KPMG

cutting through complexity

NZClearingCorp

Auditors report on the operational systems

15 February 2013

10 Customhouse Quay
Wellington
New Zealand

PO Box
Wellington 6140
New Zealand

Telephone +64(4) 816 4500
Fax +64(4) 816 4600
Internet www.kpmg.co.nz

Private and confidential
The Directors
New Zealand Clearing and Depository Corporation Limited
Level, 2 NZX Centre
11 Cable Street
Wellington

15 February 2013

To the Directors

Auditors report in connection with the operational system of New Zealand Clearing and Depository Corporation Limited and its subsidiaries

In accordance with our engagement letter dated 14 January 2013 we have been engaged to report on certain areas in respect of the settlement system, compliance framework and operational capability of the New Zealand Clearing and Depository Corporation Limited and its subsidiaries ("NZClearingCorp") for the year ended 31 December 2012.

As a professional services firm, we are required to comply with various professional standards relating to the performance of particular types of engagements. The services provided in connection with this engagement comprise an advisory engagement, which is not subject to assurance and other standards issued by the New Zealand Institute of Chartered Accountants and, consequently, no opinions or conclusions intended to convey assurance have been expressed. Any reference to 'review' in this report has not been used in the context of a review in accordance with the assurance and other standards issued by the New Zealand Institute of Chartered Accountants.

We received excellent cooperation from the staff and management of NZX Limited and NZClearingCorp during our engagement. Our overall observation is that NZClearingCorp has made improvements to its processes and controls since our previous review in March 2012. However, we identified three key areas where, in our view, further improvements should be made to enhance the operational performance of NZClearingCorp. Our findings and recommendations are summarised on pages 6 to 13 of this report.

Our report is solely for the information of NZClearingCorp and is not to be used by any other person or for any other purpose without our prior written consent. This report relates only to the areas where we are required to report on and does not extend to any other financial information of NZClearingCorp.

We would be very happy to answer questions relating to our report, or provide more information about our review, at your convenience.

Yours sincerely

Godfrey Boyce
Partner

Contents

The contacts at KPMG in connection with this report are:

Godfrey Boyce
Partner
Wellington, New Zealand
Tel: (04) 816 4514
gboyce@kpmg.co.nz

Jonathan Williams
Senior Manager
Wellington, New Zealand
Tel: (04) 816 4736
jonathanwilliams@kpmg.co.nz

Executive summary

Scope of engagement

The scope of our engagement was to evaluate certain operating activities in respect of the:

- settlement system,
- compliance framework, and
- operational capability.

The services provided in connection with this report comprise an advisory engagement and is not subject to assurance and other standards issued by the New Zealand Institute of Chartered Accountants.

No opinions or conclusions intended to convey assurance have been expressed in the report.

Overall observation

Our overall observation is that the quality of processes and controls has improved since our previous review in March 2012.

However, while there has been progress made, we believe there is still scope for improvements.

Key areas for improvement

- There continues to be no active monitoring controls in place over BaNCS for inappropriate or unauthorised access attempts to the system. We recommend that active monitoring of BaNCS is implemented to meet industry standards.
- Participant inspections are carried out to ensure that the participant has complied with the Clearing and Settlement Rules & Procedures. Enhancements to the inspection procedures could be made to improve the process for assessing compliance with the Clearing and Settlement Rules & Procedures.
- We identified three areas where improvements to user access restrictions could be made:
  - One TCS user has “super user” access rights to BaNCS allowing access to the testing and production environments. Access should be limited to “read only” in the production environment.
  - The application database can be modified by a “generic user account”. We recommend this is removed and replaced by individual accounts to improve traceability.
  - User access to the application database is not logged. We recommend that access is logged and monitored on a routine basis.

Other findings & recommendations

- One terminated employee did not have user access rights to BaNCS removed on a timely basis.
- Backups are performed on a daily basis, but no restore testing has been performed during 2012. We recommend restores are tested on an annual basis.
- Access to the job scheduling tool is through a generic user account which limits traceability of users. We recommend individual user accounts are used instead.
- Weaknesses were identified at the third party data centres. These included unlocked server doors, visitors are not required to sign in or out, no monitoring of surveillance over entrances and exits, and no monitoring of access logs.
- Risk capital stress testing has been performed for 2012 only. Stress testing should be extended over future years.
- Escalation procedures and tolerance limits should be set for daily risk capital levels.
- Secondment agreements are out of date. These should be updated to reflect new employees.

Scope of our engagement

Scope of engagement

As set out in our in our engagement letter dated 14 January 2013 our scope was to evaluate certain operating activities of NZClearingCorp in respect of the:

- settlement system,
- compliance framework, and
- operational capability.

The specific areas that we have evaluated are detailed in the boxes opposite.

Advisory engagement

The services provided in connection with this report comprise an advisory engagement and is not subject to assurance and other standards issued by the New Zealand Institute of Chartered Accountants.

Accordingly, no opinions or conclusions intended to convey assurance have been expressed in the report. Any reference to the term "review" has not been used in the context of a review in accordance with assurance and other standards issued by the New Zealand Institute of Chartered Accountants.

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 third party data centres.

Compliance framework

- Check that participant risk profiles have been calculated in accordance with the requirements of the Clearing and Settlement Rules & Procedures.
- Check that participant inspections have been carried out in accordance with the schedule of inspections required under the Clearing and Settlement Rules & 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 & 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 & 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.

Key areas for improvement

Overall observation

Our overall observation of the areas covered by this review is that the quality of processes and controls has improved since our previous review in March 2012. However, while there has been progress made, we believe there is still scope for improvements. We have identified the following three key areas for development:

- ***Security monitoring***

  There continues to be no active monitoring controls in place over BaNCS for inappropriate or unauthorised access attempts to the system. In our view, the industry benchmark requires systems such as BaNCS to be actively monitored by implementing intrusion detection software and firewall/network exception alerts. These are not currently in place. Furthermore, there is no routine monitoring for unusual access attempts.

  We recommend that active monitoring of BaNCS is implemented. We would also like to highlight that this recommendation has been carried forward from our March 2012 review. In that review management responded that they will " work with [a third party provider] to identify network monitoring options" but no further action has been taken at this stage.

- ***Participant inspections***

  Participant inspections have been carried out in order to ensure that the participant has complied with the Clearing and Settlement Rules & Procedures.

  Although inspections are carried out using a standardised inspection template, this does not provide a comprehensive coverage of all obligations that a participant must comply with. Therefore, inspections rely heavily on the knowledge of the inspector to ensure that the participant is complying with the required obligations.

  In our view, a risk based approach should be taken to assess the likelihood and impact of non-compliance with an obligation. The inspection template should then be updated to include obligations that present the greatest risk of non-compliance.

- ***Access restrictions***

  We identified three areas where improvements to user access restrictions could be made.

  - One TCS user has "super user" access rights to BaNCS (but not the application database) which allows modification in both the testing and production environments. Although we agree that TCS should have access to the production environment, this should be restricted to "read only" access.
  - The application database can be modified by a "generic user account". Only the Database Administrators and senior IT members know the password to this account. However, any changes using this account would not be able to be traced to an individual. In our view the generic user access should be removed and replaced by individual user access to improve traceability.
  - User access to the application database is not logged. We recommend that access is logged and monitored on a routine basis.

We have also made a number of other recommendations which we do not consider to be key areas for improvement but would help improve the operational performance of NZClearingCorp. These other recommendations, together with our key recommendations, are set out in the Findings & Recommendations section on pages 6 to 13

Findings & recommendations

Procedure	Findings	Recommendations	Management Response
▪ Check all change requests have been authorised, tested and approved for release to production by approved people.	▪ A new "BaNCS Change Control Management" policy was developed during the year which defines the change lifecycle including testing and authorisation requirements. ▪ Change details, including testing results, are recorded with approvals for release. ▪ All change requests were tested and approved prior to release into the production environment.	▪ None	▪ None
▪ Check all password settings meet latest industry standards.	▪ BaNCS password settings were updated during the year and now align with industry standards. ▪ Passwords are now required to include a combination of upper case letters and numeric characters. ▪ Passwords are now prohibited to re-use the past 12 password settings (previously three passwords).	▪ None	▪ None
▪ Check all user access additions, modifications, and deletions are supported by the user's role and employment status.	▪ New user access and modifications to existing users is initiated by Human Resources and the employee's manager. All access rights were appropriate for the users role and employment status. ▪ We identified one terminated employee whose access rights had not been disabled in BaNCS. The employee had left NZX four weeks earlier. ▪ A review of all user access rights is performed on a quarterly basis.	▪ Ensure application administrators are informed of employee terminations so that access rights can be revoked in a timely manner.	▪ A procedure is in place to revoke access rights for employees on leaving NZX. That procedure was not followed in this case. Further training will be delivered to ensure procedures regarding employee access are correctly followed.

Findings & recommendations

Procedure	Findings	Recommendations	Management response
▪ Check security monitoring controls are working.	▪ There is no active security monitoring controls in place to monitor inappropriate or unauthorised access attempts to BaNCS. ▪ The firewall maintains a log of access attempts, however this is only reviewed retrospectively if required.	▪ 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.	▪ Options available will be investigated in order to provide this capability.

▪ Check user access restrictions to data are working.	▪ User access restrictions to BaNCS and its application database is appropriate for all users, except in the following circumstances:
	  ▪ One TCS user has “super user” access rights to BaNCS (but not the database) which allows modification in both the testing and production environments.
	  ▪ Direct changes to the application database can be made via a generic user account. The password for this account is known only by the Database Administrators and select members of the NZX IT team.
	▪ We also identified that user access to the database is not logged.
		▪ The TCS “super user” should have their access restricted in the BaNCS production environment to “read only”.
		▪ 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.
			▪ TCS production user will be made read only.
			▪ Individuals will have individual DB users set up.
			▪ User access to the database will be logged.

▪ Check that backups/restores have been successful.	▪ Backups are performed on a daily basis and sent off-site at the end of week. ▪ No restores, or testing of restores, have been performed during the year.	▪ Restore procedures should be tested on an annual basis.	▪ Restore procedures will be tested on an annual basis.

Findings & recommendations

Procedure	Findings	Recommendations	Management response
■ 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 scheduling tool is through a generic user account and therefore any actions performed are unable to be traced to an individual user. ■ Email and text message alerts are triggered if an error occurs so that they can be investigated and resolved in a timely manner. ■ A summary report is sent each day to the IT team detailing any job processing errors.	■ Access to the job scheduler should be made via individual user accounts rather than a generic account.	■ NZX will investigate the capability to move to individual user accounts, and implement appropriately.

■ Inspect the design of physical security of IT hardware located at the third party data centres.	■ The following weaknesses were observed at data centre site 1:
	  ■ Server rack doors are not locked.
	  ■ Visitors are not always asked to sign out.
	  ■ Video surveillance is not in place over the data centre door.
	  ■ Access logs are not frequently reviewed.
	■ The following weaknesses were observed at data centre site 2:
	  ■ Video surveillance on the entrances and exits to the data centre is not actively monitored.
		■ 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.
			■ Data centre site 1 will follow the data centre site 2 practice of ensuring racks are locked.
			■ Third party data centre will be requested to ensure all visitors are signed in and out, and active monitoring of access ways is put in place.
			■ Third party data centre will be requested on a 6 monthly basis for log reviews.

Findings & recommendations

Procedure	Findings	Recommendations	Management response
▪ Check that participant risk profiles have been calculated in accordance with the requirements of the Clearing and Settlement Rules & Procedures.	▪ A standard template is used to document the participants risk profile. The methodology contained in the template captures the requirements of the Clearing and Depository Rules & Procedures ▪ Participant profiles selected had been updated during 2012 and the profile completed in accordance with the methodology.	▪ None	▪ 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 2012.	▪ None	▪ None
▪ Select three participants and check that the spot and on-site inspection records have been performed in accordance with NZClearingCorp's inspection template.	▪ The objective of an inspection is to ensure that the participant has complied with NZX and Clearing and Settlement Rules & Procedures. ▪ An inspections template, setting out the testing procedures, has been developed in-house by NZX and has been used on the inspections that we reviewed. The template is linked back to some obligations of the Clearing and Settlement Rules & Procedures, however it does not provide comprehensive coverage for all rules and procedures that a participant must comply with. A full assessment of non-compliance therefore relies on the inspector having a detailed knowledge of the rules and procedures. ▪ A new compliance analyst was employed at the end of 2012. We understand that his role is to develop comprehensive inspection programmes in order to ensure that inspections cover all relevant Clearing and Settlement Rules & Procedures . We believe this will strengthen the identification of non-compliance by a participant.	▪ A risk based approach is taken to testing non-compliance with the Clearing and Settlement Rules & Procedures during an inspection. A risk assessment for each obligation that a participant must comply with 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.	▪ A risk based approach to inspection is currently used. The documentation of this approach and the process of identification of risks for each participant will be strengthened.

Findings & recommendations

Procedure	Findings	Recommendations	Management response
■ 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 & Procedures.	■ In the majority of cases the participant provided the compliance records required by the Clearing and Settlement Rules & Procedures. There were isolated cases where the required records were not obtained, however these appear to be minor oversights rather than a systematic failure to obtain the required records.	■ None	■ None

Findings & recommendations

Procedure	Findings	Recommendations	Management response
■ Check that risk capital has been calculated in accordance with the Risk Capital Policy	■ The Risk Capital Policy and estimated risk capital calculation was updated in October 2012. Although these have been reviewed by the NZClearingCorp Risk Committee, they have not been reviewed or approved by the board. ■ 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. ■ The estimated risk capital for 2012 and 2013 was lower than actual risk capital available despite the conservative nature of the calculations. Risk capital had been calculated in accordance with the Risk Capital Policy. ■ Estimated risk capital has been stress tested for 2012 based on four different scenarios. Under all scenarios the actual risk capital was greater than the stressed risk capital. No stress testing has been performed for 2013. ■ The risk capital is calculated on a daily basis and reported to the Head of Operations. Stress scenarios are also calculated. However, there is no system of limits or escalation procedures in the event that risk capital increases beyond set amounts.	■ 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.	■ The risk capital policy is currently being updated and the revised version will incorporate this recommendation. ■ Multiple scenarios are examined in current daily reporting. Once the risk capital policy has been approved, daily reporting will be updated to ensure it remains appropriate. ■ Escalation limits will be reviewed by the Board.

Findings & recommendations

Procedure	Findings	Recommendations	Management response
▪ 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 & Procedures.	▪ The margining procedures, including the margin calculation and notification to participants, have been performed in accordance with the Clearing and Settlement Rules & Procedures ▪ The collection of collateral, including collateral form, minimum levels, delivery and returns, have been performed in accordance with the Clearing and Settlement Rules & Procedures	▪ None	▪ None
▪ 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 2012 have been made in accordance with the Investment and Treasury Policies. Investments were made with approved organisations, exposure levels were within set limits, and the investment type (e.g. call and term deposits) and duration were in accordance with the policies.	▪ None	▪ None
▪ Identify key operating areas where NZX provides secondment services and check that there are agreements in place for the service.	▪ The secondment agreement was entered into in 2010. Each secondment was initially for a period of two years, however this period has now passed without it being updated. ▪ The secondment agreement has not been updated for new employees or those who have departed NZX. ▪ Employees who are seconded to NZClearingCorp (or their replacement if they have left NZX) 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.	▪ Update the secondment agreement to reflect employee changes.	▪ The secondment agreement will be reviewed with NZX and updated as necessary.

Findings and recommendations

Procedure	Findings	Recommendations	Management response
▪ 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	▪ None