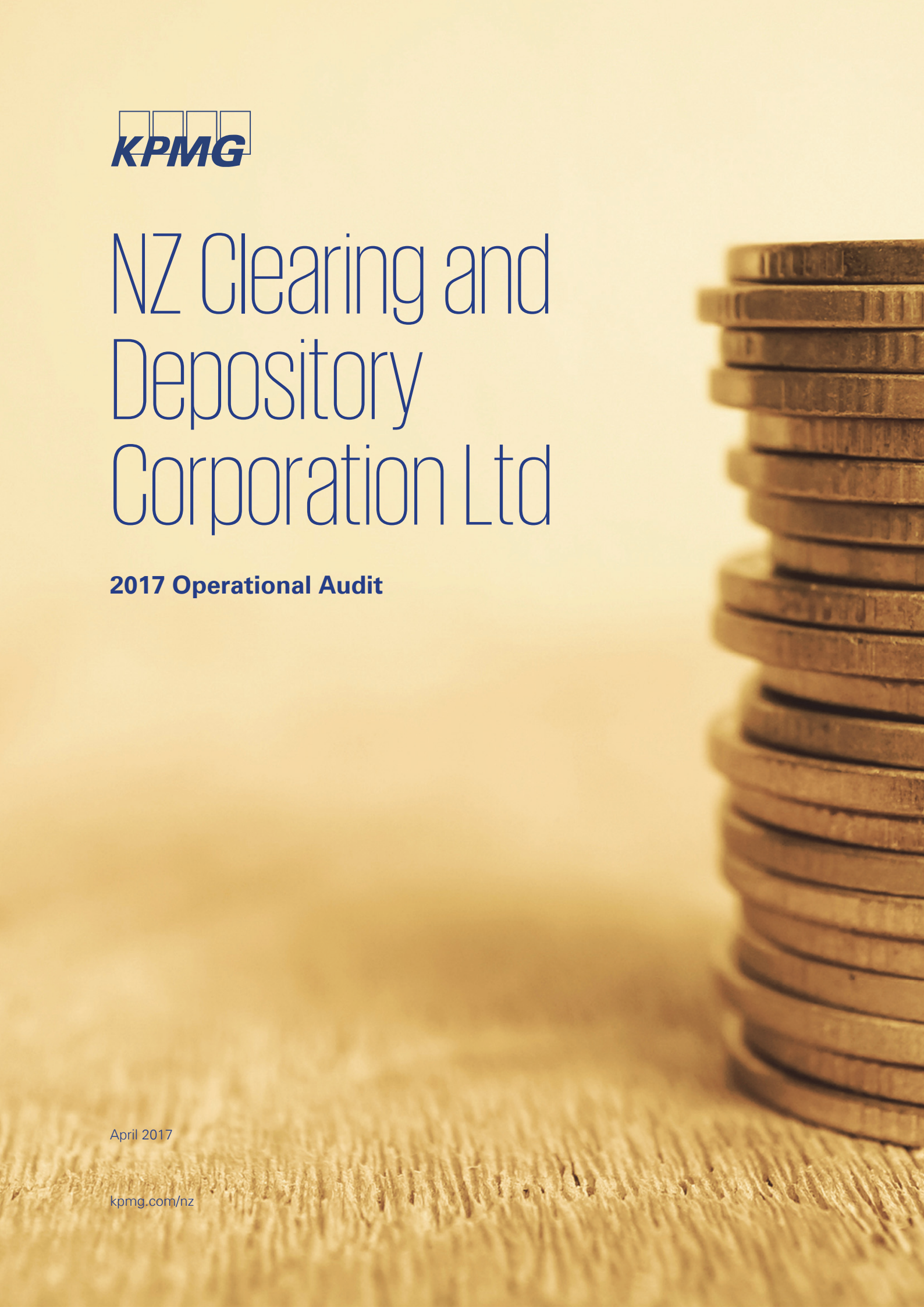

NZ Clearing and Depository Corporation Ltd

2017 Operational Audit

April 2017

kpmg.com/nz

Contents

Inherent Limitations

This report has been prepared in accordance with our Engagement Letter dated 16 December 2016. 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's 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.

1 Executive Summary

As set out in our engagement letter dated 16 December 2016, we have evaluated certain operating activities of New Zealand Clearing and Depository Corporation (NZCDC) with respect to the:

- Settlement system
- Compliance monitoring framework
- Operational capability.

Overall observation

The processes and controls over monitoring of participants and other operational areas are robust. However, we identified some weaknesses in the IT control environment that supports the settlement system (BaNCS).

Summary of findings

Settlement System

Appropriate controls were in place over the settlement system. We identified one medium risk finding, and one low risk findings, which when addressed will strengthen the security and integrity of the settlement system. These are:

Finding	Risk rating
— The user passwords for any BaNCS account can be found out through viewing the password table. — Any of the 20+ users with access to a specific database have access to view the password table.	Medium
— We identified a number of generic administrative accounts. As these accounts are not assigned to any specific individuals, when they are used it is not possible to identify who used it. Access to two separate accounts was shared between the two database administrators.	Low

Compliance monitoring framework

The compliance monitoring framework has been appropriately applied throughout 2016. All participants had reviews based on their risk scores.

Operational capability

The assumptions used in the calculation for modelling potential losses are conservative and are consistent with better market practices.

Other operational areas tested were found to be in compliance with NZCDC policy requirements.

2 Scope of our engagement

As set out in our engagement letter dated 16 December 2016, our scope was to evaluate certain operating activities of NZCDC in respect of the:

- settlement system
- compliance framework
- operational capability.

The scope of our work included the following areas of NZCDC:

Settlement system

- Check that:
  - password management processes are robust
  - the provision and revocation of access is undertaken in a structured manner
  - administrative access to systems is limited and based on business needs
  - changes to the system are authorised, tested and approved for release to production
  - the system is supported by a robust disaster recovery plan
  - a structured backup and recovery process is in place, and aligns with the disaster recovery plan
  - patches are applied on a timely basis
  - a robust vulnerability management process is in place to identify and resolve vulnerabilities
  - incidents impacting the system are managed by a structured incident management process
  - third party access to the system is restricted
  - 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 Spark Digital 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
  - 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 NZCDC's inspection memoire template
  - 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:
  - the underlying assumptions used to perform the risk capital calculation are in accordance with the Risk Capital Policy and better practice
    Note: we have not tested the model used to perform the calculation; we have only reviewed that the assumptions are in line with policy.
  - the procedures for determining margins and obtaining collateral have been performed in accordance with the Clearing and Settlement Rules and Procedures
  - financial resources held by NZCDC are invested in accordance with the Treasury Policy and Investment Policy
  - agreements are in place for key operating areas where NZX provides services to NZCDC
  - insurance policies are up to date and cover the activities of NZCDC.

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 that password management processes are robust.	— The user passwords for any BaNCS account can be found out through viewing the password table. Any of the 20+ users having access to a specific role within a specific database have access to view the password table. This would enable the user to perform activities assigned to someone else through the privileges granted to them. The impact of this is limited to what actually can be done using those privileges, which in BaNCS is not of serious operational concern.	— Management should ensure that the user passwords are securely stored in the system by implementing a password encryption or hashing mechanism.	Medium	— User passwords in BaNCS v7 will be hashed (using 'DES crypt'). BaNCS v7 is scheduled to go live in late June.
Check that the provision and revocation of access is undertaken in a structured manner.	— A formal process exists for the provisioning of user access at application level.	N/A	N/A	N/A
Check that administrative access to systems is limited and based on business needs.	— We identified a number of generic administrative accounts. As these accounts are not assigned to any specific individuals, when they are used it is not possible to identify who used it. — Access to two separate accounts was shared between the two database administrators.	— Usage of default or generic accounts should be discontinued and individual accounts should be created for each user.	Low	— NZX will switch to named users with admin privileges where practicable. However, some generic admin accounts are required due to the functions that account type can perform.

Procedure	Findings/Comments	Recommendations	Risk[1]	Management response
		— Formal ownerships should be established for the default admin accounts, and their passwords securely stored through an appropriate mechanism. — Users should have individual accounts that are unique and provide accountability in line with best practises.		
	— Two accounts that were no longer required were not disabled at the time of our review. — These accounts have since been disabled on the system.	N/A	N/A	N/A
Check that changes to the system are authorised, tested and approved for release to production.	— All changes tested were appropriately authorised for release into production.	N/A	N/A	N/A
Check that the system is supported by a robust disaster recovery plan.	— A full disaster recovery test was done comprehensively as supported by the business run sheets.	N/A	N/A	N/A
Check that a structured backup and recovery process is in place, and aligns with the disaster recovery plan.	— Backups are successfully managed by Eagle Technology. Comvault Technology has been implemented to modernise the backup process. — We noted that during the disaster recovery test, data restoration was performed.	N/A	N/A	N/A
Check that patches are applied on a timely basis.	— There is a process in place to identify and apply system patches on a timely basis.	N/A	N/A	N/A

Procedure	Findings/Comments	Recommendations	Risk[1]	Management response
Check that a robust vulnerability management process is in place to identify and resolve vulnerabilities.	— Firewall activity is logged on a daily basis. An application called Smart Viewer is used to monitor live activity. — NZX has implemented a heuristic learning engine to manage cybersecurity-related events. Monthly reporting of all security incidents is undertaken.	N/A	N/A	N/A
Check that incidents impacting the system are managed by a structured incident management process.	— There is a structured process in place to manage incidents impacting the system.	N/A	N/A	N/A
Check that third party access to the system is restricted.	— Access by third parties is managed and strictly controlled.	N/A	N/A	N/A
Check that 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.	N/A	N/A	N/A
Inspect the design of physical security of IT hardware located at the Spark Digital data centres.	— Access to the Auckland and Wellington data centres is managed effectively. — Environmental controls are well designed and operating effectively within the data centres.	N/A	N/A	N/A

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.	N/A	N/A	N/A
Check that participant inspections have been carried out in accordance with the schedule of inspections required under the Clearing and Settlement Rules and Procedures.	— NZCDC has undertaken all planned inspections for participants during 2016.	N/A	N/A	N/A
Select three participants and check that the spot and on-site inspection records have been performed in accordance with NZCDC's inspection memoire template.	— The participant inspection records tested showed that on-site inspection records have been performed in accordance with the 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 evidences that a risk based approach is applied prior to each inspection, and detailed risk profiles are updated at the time of onsite inspections.	N/A	N/A	N/A

Procedure	Findings/Comments	Recommendations	Risk	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 and Procedures.	— We reviewed the records held for each of the selected participants and confirmed that compliance records were in accordance with the Clearing and Settlement Rules and Procedures.	N/A	N/A	N/A

3.4 Operational capability

Procedure	Findings/Comments	Recommendations	Risk	Management response
Check that the underlying assumptions used to perform the risk capital calculation are in accordance with the Risk Capital Policy and better practice.	— The assumptions used in the calculation are in accordance with the Risk Capital Policy and consistent with market practices for modelling potential losses. — The methodology for determining estimated risk capital requirements is based on modelled losses caused by the default of market participants during a period of extreme market movements. — The defaulted participant positions are based on the largest historic exposure increased by future growth assumptions. Additional stress conditions are applied to determine the estimated risk capital requirement.	N/A	N/A	N/A
Check that the procedures for determining margins and obtaining collateral 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.	N/A	N/A	N/A
Check that financial resources held by NZCDC are invested in accordance with the Treasury Policy and Investment Policy.	— NZ Clearing's risk capital and cash collateral received is placed on call and in term deposits in accordance with the Treasury Policy and the Investment Policy.	N/A	N/A	N/A
Check that there are agreements in place for key operating areas where NZX provides secondment services.	— Service, Infrastructure and Employee Secondment agreements are in place for the provision of services by NZX and cover all key operational activities required by NZCDC.	N/A	N/A	N/A

Procedure	Findings/Comments	Recommendations	Risk	Management response
	— There have been no significant changes to the operations for NZCDC requiring amendments to the agreements.			
Check that insurance policies are up to date and cover the activities of NZCDC.	— Insurance policies are taken out by NZX Limited on behalf of its subsidiaries, including NZCDC. — The NZX Board receives a report from the Broker regarding insurance options every year. The Board discusses and agrees the level of cover on an annual basis. — The insurance cover for Directors and Officers Liability, Directors and Officers Costs and Expenses Liability, Statutory Liability, Employers Liability, Public and Products Liability has been renewed for twelve months.	N/A	N/A	N/A

4 Prior Year Recommendations

The table below summarises the progress made against recommendations raised in the 2016 Operational Audit.

Procedure	Recommendations	Status	Risk	2017 Update
Settlement System				
Checked that password management processes are robust.	— That insecure protocols be disabled and only TLS 1 and above be used for improved security.	Closed	N/A	The recommendation has been implemented, and no further findings were identified in the 2017 Operational audit.
Checked that administrative access to systems is limited and based on business needs.	— To implement a user access review process for all systems to periodically review user access rights within the systems at all levels.	Open	Low	This recommendation is still open as we identified a number of generic administrative accounts with no clear ownership and traceability of usage.
Checked that third party access to the system is restricted.	— To implement strict monitoring controls for the TCS account. Access should be granted on a needs basis, supported by an access request notification detailing need for access and time period. — To disable the TCS account when not in use.	Closed	N/A	No findings were identified in the 2017 Operational audit. Monitoring controls have been implemented for the use of the TCS account.
Inspected the design of physical security of IT hardware located at the Spark Digital data centres.	— That security areas should always remain restricted in the absence of security personnel. Strict control measures should be implemented — That fire hazard equipment be removed from the server room. — That security cameras at reception be covered for security reasons.	Closed	N/A	No findings were noted during the 2017 Operational audit review of data centres.

Procedure	Recommendations	Status	Risk	2017 Update
Selected three participants and checked whether the compliance records for each participant had been obtained in accordance with the requirements of the Clearing and Settlement Rules and Procedures.	— To amend the checklist to clearly separate out each certificate within the review process. — To ensure electronic files are correctly labelled, and scan hard copy documents to minimise the risk of losing information.	Closed	N/A	No findings were identified in the 2017 Operational audit. The revised checklist identifies required documents individually. Documents are stored electronically and no missing information was identified in the completing of compliance testing.

Appendix A 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.

Contact us

David Sutton
Partner,
Advisory
T (09) 367 5844
E davidsutton@kpmg.co.nz

Greg Davies
Senior Manager
Advisory
T (04) 816 4808
E gregdavies@kpmg.com

kpmg.com/nz