



ASAE 3402

Assurance Report on Controls at a Service Organisation relating to the Austraclear System

1 JULY 2020 – 30 JUNE 2021



Contents

1.	Assertion by Management	3
2.	Independent Assurance Report	5
3.	Introduction	8
4.	Overview of the ASX Group	9
5.	Overall Control Environment	10
6.	Overview of Austraclear	12
7.	Use and Scope of the Report	14
8.	Control Objectives and Related Control Procedures	16



01 / Statement by ASX as the Service Organisation

The information provided by ASX management in this report has been prepared for participants who have used Austraclear (formerly known as EXIGO) (participants) and their auditors who have a sufficient understanding to consider the description, along with other information (including information about controls operated by participants themselves), when assessing the risks of material misstatement of participant's financial reports / statements. ASX confirms:

- (a) The accompanying description in Sections 5, 6 and 8 fairly presents Austraclear for processing participant's transactions throughout the period 1 July 2020 to 30 June 2021.

The criteria used in making this statement were that the accompanying description:

- (i) presents how the system was designed and implemented, including:
- the types of services provided including, as appropriate, classes of transactions processed
 - the procedures, within both information technology and manual systems, by which those transactions were initiated, recorded, processed, corrected as necessary, and transferred to the reports prepared for participants
 - the related accounting records, supporting information and specific accounts that were used to initiate, record, process and report transactions; this includes the correction of incorrect information and how information was transferred to the reports prepared for participants
 - how the system dealt with significant events and conditions, other than transactions
 - the process used to prepare reports for participants
 - relevant control objectives and controls designed to achieve those objectives
 - controls that ASX assumed, in the design of the system, would be implemented by participants, and which, if necessary to achieve control objectives stated in the accompanying description, are identified in the description along with the specific control objectives that cannot be achieved by ASX alone, and
 - other aspects of the ASX control environment, risk assessment process, information system (including the related business processes) and communication, control activities and monitoring controls that were relevant to processing and reporting participants' transactions.
- (ii) includes relevant details of changes to Austraclear during the period 1 July 2020 to 30 June 2021, and
- (iii) does not omit or distort information relevant to the scope of the system being described, while acknowledging that the description is prepared to meet the common needs of a broad range of participants and their auditors and may not, therefore, include every aspect of the system that each individual participant may consider important in its own particular environment.

- (b) The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period 1 July 2020 to 30 June 2021. The criteria used in making this statement were that:

- (i) the risks that threatened achievement of the control objectives stated in the description were identified
- (ii) the identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved and



- (iii) the controls were consistently applied as designed, including that manual controls were applied by individuals who have the appropriate competence and authority, throughout the period 1 July 2020 to 30 June 2021.

- (c) In response to the COVID-19 pandemic and in accordance with Government and other expert advice, ASX transitioned to a hybrid operating model with the majority of personnel working remotely full or part time, including some responsible for transaction processing and operational support of the Austraclear system. There has been no material change to the control environment, including the design and operating effectiveness of the controls listed in section 8 of this report, as a result of this change.

Signed on behalf of management

DocuSigned by:
Val Mathews
C3D74511705146C...

Val Mathews

Chief Customer and Operating Officer

27 July 2021



02 / Independent Service Auditor's assurance report on the description of controls, their design and operating effectiveness

To: Directors of ASX Limited (ASX)

Scope

In accordance with the terms of the engagement letter dated 17 December 2020, we were engaged to report on ASX Limited's description in Sections 5, 6 and 8 of its Austraclear system (System) for processing Participant's transactions throughout the period 1 July 2020 to 30 June 2021 (the description), and on the design and operation of controls related to the control objectives stated in the description.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls contemplated in the design of ASX's controls are suitably designed and operating effectively, along with related controls at the service organisation. We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

ASX's Responsibilities

ASX is responsible for preparing the description and accompanying statement in Section 1, including the completeness, accuracy and method of presentation of the description and statement; providing the services covered by the description; stating the control objectives; and designing, implementing and effectively operating controls to achieve the stated control objectives.

Our Independence and Quality Control

We have complied with relevant ethical requirements related to assurance engagements, which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

The firm applies Auditing Standard ASQC 1 *Quality Control for Firms that Perform Audits and Reviews of Financial Reports and Other Financial Information, Other Assurance Engagements and Related Services Engagements* and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.



Service Auditor's Responsibilities

Our responsibility is to express an opinion on ASX's description and on the design and operation of controls related to the control objectives stated in that description, based on our procedures. We conducted our engagement in accordance with Standard on Assurance Engagements ASAE 3402 *Assurance Reports on Controls at a Service Organisation (ASAE 3402)*, issued by the Auditing and Assurance Standards Board. That standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented and the controls are suitably designed and operating effectively.

An assurance engagement to report on the description, design and operating effectiveness of controls at a service organisation involves performing procedures to obtain evidence about the disclosures in the service organisation's description of its System, and the design and operating effectiveness of controls. The procedures selected depend on our judgement, including the assessment of the risks that the description is not fairly presented, and that controls are not suitably designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the objectives stated therein, and the suitability of the criteria specified by the service organisation and described in Section 1.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Limitations of Controls at a Service Organisation

ASX's description is prepared to meet the common needs of a broad range of Participants and their auditors and may not, therefore, include every aspect of the System that each individual Participant may consider important in its own particular environment. In addition to this, because of their nature, controls at a service organisation may not prevent or detect all errors or omissions in processing or reporting transactions. Further, the projection of any evaluation of effectiveness to future periods is subject to the risk that controls at a service organisation may become inadequate or fail.

Opinion

Our opinion has been formed on the basis of the matters outlined in this report. The criteria we used in forming our opinion are those described in ASX's statement in Section 1. In our opinion, provided Participants have applied the complementary user entity controls contemplated in the design of ASX's System and those controls were operating effectively, in all material respects:

- (a) The description fairly presents the System as designed and implemented throughout the period from 1 July 2020 to 30 June 2021.
- (b) The controls related to the control objectives stated in the description were suitably designed throughout the period from 1 July 2020 to 30 June 2021.
- (c) The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period from 1 July 2020 to 30 June 2021.

PricewaterhouseCoopers, ABN 52 780 433 757

One International Towers Sydney, Watermans Quay, Barangaroo NSW 2000, GPO BOX 2650 Sydney NSW 2001

T: +61 2 8266 0000, F: +61 2 8266 9999, www.pwc.com.au

Level 11, 1PSQ, 169 Macquarie Street, Parramatta NSW 2150, PO Box 1155 Parramatta NSW 2124

T: +61 2 9659 2476, F: +61 2 8266 9999, www.pwc.com.au



Description of Tests of Controls

The specific controls tested and the nature, timing and results of those tests are listed in Section 8.

Intended Users and Purpose of the report

This report and the description of tests of controls in Section 8 are intended only for Participants who have used ASX's System and their auditors, who have sufficient understanding to consider it, along with other information including information about controls operated by Participants themselves, when assessing the risks of material misstatements of Participant's financial reports / statements.

This report is prepared only for the purpose set out above and we disclaim any liability in relation to our report or any assumption of responsibility for any reliance on our report to any person other than ASX, Participants who have used ASX's System and their auditors or for any purpose other than that for which it was prepared.

PricewaterhouseCoopers

DocuSigned by:
Corinne Best
11E86C4F3C634B7...

Corinne Best

Partner

Sydney

27 July 2021



03 / Introduction

Austraclear Limited is a wholly-owned subsidiary of ASX Limited, the holding company of the ASX Group. The securities settlement facility operated by Austraclear Limited is known as the Austraclear system.

ASX management is responsible for the design, implementation and maintenance of the internal control procedures and for the declarations and assertions in this report. In carrying out this responsibility, management has regard to the interests of participants, the general effectiveness of the operation of Austraclear, and the overall stability of the Australian financial system.

This report has been prepared to provide:

- an overview of the ASX Group
- an overview of Austraclear and its role in the clearing and settlement process
- a summary of ASX's corporate governance arrangements relating to the Austraclear operating environment
- the control objectives and control procedures that underpin the Austraclear control environment, and
- the independent auditor's report on the control objectives and procedures.

The report has been prepared in compliance with *ASAE 3402 Assurance Reports on Controls at a Service Organisation*.



04 / Overview of the ASX Group

ASX is an integrated exchange offering listings, trading, clearing, settlement, technical and information services, and other post-trade services. It operates markets for a wide range of asset classes including equities, fixed income, commodities and energy and is a top 10 global securities exchange by value and the largest interest rate derivatives market in Asia.

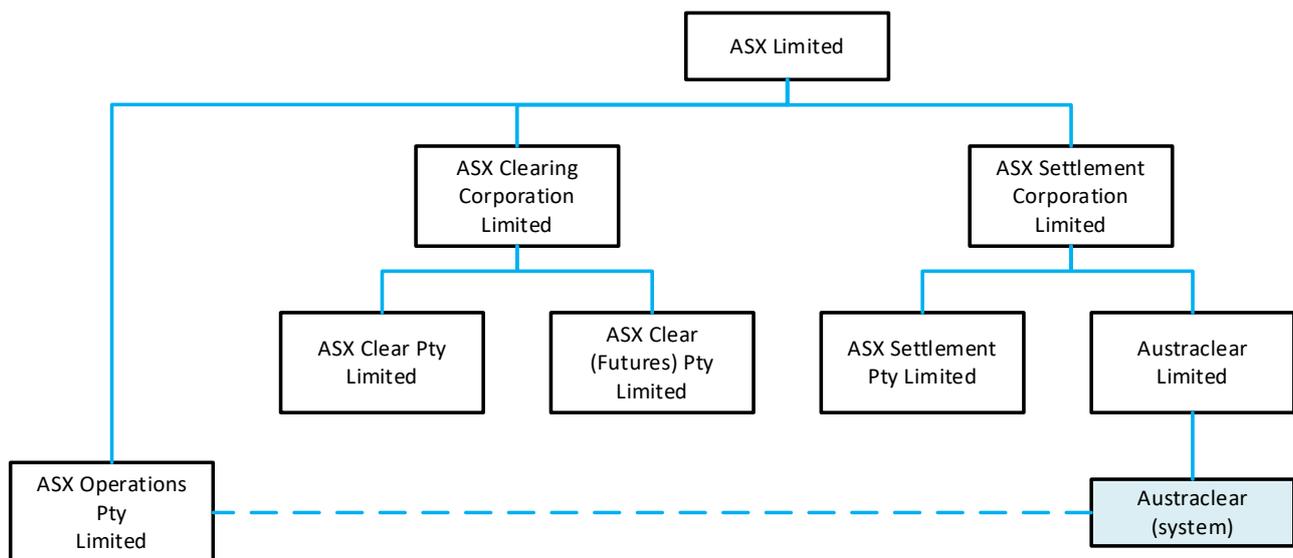
Companies, corporates and issuers of capital from Australia and around the world engage with ASX to manage risk and to raise capital to grow. ASX operates liquid, transparent and reliable markets of integrity. The certainty of its clearing and settlement activities helps to underpin the systemic stability of the Australian economy.

ASX also provides data and technology services to intermediaries, banks, information vendors and software developers to help them make informed decisions, offer services to their clients and connect with one another.

More information about ASX can be found at: www2.asx.com.au.

Structure

Relevant parts of the ASX Group structure, including the responsibility for the Austraclear system, are depicted below:





05 / Overall Control Environment

Corporate Governance

The control environment within which ASX operates Austraclear is not restricted to the control objectives and procedures outlined in this report.

The ASX Group maintains a high standard of corporate governance and has implemented governance arrangements which are consistent with the ASX Corporate Governance Council's Corporate Governance Principles and Recommendations (4th Edition). An overview of those components of ASX's corporate governance framework which are relevant to the operation of Austraclear is set out below. More information on ASX's corporate governance framework is available on ASX's website and in its Annual Report.

Austraclear is operated by ASX Operations Pty Limited, a wholly-owned ASX Group subsidiary, to fulfil the settlement functions of Austraclear Limited, a clearing and settlement facility licensee. It is one of four clearing and settlement facility licensees in the ASX Group.

The ASX Board relies on the Clearing and Settlement Boards to provide oversight of the clearing and settlement operations of the clearing and settlement subsidiaries including, the management of clearing and settlement risk, and compliance with the Financial Stability Standards determined by the Reserve Bank of Australia (RBA). The Clearing and Settlement Boards' Charter sets out further details regarding their functions and governance.

ASX Limited has established an Audit and Risk Committee (ARC) (comprising independent, non-executive directors of ASX Limited). The ARC also serves as the audit and risk committee of ASX's Clearing and Settlement Boards (including Austraclear).

The following Committees (comprised of Senior Management) also form an integral part of the overall control environment in which Austraclear operates:

- Risk Committee
- Regulatory Committee, and
- Technology, Operations and Security Committee.

The system of internal control and risk management is reviewed by Internal Audit. The General Manager of Internal Audit reports to the Chair of ARC, and to the Chief Risk Officer for administrative purposes. The General Manager Internal Audit presents an Internal Audit Plan and quarterly audit findings to the ARC.

In addition, ASX's Enterprise Compliance function conducts oversight of the ASX Group and provides quarterly reports to the ARC on compliance with key licence obligations.

Charters of the ASX Board, Clearing and Settlement Boards, ARC and Internal Audit are available on ASX's website: www2.asx.com.au.



Regulatory Governance

Licensed entities in the ASX Group are subject to review by ASIC and the RBA.

Operational Governance

The primary divisions that have direct control over the operational governance of Austraclear are Operations and Technology.

Operations is responsible for the day to day processing of trading, clearing and settlement transactions. The Austraclear operational environment includes processes and controls in the following areas:

- transaction processing
- error resolution and escalation, and
- security and operational resilience.

Operations is headed by the Chief Customer and Operating Officer of ASX.

Technology is responsible for the IT support and development of Austraclear. The control environment in operation within Technology includes the following processes and controls areas:

- system operations
- change management
- security, and
- system resilience.

Technology is headed by the Group Executive Technology and Data and Chief Information Officer of ASX.

Logical access

ASX has an established enterprise-wide identity and access management policy that is available to all staff. A centralised Identity and Access Management team is responsible for the implementation and operation of controls relating to user maintenance (i.e. provisioning, changing and de-activating accounts including remote access), password management and the performance of user access reviews for the ASX network, application software, operating systems and databases relevant to Austraclear. In addition, ASX maintains documented procedures and network security mechanisms for the prevention, detection and remediation of a malicious attack.

Change management

Changes relating to Austraclear follow the enterprise-wide change management process that requires all changes to be logged in a centralised IT Service Management tool and approved, tested and monitored through the change life cycle. The process requires all changes to be assessed and signed off by the relevant Technology, Business and Change Approval Board (CAB) representatives prior to implementation, with the exception of those changes designated as standard changes. Standard changes are pre-authorised by the CAB and are very low risk changes that are well understood, repeatable and fully documented in an approved standard template. System and user documentation is updated, as appropriate, for each completed change.

Emergency changes also follow a defined and approved process, however, due to the nature of an emergency change, verbal or email approvals are obtained prior to implementation. Emergency changes may only be initiated if there is a corresponding incident ticket in the ITSM tool. Testing and formal approvals are performed as soon as practical following the change.



ASX maintains separate development, test and production environments for Austraclear as well as segregation of duties between development and production migration and support activities.

Physical security

In addition to the head office in the CBD, there are two data centres – a primary data centre managed by ASX, and a secondary vendor-managed data centre (SDC). The SDC has dedicated and secured areas for ASX infrastructure, office space and control room, over which ASX maintains direct control of physical security. As such, the data centre provider is not considered a sub-service organisation for the purpose of this report.

ASX implements and operates physical security controls at both data centres to ensure access to these data centres is limited to authorised personnel. The controls include access provisioning and removal, regular review of physical access, as well as established policies and procedures, electronic and biometric security devices and CCTV.

Environmental controls

There are environmental control mechanisms in place at both data centres. These are maintained on a regular basis to facilitate continued operation of the systems. Maintenance activities for the primary data centre are managed by ASX, while the vendor manages the maintenance for the SDC. ASX monitors the completion of the maintenance per an agreed schedule.

Disaster recovery

ASX operates using a dual site model for all key operational and technology functions, with one operational site (also the primary data centre) outside of the Sydney CBD and the SDC approximately 30km from the CBD. ASX maintains a Business Continuity Framework and dedicated plan for each key business unit, including those operating Austraclear. A Disaster Recovery (DR) plan is in place for the system with testing conducted annually to ensure the system redundancy, secondary services and fail-over processes remain current and operational, and the system is able to meet the targeted 2 hour recovery timeframe.

In addition, all ASX staff have the ability to work remotely, however some job functions may require an element of physical access to technology assets. Remote access is secured using multi-factor authentication.

IT processing

The following provides a summary of the other key technology processes relating to Austraclear:

- **System backup:** Austraclear application data is replicated to the secondary data centre. In addition, a regular backup cycle exists with tapes stored in an offsite facility by a specialist third party.
- **System monitoring:** There is automated monitoring in place for key functions and processing to support the operational integrity of the system with exception reporting and alerting to the relevant support teams for issues and failures. Network capacity, performance incidents, operational incidents and system availability is monitored and reported to management on a monthly basis.
- **Job scheduling:** A number of job schedules exist that are key to the successful processing of transactions in Austraclear. The status of the batch processes is monitored to ensure they are successfully completed. Changes to the schedules require approval prior to being implemented.



06 / Overview of Austraclear

Austraclear Limited operates a securities settlement facility and central securities depository (CSD) for debt securities traded in the OTC market. The CSD provides settlement and depository services for a wide range of financial instruments, including fixed income securities, foreign exchange confirmations and short-dated money market instruments (bills, certificates of deposits and promissory notes).

Austraclear offers participants true delivery versus payment, exchanging cash for securities irrevocably and in real-time via a process called Delivery versus Payment (DvP).

Austraclear also provides a real time cash transfer facility which enables payments to and from ASX's central counterparties, including margin payments relating to derivative and futures positions and transactions relating to ASX's collateral management service.

Austraclear authorises participants such as banks, custodians, institutional investors, settlement agents and others to access Austraclear and settle trades made by themselves or on behalf of their clients.

CSD functions include a full range of registry, issuing and payment services for all corporate actions over a security's lifecycle.

Austraclear also offers settlement services for foreign currency payments, currently covering payments denominated in Chinese renminbi (RMB) and US dollars (USD). The services are segregated from Austraclear's Australian dollar (AUD) services.

Other services include Euroentitlements and Issuing and Paying Agency (IPA).

The Euroentitlement service gives participants access to investment grade A\$ denominated securities deposited with international CSDs (e.g. Clearstream). It allows participants to settle A\$ denominated Eurobonds within Austraclear in the same manner as a domestic security.

Austraclear Limited, via its IPA service, can undertake for issuers, the full range of corporate actions relating to the life cycle of a security, from origination to maturity. Actions include deposit/lodgement of securities, payments, coupon and maturity payments and the transfer of ownership.

ASX Collateral is a tri-party collateral management service that provides a flexible, scalable solution to efficiently collateralise exposures across a range of A\$ products. The automated service uses proven asset optimisation algorithms and integrates directly with ASX's Austraclear system to ensure a smooth transition of collateral between collateral givers and takers.

Transaction Processing

Settlement transactions are initiated by either Austraclear participants or ASX by entering a trade in Austraclear. Trades are two sided transactions, matched between the participant and the counterparty to the trade. Each matched transaction will generate a settlement instruction and, when required, a cash payment instruction will be sent to RBA RITS for real time gross settlement and processing through the relevant Exchange Settlement Account with the RBA.

In March 2021, Austraclear linked settlement functionality was made available to participants on an optional basis. This allows them to link a group of eligible transactions in a Linked Settlement Group for simultaneous settlement by transfer of the net amount of cash and securities for all transactions in that group. At this time, linked settlement functionality is offered on a bi-lateral basis only and requires the same two participants to be a party to all transactions in the Linked Settlement Group. Both participants will be required to agree to the Linked Settlement Group for it to proceed to simultaneous settlement.

Austraclear also interfaces with other external applications for accepting transactions (e.g. transactions performed as part of ASX's Collateral Management Service – refer to www2.asx.com.au for additional information).



Processing errors are either flagged by Austraclear or identified by ASX via operational monitoring of the system and transaction reports. Once identified, errors follow a defined escalation path.

The system is available from 6:00am and closes at 7:00pm (9:00pm daylight savings time).

Regulation

Austraclear Limited is a licensed CS facility under the Corporations Act and must comply with the Financial Stability Standards (FSS) published by the RBA. In addition, as a CS facility licensee, it must:

- to the extent that it is reasonably practicable to do so, do all other things necessary to reduce systemic risk
- to the extent that it is reasonably practicable to do so, do all things necessary to ensure that the facility's services are provided in a fair and effective way, and
- have an adequate arrangement for supervising the facility.

Reporting

Austraclear automatically produces a number of reports to participants, including:

- cash reports
- settlement instruction reports (e.g. activity statement, holding statement), and
- holdings reports (issuer and participant).

System Change

During the period, there were changes made to the Austraclear environment as part of usual management and support.

Control Objectives and Control procedures

Set out in this report are the control objectives relevant to the Austraclear system. The controls listed in Section 8 of the report have been designed to achieve each of the control objectives, and any references to the network, application, operating system and database are specific to Austraclear.

Complementary User Entity Controls

Achievement of control objectives 1 and 7 as set out in Section 8 may also be dependent on controls performed by participants as well as controls performed by other related party entities. These are known as Complementary User Entity Controls, or CUECs.

Internal controls, no matter how well designed and operated, can provide only reasonable, not absolute, assurance to management of achieving an entity's objectives. All internal control systems are subject to inherent limitations.

Each participant must evaluate its internal controls to determine if appropriate procedures are in place. In order to rely on the controls in this report, the participant's auditors should consider whether the following CUECs are operating.

Ref	Control Description	Relevant control objectives in section 8
CUEC 1	Participants are responsible for designing and implementing effective user access management controls to their dedicated sub-participant module within Austraclear. Participants should have controls in place to ensure that access requests to the sub-participant module are authorised.	1



Ref	Control Description	Relevant control objectives in section 8
CUEC 2	Participants should have controls in place to ensure that terminated users' access to the sub-participant module are removed in a timely manner.	1
CUEC 3	Participants should have controls in place to ensure that periodic user access review is performed to ensure access to the sub-participant module remains commensurate with job responsibilities. Follow up actions should be completed in a timely manner	1
CUEC 4	Participants should have controls in place to ensure that super user and privileged access to the sub-participant module is restricted and/or monitored	1
CUEC 5	Participants should have controls in place to ensure that remote access to the Austraclear system is monitored. Monitoring tools should be used to identify unusual events. Any deviations identified should be tracked and remediated.	1
CUEC 6	Participants should have controls in place to ensure that network security measures and incident response plans are in place to safeguard against the threat of malicious attack. Security alerts should be tracked and resolved in a timely manner	1
CUEC 7	Participants should perform a regular reconciliation of the ASX provided settlement obligations to their internal records. Where variances are noted, ASX should be notified accordingly for investigation and resolution.	7



07 / Use and Scope of the Report

Requirement for the Report

The requirement for and scope of the independent audit is mandated in the Austraclear Operating Rules (known as the Austraclear Regulations). The following table provides the requirements under section 18 of the Austraclear Regulations.

Rule Ref	Title	Content
18.1	Appointment of Auditor	Austraclear must appoint an auditor who will be responsible for conducting an audit of Austraclear's information technology control environment procedures in relation to the System ("Procedures") on a regular basis.
18.2	Scope of Audit	In conducting an audit of the Procedures, the Auditor must at least ascertain that the Procedures: <ul style="list-style-type: none"> (a) are suitably designed to meet Austraclear's internal control objectives and (b) have operated effectively to provide reasonable assurance that Austraclear's internal objectives were achieved throughout the audit period under review.
18.3	Report by the Auditor	The Auditor must issue an annual report to Austraclear in the prescribed form and within the prescribed time after the financial year end for Austraclear based on the Auditor's latest audit of the Procedures.
18.4	Participant Report by Austraclear	At the request and expense of a Participant, Austraclear will issue a report relating to Securities held in safekeeping by Austraclear in the prescribed form, either to that Participant or as that Participant may direct by notice to Austraclear.
18.5	Rights of access	A Participant, or auditor or other representative of a Participant, has no right of access to or right to sight or inspect: <ul style="list-style-type: none"> (a) any Deposited Securities except by Withdrawing the Security from the System or (b) Austraclear's computer and operational facilities.

The Austraclear Procedures, Determinations and Practice Notes in section 18 provide a description of the form of the report, the timeframe for issuance, the inherent limitations and examples of the internal control procedures that Participants should maintain within their own control environment.

Use of the Report

The report has been prepared for Austraclear Limited to comply with the Austraclear Regulations. It is intended only for participants who have used the Austraclear system and their auditors, who have sufficient understanding to consider it along with other information, including controls operated by the participant themselves, when assessing the risks of material misstatements of participant's financial reports and statements. While Austraclear Limited understands participants may provide the report to external parties, including their own auditors, Austraclear Limited has no knowledge or understanding of the individual circumstances of participants, their auditors, or other external parties.



08 / Control Objectives and Related Control Procedures

The scope in relation to this control report has been defined in the control objectives and associated control procedures for Austraclear that have been included below. Any references made to the network, application, operating system and database are specific to Austraclear.

Logical Access

Control Objective 1: *Controls provide reasonable assurance that logical access is restricted to prevent inappropriate or unauthorised access to the ASX network, application software, operating systems and underlying databases.*

Description of controls	Test performed by PwC	Results
1.1 The ASX Identity and Access Management Policy (the Policy) outlines the principles for restricting access to the network, application software, operating systems and underlying databases. The Policy is available to all staff.	Inspection Verified through inspection that the ASX Identity and Access Management Policy outlines the principles for restricting access to the network, application software, operating systems and underlying data and is available to all staff.	No exception noted.
1.2 Processes are in place for administering access to the network, application software, operating systems and the underlying databases. This includes approval of access granted and the timely termination of accounts no longer required.	Inspection For a sample of new users, verified through inspection that access to the network, application, operating system and database was approved prior to access being granted. Inspection For a sample of user revocations, verified through inspection that access to the network, application, operating system and database was revoked in a timely manner in accordance with the ASX Policy.	No exception noted.



Description of controls	Test performed by PwC	Results
	<p>Observation</p> <p>Verified through onscreen observation that an automated deactivation process is in place to disable terminated staff network access on the last day of service.</p>	
<p>1.3 Access to the application is authenticated and restricted through the use of password controls at the application and network layer. Per the Policy, controls include the following:</p> <ul style="list-style-type: none"> - authentication by a unique user ID and password - system enforced a minimum password length - the requirement to change passwords at predefined intervals, and - the lockout of user accounts after a pre-defined number of invalid sign-in attempts. 	<p>Observation</p> <p>Verified through onscreen observation that access to the application, operating system and database required the use of a user ID and password at the time of testing</p> <p>Inspection</p> <p>Verified through inspection that there are unique user IDs assigned to authenticate to the application, operating system and database at the time of testing.</p> <p>Inspection</p> <p>Verified through inspection at the time of testing that password parameters at the application, operating system and database layer are in line with the ASX Identity and Access Management Policy requirements which include:</p> <ul style="list-style-type: none"> - system enforced a minimum password length - users changing passwords at pre-defined intervals, and - lockout of user accounts after a pre-defined number of invalid sign-in attempts. 	<p>No exception noted.</p>



Description of controls	Test performed by PwC	Results
	<p>Inspection</p> <p>Where the password parameters are not in compliance with the ASX Identity and Access Management Policy requirements, validated through inspection that a current exemption for the deviation exists.</p>	
<p>1.4 Regular user access reviews are performed to confirm currency and appropriateness of access.</p>	<p>Inspection</p> <p>For a sample of application, operating system and database user access reviews, verified through inspection that the reviews were performed to confirm currency and appropriateness of access.</p> <p>Inspection</p> <p>Verified through inspection that all follow up actions resulting from the sampled user access reviews were completed in a timely manner in accordance to ASX Policy.</p>	<p>No exception noted.</p>
<p>1.5 Documented procedures are in place outlining the principles for safeguarding against the threat of malicious attack.</p>	<p>Inspection</p> <p>Verified through inspection of the Security Patching Policy, Malicious Code Management Standard and Cyber Security Escalation Procedure that principles for safeguarding against the threat of malicious attack are outlined.</p> <p>Inspection</p> <p>For a sample of monthly patching meetings, verified through inspection that the available patches are evaluated in line with the Security Patching Policy</p>	<p>No exception noted.</p>



Description of controls	Test performed by PwC	Results
<p>1.6 Network security measures include the following: firewalls, intrusion detection software, anti-virus software and incident response procedures are in place.</p>	<p>Inspection and Observation</p> <p>Verified through inspection of network documentation and onscreen observation that a number of measures including firewalls, intrusion detection software and anti-virus software are in place.</p> <p>Inspection</p> <p>Verified through inspection of the Cyber Security Escalation Procedure and playbooks document that incident response procedures are in place.</p>	<p>No exception noted.</p>
<p>1.7 Remote access to the network, application software, operating system and underlying databases is restricted and further security measures include digital certificates and/or RSA tokens.</p>	<p>Observation</p> <p>Verified through onscreen observation that User IDs and passwords, as well as digital certificates or RSA tokens, are required to access the ASX network remotely.</p> <p>Inspection</p> <p>Verified through inspection of the ASX Mobility and Remote Access Standard that remote access using RSA token is required to be authorised.</p> <p>Inspection</p> <p>For a sample of new remote access granted with the use of RSA tokens, verified through inspection that remote access to the ASX network, application software, operating system and database was authorised in accordance with the standard.</p>	<p>No exception noted.</p>



Description of controls	Test performed by PwC	Results
	<p>Inspection</p> <p>For a sample of user departures with remote access accounts, verified through inspection that remote access was removed in a timely manner.</p>	



Change Management

Control Objective 2: *Controls provide reasonable assurance that all changes relating to the application software, operating system software and underlying databases within the Austraclear production environment are authorised and tested in accordance with the ASX change management policy.*

Description of controls	Test performed by PwC	Results
2.1 Documented change management procedures are in place. All changes and upgrades follow the procedures.	<p>Inspection</p> <p>Verified through inspection that documented change management procedures are in place covering the change lifecycle.</p> <p>Inspection</p> <p>For a sample of changes, verified through inspection that they follow the documented change management procedures.</p>	No exception noted.
2.2 All changes are logged and monitored throughout the life cycle of the change.	<p>Inspection</p> <p>For a sample of changes, verified through inspection that changes were logged and monitored throughout the life cycle of the change.</p>	No exception noted.
2.3 Testing results are recorded, tracked and signed off.	<p>Inspection</p> <p>For a sample of changes, verified through inspection that testing results were recorded, tracked and signed off.</p>	No exception noted.
2.4 Test documentation exists, including test plans / strategies, test cases / criteria, test logs and issue reporting.	<p>Inspection</p> <p>For a sample of changes, verified through inspection that test documentation existed, including test plans / strategies, test cases / criteria, test logs and issue reporting.</p>	No exception noted.



Description of controls	Test performed by PwC	Results
2.5 Changes are subject to levels of system (i.e. developer) and user testing prior to implementation.	<p>Inspection</p> <p>For a sample of changes, verified through inspection of relevant documentation that each change was subject to levels of system and user testing prior to implementation.</p>	No exception noted.
2.6 Changes are subject to authorisation by Technology and/or the Business prior to implementation.	<p>Inspection</p> <p>For a sample of changes, verified through inspection that each change was subject to authorisation by Technology and/or the Business prior to implementation.</p>	No exception noted.
2.7 There is segregation of the development, test and production environments.	<p>Observation</p> <p>Verified through onscreen observation that segregated development, test and production environments exist.</p>	No exception noted.
2.8 Documented procedures for emergency changes are in place. Emergency changes are subject to formal authorisation prior to or as soon as practical after implementation. Emergency changes are documented and tested as soon as practical upon implementation.	<p>Inspection</p> <p>Verified through inspection that documented procedures for emergency changes are in place.</p> <p>Inspection</p> <p>For a sample of emergency changes, verified through inspection that each change was formally authorised, tested and documented according to emergency procedures.</p>	No exception noted.



Description of controls	Test performed by PwC	Results
2.9 All system and user documentation is updated accordingly.	Inspection For a sample of changes, verified through inspection that release notes were published and user documentation was updated.	No exception noted.



Physical Security

Control Objective 3: Controls provide reasonable assurance that physical security prevents unauthorised access to the primary and secondary data centres hosting Austraclear infrastructure.

Description of controls	Test performed by PwC	Results
3.1 Documented physical security policies and procedures are in place. This includes site visitation procedures for each category of access.	Inspection Verified through inspection that the documented physical security policies and procedures are in place.	No exception noted.
3.2 Access to the primary and secondary data centres is restricted and monitored through the use of electronic security devices and other arrangements.	Observation Verified through observation of the primary and secondary data centre that access to the ASX data centres is restricted and monitored through the use of electronic security devices and other arrangements, including: <ul style="list-style-type: none"> - exterior doors were locked - electronic access cards were required to enter the data centres, and - the data centres were monitored by CCTV. 	No exception noted.
3.3 Access requests to the primary and secondary data centres are approved prior to access being granted.	Inspection For a sample of access requests to the primary and secondary data centres, verified through inspection that access to the ASX data centres was approved prior to access being granted.	No exception noted.



Description of controls	Test performed by PwC	Results
3.4 Staff, visitors, contractors and customers are required to wear identification badges / tags.	<p>Observation</p> <p>Verified through observation that staff, visitors, contractors and customers were required to wear identification badges / tags.</p>	No exception noted.
3.5 Access is removed in a timely manner for employees who no longer require access to the primary and secondary data centres.	<p>Inspection</p> <p>For a sample of terminated employees, verified through inspection that access to the primary and secondary data centres were removed in a timely manner.</p>	No exception noted.
3.6 Regular access reviews are performed to confirm currency and appropriateness of access to the primary and secondary data centres.	<p>Inspection</p> <p>For a sample of data centre user access reviews, verified through inspection that regular access reviews were performed to confirm currency and appropriateness of access to the ASX data centres.</p> <p>Inspection</p> <p>Verified through inspection that all follow up actions resulting from the sampled user access reviews were completed in a timely manner in accordance to ASX Policy.</p>	No exception noted.



Disaster Recovery Procedures

Control Objective 4: Controls provide reasonable assurance that in the event of a disaster, measures are in place to enable Austraclear to resume effective operations within two hours.

Description of controls	Test performed by PwC	Results
4.1 A documented Disaster Recovery Plan for the System is in place.	Inspection Verified through inspection that the Disaster Recovery Plan exists.	No exception noted.
4.2 The Disaster Recovery Plan for the System is tested on a regular basis.	Inspection Verified through inspection that the Disaster Recovery Plan was tested on a regular basis to enable Austraclear to resume effective operations within two hours.	No exception noted.



IT Processing

Control Objective 5: *Controls provide reasonable assurance that the Austraclear system is backed up, and system processing and performance is monitored.*

Description of controls	Test performed by PwC	Results
5.1 Documented backup policies and procedures are in place.	<p>Inspection</p> <p>Verified through inspection that backup policies and procedures have been documented.</p>	No exception noted.
5.2 Application data is backed up on a regular basis.	<p>Observation</p> <p>Verified through onscreen observation that the backup schedule for application data was setup in line with policy requirements.</p> <p>Observation and Inspection</p> <p>Verified through onscreen observation and inspection that an automated notification is generated upon failure of a backup job.</p> <p>Inspection</p> <p>For a sample of days, verified through inspection that backups were completed successfully.</p> <p>Inspection</p> <p>For a sample of incident tickets raised due to backup failures, verified through inspection that they were resolved in a timely manner.</p>	No exception noted.



Description of controls	Test performed by PwC	Results
5.3 Backed up data is stored in an offsite secure location and restricted to authorised personnel.	<p>Inspection</p> <p>Verified through inspection of a copy of the agreement with the third-party service provider that backed up data is taken and stored in an offsite secure location.</p> <p>Inspection</p> <p>For a sample of days, verified through inspection that sign-off was obtained by an authorised representative indicating that backup tapes had been taken off-site for storage.</p> <p>Inquiry and Inspection</p> <p>Verified through inquiry with management and inspection of the listing of individuals with access to ASX data stored at offsite locations that they were authorised personnel.</p>	No exception noted.
5.4 Network capacity, performance incidents, operational incidents and system availability is monitored and reported.	<p>Inspection</p> <p>Verified through inspection of a sample of management status reports that network capacity, performance incidents, operational incidents and system availability are monitored and reported.</p>	No exception noted.



Description of controls	Test performed by PwC	Results
<p>5.5 Automated system monitoring tools are used to monitor operational integrity. Exception reporting is used to alert staff of operational failures.</p>	<p>Observation</p> <p>Verified through onscreen observation that system monitoring tools are utilised to monitor the operational integrity of the System.</p> <p>Inspection</p> <p>Verified through inspection that exception reporting functionality alerted staff of operational failures.</p>	<p>No exception noted.</p>
<p>5.6 Job schedules are in place for batch processing. Each time a job schedule is run the results are documented and reviewed.</p>	<p>Inspection</p> <p>Verified through inspection that job schedules are in place for batch processing.</p> <p>Inspection</p> <p>For a sample of days, verified through inspection that the job schedules results were documented and reviewed.</p>	<p>No exception noted.</p>
<p>5.7 Changes to job schedules are approved.</p>	<p>Inspection</p> <p>For a sample of changes to job schedules, verified through inspection that they were approved.</p>	<p>No exception noted.</p>



Environmental Controls

Control Objective 6: *Controls provide reasonable assurance that environmentally-controlled data centres exist to facilitate continuity of data processing operations.*

Description of controls	Test performed by PwC	Results
<p>6.1 The data centres contain the following environmental mechanisms</p> <ul style="list-style-type: none"> - fire detection and suppression systems - air conditioning systems - uninterruptible power supplies, and - water detection systems. 	<p>Observation</p> <p>Verified through observation of the primary and secondary data centres that they contain the following environmental mechanisms:</p> <ul style="list-style-type: none"> - fire detection and suppression systems - air conditioning systems - uninterruptible power supplies, and - water detection systems. <p>Inspection</p> <p>For the vendor-managed secondary data centre, for a sample of months, verified through inspection that management receives and reviews a report which includes information on these relevant environmental mechanisms.</p>	<p>No exception noted.</p>



Description of controls	Test performed by PwC	Results
6.2 A schedule of maintenance is performed on a regular basis to assist in preventing operational failure of the above environmental mechanisms.	<p>Inspection</p> <p>Verified through inspection of the primary and secondary data centres maintenance schedule that maintenance of the above environmental mechanisms is performed on a regular basis.</p> <p>Inspection</p> <p>For primary data centre, verified through inspection of a sample of maintenance reports that the preventative maintenance occurred in accordance with the schedule.</p> <p>Inspection</p> <p>For the vendor-managed secondary data centre, verified through inspection that management has performed a monitoring check to ensure maintenance for environmental mechanisms relevant to ASX have been completed in accordance with the pre-defined schedule.</p>	No exception noted.



Austraclear

Control Objective 7: Controls provide reasonable assurance that the process of daily settlement is complete and accurate.

Description of controls	Test performed by PwC	Results
<p>7.1 Automated monitoring of the system is in place with any technical alerts actioned. Each time the job schedule is run results are reviewed.</p> <p>As a result of successful job schedule, Participant reports are available directly from the System and include:</p> <ul style="list-style-type: none"> - Cash Report - Holding Report, and - Settlement Instructions Report. 	<p>Observation</p> <p>Verified through onscreen observation that automated monitoring tools were utilised to monitor the operational integrity of the System.</p> <p>Inspection</p> <p>For a sample of technical alerts, validated that they were actioned.</p> <p>Observation</p> <p>Verified through onscreen observation that Participant reports were available directly from the System and include:</p> <ul style="list-style-type: none"> - Cash Report - Holding Report, and - Settlement Instructions Report. 	No exception noted.
<p>7.2 Documented procedures are in place for session extensions.</p>	<p>Inspection</p> <p>Verified through inspection that documented procedures are in place for session extensions.</p> <p>Inspection</p> <p>For a sample of session extensions, verified through inspection that the documented procedures were followed.</p>	No exception noted.



Description of controls	Test performed by PwC	Results
<p>7.3 In the event ASX is notified by a participant of a discrepancy in the settlement obligations, an incident record is raised and tracked to resolution.</p>	<p>Inspection</p> <p>Verified through inspection that documented policy and procedures are in place for operational incident management.</p> <p>Inspection</p> <p>For a sample of incidents where ASX was notified of a discrepancy in either the settlement obligations or security by a Participant, verified through inspection that the incident record was raised and tracked to resolution.</p>	<p>No exception noted.</p> <p>There was no instance during the between 1 July 2020 to 30 June 2021 where ASX was notified of discrepancies in the settlement obligations by a Participant. Therefore, testing over the operating effectiveness of this control could not be performed and our procedures were limited.</p>