to implementation.	<ul style="list-style-type: none"> <li>• All emergency changes are tested before implementation, unless approved by senior management</li> <li>• Emergency changes are authorised before implementation</li> <li>• First Aid (a defined user account for the migration of emergency changes) log is authorised and documented for all emergency changes.</li> </ul>
System failure due to RBNZ failing to proactively manage the system.	RBNZ monitors and manages the Austraclear system.	<ul style="list-style-type: none"> <li>• Austraclear Operations Checklists are used to monitor file-system usage, backup success, disk space, journal archives and other key metrics</li> <li>• Automatic alerts are paged to support personnel when the system self-diagnoses unexpected conditions.</li> </ul>
<b>Problem Management</b>		
Problems within the system are not identified and in sufficient time to avoid system impacts.	Problems are identified and resolved in a timely manner.	<ul style="list-style-type: none"> <li>• A PPM (proactive problem management form) document is completed for each problem encountered, outlining a description of the problem, consequences of the problem, cause of the problem and the actions taken to remedy the problem</li> <li>• All problems are subject to review by the Chief Financial Officer</li> <li>• Specific actions are taken to resolve problems and prevent recurrence</li> <li>• PPM processes and procedures are documented.</li> </ul>

System Risks	Control Objectives	Key Controls
<b>Backup and Recovery</b>		
Processes and procedures for system backups and file recovery are inadequate.	Adequate processes and procedures are in place for system backups.	<ul style="list-style-type: none"> <li>System backup and operator procedures are in place and adhered to</li> <li>Daily backups are performed.</li> </ul>
	Adequate processes are in place for system and file recovery.	<ul style="list-style-type: none"> <li>File and system restoration processes and procedures are in place and adhered to</li> <li>Regular tests of file and system restoration are undertaken.</li> </ul>
	Processing power is protected.	<ul style="list-style-type: none"> <li>UPS for all critical systems are maintained and tested on a regular basis</li> <li>Backup power generators are available and tested on a regular basis.</li> </ul>
	Disaster recovery provisions are in place.	<ul style="list-style-type: none"> <li>Technically trained persons are available for restoration of systems</li> <li>Redundant equipment (including a full hot site) is available for restoration purposes.</li> </ul>
Recovery of business operations is not possible in a timely manner.	Business operations can be recovered within acceptable timeframes.	<ul style="list-style-type: none"> <li>An up-to-date business continuity plan is in place</li> <li>Austraclear operations can be resumed from alternating sites (Wellington and Auckland) if required</li> <li>The Bank alternates production processing on a regular basis, between Auckland and Wellington.</li> </ul>
<b>SLA Monitoring and Management</b>		
Service level agreements in place with Datacom and third parties are not complied with.	Service level agreement compliance is monitored and managed.	<ul style="list-style-type: none"> <li>An SLA is in place between Datacom and the Reserve Bank for the management of the Austraclear / ESAS environment</li> <li>A monthly meeting is held between the Reserve Bank and Datacom to discuss any issues with the environment and ensure compliance with the agreement</li> <li>Datacom provide monthly reports detailing any issues during the month and reporting against KPIs as detailed in the SLA</li> <li>Processes are in place to monitor Datacom adherence to required processes and procedures.</li> </ul>

System Risks	Control Objectives	Key Controls
<b>Period End Processing</b>		
End of day processing is not complete, accurate or timely.	End of day processing is complete, accurate and timely.	<ul style="list-style-type: none"> <li>• End of day processing is automated</li> <li>• KSG Operations perform online monitoring of processing</li> <li>• Austraclear Operations Checklists are completed on a daily basis to ensure that all operational activities are performed as required.</li> </ul>
<b>Transaction Integrity</b>		
Member account balances or transactions are incorrect.	Member account balances within Austraclear are correct.	<ul style="list-style-type: none"> <li>• Quarterly confirmation of a sample of member holdings.</li> </ul>