New Zealand Clearing and Depository Corporation Limited

2014 Operational Audit

April 2014
This report contains 14 pages

Inherent Limitations

This report has been prepared in accordance with our Engagement Letter dated 31 January 2014. The services provided under our engagement letter ('Services') have not been undertaken in accordance with any auditing, review or assurance standards. The term "Audit/Review" used in this report does not relate to an Audit/Review as defined under professional assurance standards.

The information presented in this report is based on information provided by New Zealand Clearing Corporation and Depository Limited. We have indicated within this report the sources of the information provided. Unless otherwise stated in this report, we have relied upon the truth, accuracy and completeness of any information provided or made available to us in connection with the Services without independently verifying it.

No warranty of completeness, accuracy or reliability is given in relation to the statements and representations made by, and the information and documentation provided by, New Zealand Clearing Corporation and Depository Limited consulted as part of the process.

KPMG is under no obligation in any circumstance to update this report, in either oral or written form, for events occurring after the report has been issued in final form.

Third Party Reliance

This report is solely for the purpose set out in Section 2 of this report and for New Zealand Clearing Corporation and Depository Limited information, and is not to be used for any other purpose or copied, distributed or quoted whether in whole or in part to any other party without KPMG's prior written consent.

Other than our responsibility to New Zealand Clearing Corporation and Depository Limited, neither KPMG nor any member or employee of KPMG undertakes responsibility arising in any way from reliance placed by a third party on this report. Any reliance placed is that party's sole responsibility.

Internal Controls

Due to the inherent limitations of any internal control structure it is possible that errors or irregularities may occur and not be detected. Our procedures were not designed to detect all weaknesses in control procedures as they are not performed continuously throughout the period and the tests performed are on a sample basis. As such, except to the extent of sample testing performed, it is not possible to express an opinion on the effectiveness of the internal control structure.

Contents

1 Executive summary

Scope

As set out in our engagement letter dated 31 January 2014, the scope of our engagement was to evaluate certain operating activities of New Zealand Clearing and Depository Corporation (NZClearingCorp) with respect to the:

- settlement system
- compliance monitoring framework
- operational capability.

Overall observation

The processes and controls over the monitoring of participants, calculation of risk capital, and other operational areas are appropriate and robust. We have identified certain weaknesses in the IT control environment that supports the settlement system. The majority of these findings were identified in previous years (refer Section 5 of this report).

Management have agreed with our findings and have put in place plans to address the identified issues.

All other recommendations made last year regarding the compliance monitoring framework and operational capability areas have been addressed.

Summary of findings

Settlement System

We identified the following control deficiencies relating to the settlement system:

- The change management system does not enforce the requirement that users are not authorised to approve their own change requests. However, it is important to note that our testing did not identify any instances where this occurred.
- Processes for adding, modifying and terminating user access are informal and evidence of management approval is not retained.
- There is no active monitoring of security incidents. NZClearingCorp has implemented a project to address this which is due for completion in 2014.
- NZClearingCorp has undertaken a number of external reviews during 2013 to identify and remediate security threats.
- NZX IT staff are able to access the application database directly. This access is not logged or monitored.
- There is no formal test schedule to ensure that backup restores have not been tested throughout the year.

Compliance monitoring framework

No deficiencies noted.

Operational capability

No deficiencies noted.

2 Scope of our engagement

As set out in our engagement letter dated 31 January 2014 our scope was to evaluate certain operating activities of NZClearingCorp in respect of the:

- settlement system
- compliance framework
- operational capability.

The specific areas that we have evaluated are detailed below:

Settlement System

- Check all change requests have been authorised, tested, and approved for release to production by approved people.
- Check all password settings meet latest industry standards.
- Check all user access additions, modifications, and deletions are supported by the user's role and employment status.
- Check security monitoring controls are working.
- Check user access restrictions to data are working.
- Check that backups/restores have been successful.
- Check user access to the job scheduler is supported by the user's role and that scheduling errors have been addressed and resolved.
- Inspect the design of physical security of IT hardware located at the Telecom data centres.

Compliance monitoring framework

- Check that participant risk profiles have been calculated in accordance with the requirements of the Clearing and Settlement Rules and Procedures.
- Check that participant inspections have been carried out in accordance with the schedule of inspections required under the Clearing and Settlement Rules and Procedures.
- Select three participants and check that the spot and on-site inspection records have been performed in accordance with NZClearingCorp's inspection memoire template.
- Select three participants and check whether the compliance records for each participant have been obtained in accordance with the requirements of the Clearing and Settlement Rules and Procedures.

Operational capability

- Check that risk capital has been calculated in accordance with the Risk Capital Policy.
- Inspect the procedures for determining margins and obtaining collateral and check whether the procedures have been performed in accordance with the Clearing and Settlement Rules and Procedures.
- Identify financial resources held by NZClearingCorp and report on whether these resources are invested in accordance with the Treasury Policy and Investment Policy.

- Identify key operating areas where NZX provides secondment services and check that there are agreements in place for the service.
- Identify insurance policies and check that they are up to date and cover the activities of NZClearingCorp.

3 Findings and recommendations

The tables below summarise the findings and recommendations identified during our review.

3.1 Settlement system

Procedure	Findings/Comments	Recommendations	Risk[1]	Management response
Check all change requests have been authorised, tested and approved for release to production by approved people.	• All changes tested were authorised, tested and approved for release into production by approved people. • NZClearingCorp policy requires all changes to be approved by someone other than the change requestor. However, the change system does not enforce this policy. Our testing did not identify any instances where changes were approved by the same person who requested the change.	• Implement system controls within the change system to require the approver of a change to be a different user than the person who requested the change.	Low	Functionality requested from 3rd party provider. Process and spot checks on the control are being used in the interim.
Check all password settings meet latest industry standards.	• All password settings meet latest industry standards.	*None*	*n/a*	*None*
Check all user access additions, modifications, and deletions are supported by the user's role and employment status.	• There is no evidence to support management approval of user additions, modifications, and deletions. This approval is given verbally. • Access reviews are performed on an annual basis. • We identified one terminated employee whose access had not been revoked in a timely manner. Their account remained active for two months after their termination date.	• Document all additions, modifications, and deletions and require manager sign-off before access is granted. • Implement a formal process where Human Resources inform the administrator of all NZClearingCorp terminations.	Low	All approvals will be required in writing and a copy maintained. The BaNCS administrator will be added to the HR termination form distribution list.

[1] Refer to Appendix 1 for description of risk ratings.

Procedure	Findings/Comments	Recommendations	Risk[1]	Management response
Check security monitoring controls are working.	• Appropriate network controls are in place to prevent unauthorised access (e.g. firewall, anti-virus). • NZClearingCorp have had a number of external security reviews throughout the year to identify and remediate security weaknesses. • Firewall logs are generated but not reviewed. • Processes to actively monitor security events have been implemented during 2013 and continue to be further refined and embedded. NZClearingCorp has a project in place to enhance their security monitoring controls. This is expected to be completed during 2014.	• Further develop processes to actively monitor security events. We are aware that NZClearingCorp has a project in place to address this issue.	Medium	During 2013 considerable additional real time monitoring has been put in place. This provides a single view across all of the Clearing system logs for functionality such as: • batch processing logs • scheduler logs • web logs • application logs • messaging session control logs • report logs • database logs. During 2013 the database was upgraded and additional security features enabled: • Permissible network policies – locking where the database will accept connections from. • Passwords changed to over 20 characters, 131-bit randomly generated keys with mixed case and numbers. • Auditing on login enabled and monitored for failed attempts with appropriate notifications on each occurrence. Firewall logs will be added to the monitoring tool.

Procedure	Findings/Comments	Recommendations	Risk[1]	Management response
Check user access restrictions to data are working.	• BaNCS application access is restricted to appropriate personnel. • One TCS user had "super user" access to BaNCS throughout the year. This access was revoked on 17 December 2013. • There is one generic user account which is set up for disaster recovery purposes. Logs indicate that this account was accessed eight times during the year. • NZX IT staff have direct data access via a generic account. Direct data access is not monitored.	• Implement a periodic review of the generic user accounts to obtain explanations as to their use. • Direct access to the application database should be logged and regularly reviewed.	Low	The right to set up new users is already restricted to the minimum number of personnel practical to ensure that someone is always available to provide appropriate support to the participant network. Use of the generic user account and direct access to BaNCS will be logged and reviewed.
Check that backups/restores have been successful.	• Backups are performed on a daily basis. • Backup restores to the test environment have been performed on an ad-hoc basis. • There is no backup testing schedule to ensure that backup testing is performed on a regular basis.	• Establish a backup testing schedule where restores are tested at least annually.	Low	Numerous restores of production backups off network storage to the test environment have occurred. Testing of restores from offsite media has not been implemented to date but will undergo annual testing in future.
Check user access to the job scheduler is supported by the user's role and that scheduling errors have been addressed and resolved.	• Access to the job scheduler is restricted to appropriate personnel. • Alert triggers are in place to ensure that job processing errors are investigated and resolved in a timely manner.	*None*	*n/a*	*None*
Inspect the design of physical security of IT hardware located at the third party data centres.	• Appropriate controls are in place to restrict access to IT hardware located at third party data centres.	*None*	*n/a*	*None*

3.2 Compliance monitoring framework

Procedure	Findings/Comments	Recommendations	Risk	Management response
Check that participant risk profiles have been calculated in accordance with the requirements of the Clearing and Settlement Rules and Procedures.	• A standard template has been used to document the participants risk profile. The methodology contained in the template captures the requirements of the Clearing and Settlement Rules and Procedures.	*None*	*n/a*	*None*
Check that participant inspections have been carried out in accordance with the schedule of inspections required under the Clearing and Settlement Rules and Procedures.	• NZClearingCorp has undertaken inspections for all participants during 2013.	*None*	*n/a*	*None*

Procedure	Findings/Comments	Recommendations	Risk	Management response
Select three participants and check that the spot and on-site inspection records have been performed in accordance with NZClearingCorp's inspection template.	• The participant inspection records tested showed that on-site inspection records have been performed in accordance with NZClearingCorp's inspection template. • Participant inspections have been designed to ensure that the participant has complied with NZX and Clearing and Settlement Rules and Procedures. • The inspection process is clearly documented. Review of these documents, and participant inspection files, evidences a risk based approach is applied. Risk profiles are updated and reviewed prior to each inspection. Participants are assessed to determine the likelihood of non-compliance for each obligation. These results drive customisation of the inspection template to capture the obligations that present the greatest risk of non-compliance. • Rules that require ongoing compliance are also mapped to the inspection template. The result is an inspection template that incorporates both a risk based approach, as well as other necessary compliance tasks.	*None*	*n/a*	*None*
Select three participants and check whether the compliance records for each participant have been obtained in accordance with the requirements of the Clearing and Settlement Rules and Procedures.	• In all cases the participant provided the compliance records required by the Clearing and Settlement Rules and Procedures. There were isolated cases where the required records were not obtained all at the same time, however these were identified and remediated in a timely manner.	*None*	*n/a*	*None*

3.3 Operational capability

Procedure	Findings/Comments	Recommendations	Risk	Management response
Check that risk capital has been calculated in accordance with the Risk Capital Policy	• The Risk Capital Policy and estimated risk capital calculations were updated in March 2013. The policy has been reviewed by the Board and provided to the regulators. • In April 2013, NZX agreed to increase the standby capital commitment provided to NZClearingCorp by $5 million, taking the total available risk capital to $20 million. This increase was required to take into account the actual and expected increase in trading volumes. • The methodology for determining estimated risk capital is based on the minimum industry standard of default by the participant with the largest historic exposure. Additional stress conditions are applied to determine the estimated risk capital. The assumptions and inputs into the risk capital calculation are conservative. • Estimated risk capital has been stress tested for 2013 and 2014 based on three different scenarios. Under all scenarios the actual risk capital was greater than the stressed risk capital.	*None*	*n/a*	*None*
Inspect the procedures for determining margins and obtaining collateral and check whether the procedures have been performed in accordance with the Clearing and Settlement Rules and Procedures.	• The margining procedures, including the margin calculation and notification to participants, have been performed in accordance with the Clearing and Settlement Rules and Procedures. • The collection of collateral, including collateral form, minimum levels, delivery and returns, have been performed in accordance with the Clearing and Settlement Rules and Procedures.	*None*	*n/a*	*None*

Procedure	Findings/Comments	Recommendations	Risk	Management response
Identify financial resources held by NZClearingCorp and report on whether these resources are invested in accordance with the Treasury Policy and Investment Policy.	• The financial investments at 31 December 2013 have been made in accordance with the Treasury Policy and Investment Policy. • In particular, we confirmed that investments were made with approved organisations, exposure levels were within set limits, the investment type (e.g. call and term deposits) and duration were in accordance with the policies.	*None*	*n/a*	*None*
Identify key operating areas where NZX provides secondment services and check that there are agreements in place for the service.	• A Secondment Agreement Variation was approved in May 2013 that updated the positions currently seconded to NZClearingCorp. • Employees who are seconded to NZClearingCorp are undertaking risk management, settlements and operational duties for NZClearingCorp. This is consistent with the Secondment Agreement. • The service and infrastructure agreements for the provision of services by NZX cover all key operational activities required by NZClearingCorp.	*None*	*n/a*	*None*
Identify insurance policies and check that they are up to date and cover the activities of NZClearingCorp.	• Insurance policies are taken out by NZX Limited on behalf of its subsidiaries, including NZClearingCorp. • NZClearingCorp has insurance cover for Directors and Officers Liability, Civil Liability, Fidelity and Computer Crime, Statutory Liability, Employers Liability, and General Liability. The level of cover provided is suitable for the activities of NZClearingCorp.	*None*	*n/a*	*None*

4 Prior year recommendations

The table below summarises the progress made against recommendations raised in the 2013 Operational Audit.

Procedure	Prior year recommendation	Status	Risk	Comments
Settlement system				
Check all user access additions, modifications, and deletions are supported by the user's role and employment status.	Ensure application administrators are informed of employee terminations so that access rights can be revoked in a timely manner.	Open	Low	Process for informing the application administrator of employee terminations is informal. We identified one terminated employee whose access was not revoked in a timely manner.
Check security monitoring controls are working.	To meet industry standards, access attempts to BaNCS should be monitored actively. This could be achieved by implementing intrusion detection software and firewall/network level exception alerts. BaNCS should also be routinely monitored for unusual access attempts.	In progress	Medium	NZClearingCorp has implemented a project to address this issue. This work is on-going with security monitoring processes due to be implemented in 2014.
Check user access restrictions to data are working.	The application database should only be accessed by individual user accounts. When a generic user account is used, modifications can only be traced to the generic account, rather than a specific individual. Therefore, generic user access should be removed and replaced by individual user access when accessing the database directly. Access to the application database should be logged and regularly monitored.	Open	Low	Direct data access is not logged or reviewed on a regular basis.
Check that backups/restores have been successful.	Restore procedures should be tested on an annual basis.	Open	Low	Backup restores have been performed to the test environment. However no formal test schedule exists to ensure that testing is performed on a regular basis.

Procedure	Prior year recommendation	Status	Risk	Comments
Check user access to the job scheduler is supported by the user's role and that scheduling errors have been addressed and resolved.	Access to the job scheduler should be made via individual user accounts rather than a generic account.	Closed	n/a	Access to the job scheduler is restricted to appropriate personnel.
Inspect the design of physical security of IT hardware located at the third party data centres.	Require the data hosting vendor to: • lock server rack doors • ensure that visitors sign in and out • actively monitor surveillance over data centre entrances and exits • review access logs on a regular basis.	Closed	n/a	Improvements have been made, in particular all server rack doors were locked.
Compliance monitoring framework				
Select three participants and check that the spot and on-site inspection records have been performed in accordance with NZClearingCorp's inspection template.	A risk based approach is taken to testing non-compliance with the Clearing and Settlement Rules and Procedures during an inspection. A risk assessment for each obligation with which a participant must comply is completed to determine the likelihood and impact of non-compliance. The inspection template is then updated to capture the obligations that present the greatest risk to non-compliance.	Closed	n/a	Review of inspection profiles demonstrate that a risk based approach is applied. Participants are assessed to determine the likelihood of non-compliance for each obligation. These results drive customisation of the inspection template to capture the obligations that present the greatest risk to non-compliance

Procedure	Prior year recommendation	Status	Risk	Comments
Operational capability				
Check that risk capital has been calculated in accordance with the Risk Capital Policy.	The Risk Capital Policy could be improved by clearly stating the combination of scenarios that should be applied and extending the stress testing across future years (currently only performed for 2012). The stress scenarios should also be applied to daily reporting and a system of limits and escalation policies introduced to monitor the stress scenarios.	Closed	n/a	Stress testing has been applied across a two year period. NZClearingCorp decided that extending testing further out than this was of little value due to the uncertainty of future trading volumes and market conditions. Stress scenarios are applied to daily reporting.

Appendix 1: Risk Ratings

Findings identified during the course of the audit are assigned a risk rating, as outlined in the table below. The risk rating is based on the impact the issue identified has on maintenance of an effective internal control environment and management of identified business risks.

Rating	Description
High	The issue represents a control breakdown, which is causing severe disruption of the process or adversely affecting the ability to achieve process objectives. The issue requires immediate management action.
Medium	The issue represents a control weakness, which could have or is having some adverse effect on the ability to achieve process objectives. The issue requires management action within a reasonable time period.
Low	The issue represents a minor control weakness with minimal but reportable impact.