ASAE 3402

Assurance Report on Controls at a Service Organisation relating to the Derivatives Clearing System (DCS)
1 July 2024 – 30 June 2025

Contents

1 / Statement by ASX as the Service Organisation

The accompanying description provided by ASX management in this report has been prepared for participants who have used the DCS System (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 participants' financial reports / statements. ASX confirms that:

(a) The accompanying description in Sections 5, 7 and 9 fairly presents DCS ('DCS' or 'system') for processing Participants' transactions throughout the period 1 July 2024 to 30 June 2025.

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 DCS during the period 1 July 2024 to 30 June 2025, 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 2024 to 30 June 2025. 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 2024 to 30 June 2025.

Signed on behalf of management

Signed by:
Darren Yip
9AA6FB6F2207461...

Darren Yip

Group Executive, Markets

29 July 2025

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

To: Directors of ASX Limited

Scope

In accordance with the terms of the engagement letter dated 4 February 2025, we were engaged to report on ASX Limited's (ASX) description in Sections 5, 7 and 9 of its Derivatives Clearing System (DCS) system (System) for processing Participants' transactions throughout the period 1 July 2024 to 30 June 2025 (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 Management

We have complied with the ethical requirements of the Accounting Professional and Ethical Standard Board's APES 110 *Code of Ethics for Professional Accountants (including Independence Standards)* relevant to assurance engagements, which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

Our firm applies Australian Standard on Quality Management ASQM 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Reports and Other Financial Information*, or Other Assurance or Related Services Engagements, which requires the firm to design, implement and operate a system of quality management including policies or 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

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

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 Particiapants 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 2024 to 30 June 2025.

(b) The controls related to the control objectives stated in the description were suitably designed throughout the period from 1 July 2024 to 30 June 2025.

(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 2024 to 30 June 2025.

Description of Tests of Controls

The specific controls tested and the nature, timing and results of those tests are listed in Section 9.

Other Information

The information included in sections 3, 4, 6 and 8 is presented by the service organisation to provide additional information and is not part of the service organisation's description of controls that may be relevant to Participants' internal control as it relates to financial reporting. Such information has not been subjected to the procedures applied in the examination of the description of the service organisation and accordingly, we express no opinion on it.

Intended Users and Purpose of the report

Anyone accessing this report is taken to have acknowledged and agreed to the following:

This report and the description of tests of controls in Section 9 are intended only for ASX and Participants who have used ASX's DCS 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 Participants financial reports / statements.

This report was prepared on the instructions of our client, ASX, in connection with certain of ASX's internal controls. We have no knowledge or understanding of the circumstances or position of each Participant or any other party. Our work was not planned or conducted having regard to the information any party may require regarding ASX's DCS system (including the control objectives or controls within the System), or the ways in which they may seek to make use of our report or the accompanying description of tests of controls and we therefore make no representation concerning the appropriateness of this report or the accompanying description of tests of controls for them. Except to the extent set out above, we performed our work and this report is prepared in accordance with the purpose and terms of our engagement by ASX and we accept no responsibility or liability to anyone else

(other than the Participants) in connection with it. Anyone else who chooses to use or rely on our reports for their own individual purposes do so at their own risk.

This disclaimer applies:

- to the maximum extent permitted by law and, without limitation, to liability arising in negligence or under statute; and
- even if we consent to anyone other than ASX and the Participants and their auditors receiving or using this report or the accompanying description of tests of controls.

DocuSigned by:
92855915345E477...

PricewaterhouseCoopers

DocuSigned by:
92855915345E477...

Scott Hendry
Partner

Sydney
29 July 2025

3 / Introduction

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 ASX Clear Operating Rules, the general effectiveness of the operation of DCS 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 DCS and its role in the clearing and settlement process
- a summary of ASX's corporate governance arrangements relating to the DCS operating environment
- the control objectives and control procedures that underpin the DCS control environment, and
- the independent auditor's report on the control objectives and control activities supporting those control objectives.

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

4 / Overview of the ASX Group

ASX is an integrated exchange offering listings, markets, securities and payments, and technology and data 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.

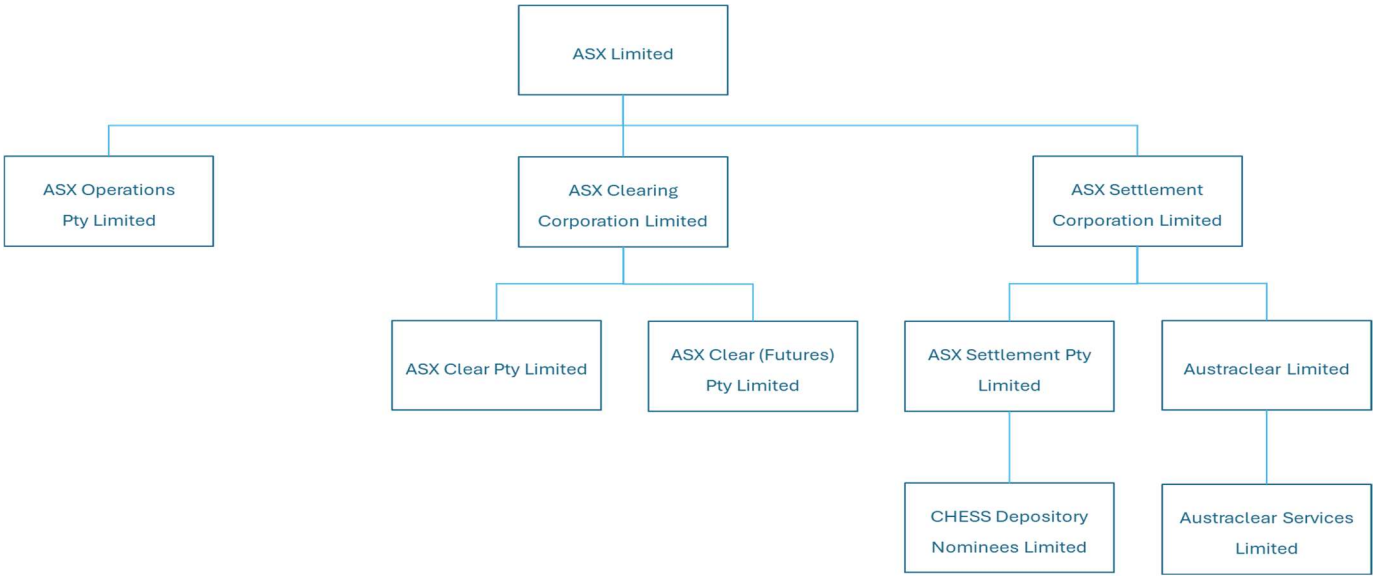
Companies and other issuers of capital from Australia and around the world engage with ASX to manage risk and raise capital to sustain and grow their businesses. ASX operates liquid, transparent and reliable markets of integrity. The certainty and security of its clearing and settlement activities help 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: www.asx.com.au.

Structure

Relevant parts of the ASX Group structure are depicted below:



5 / Overall control environment

Corporate Governance

The control environment within which ASX operates DCS 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 DCS is set out below. More information on ASX's corporate governance framework is available on ASX's website and in its Annual Report and Corporate Governance Statement.

DCS is operated by ASX Pty Limited (ASX Clear). ASX Clear is a clearing and settlement facility licensee and a wholly-owned subsidiary of ASX. It is one of the four clearing and settlement facility licensees in the ASX Group.

The ASX Board relies on the Clearing and Settlement (CS) 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 following table sets out key responsibilities of the CS Boards in relation to risk management:

Operational risk tolerance	Set the operational risk tolerance for the CS facility licensees, and in doing so, have regard to the legitimate business interests of ASX as a provider of capital to the central counterparties.
Risk management framework & internal controls	Review and approve the risk management framework and oversee the adequacy of internal controls, systems and processes for the management of clearing and settlement risks of the CS facility licensees.
Oversee management systems and processes	Oversee management systems and processes for the purpose of: • ongoing compliance with the Financial Stability Standards • ongoing compliance with statutory obligations of the CS facility licensees • management of the CS facility licensees within risk appetite and operational risk tolerances.

Each of the CS Boards is comprised of a majority of directors who are independent non-executives. The Chair is also an independent non-executive director. For each of the CS facility licensees (ASX Clear, ASX Settlement, ASX Clear (Futures) and Austraclear), there is an additional requirement that their Boards comprise at least 50 percent of the non-executive directors who are not also directors of ASX Limited ('**non-ASX directors**') and that the Chair is a non-ASX director.

These arrangements allow the non-ASX directors of ASX Clear and ASX Settlement to form a quorum and meet separately to consider matters that relate to providing clearing and settlement services to non-ASX affiliated market operators or listing venues, including the consideration of confidential and competitively sensitive information. The non-ASX directors may also meet separately to consider potential intra-group conflicts and any recommendations on the management of those intra-group conflicts.

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 the Boards of ASX Clear and ASX Settlement) and there is a standing invitation for a representative of the non-ASX directors of ASX's Clearing and Settlement Boards to attend.

ASX Limited and ASX's Clearing and Settlement Boards have established a Technology Committee (comprising independent, non-executive directors of those boards). At least one member is required to be a non-ASX director of ASX's Clearing and Settlement Boards, and currently, the rest of the members are independent non-executive directors of ASX Limited. The Technology Committee assists the CS Boards to review and oversee arrangements for the CS facility licensees to achieve compliance with their statutory obligations as licence holders in relation to technological resources and human resources (with respect to technology) for operating the CS facilities.

The following Committees and supporting governance forums (comprised of Senior Management) also form an integral part of the overall control environment in which DCS operates:

- Risk Committee
- Technology Management Committee
- Executive Team
- Monthly and Quarterly Business Reviews (Enterprise wide)
- Portfolio Business Review

Each clearing and settlement facility licensee has a lead business executive (each, a CS Lead Executive) responsible for the operation of the facility, and for the achievement of strategies and objectives for the facility as determined by the relevant ASX Clearing and Settlement Board. The Group Executive, Markets is a CS Lead Executive for ASX Clear (Futures) and the Group Executive, Securities and Payments is a CS Lead Executive for Austraclear, ASX Settlement and ASX Clear.

ASX's Enterprise Compliance function conducts oversight of the ASX Group and provides quarterly reports to the Risk Committee, Audit and Risk Committee, Clearing and Settlement Boards and a meeting of non-ASX directors of Clearing and Settlement Boards in relation to regulatory compliance matters.

Charters of the ASX Board, Clearing and Settlement Boards, ARC and the Technology Committee are available on ASX's website: www.asx.com.au.

Risk Management

ASX has an established enterprise risk management framework that supports ASX's approach to risk management, and encompasses risk appetite, risk culture and behaviours, and supporting frameworks and processes governing risk identification and assessment, treatment, monitoring and reporting.

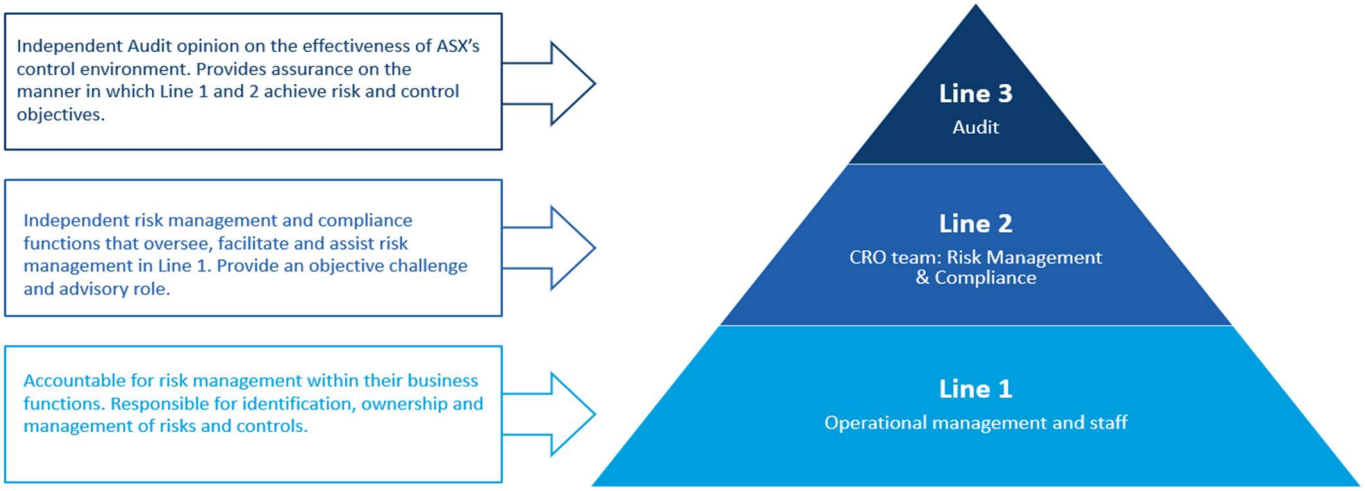
ASX's enterprise risk management function has day-to-day responsibility for implementation of the enterprise risk management framework. The ARC reviews the enterprise risk management framework annually.

ASX's enterprise risk management framework is founded on the Three Lines of Defence model, which sets out clear roles and responsibilities for managing risks and controls across the organisation.

The Three Lines of Defence are as follows:

- **Line 1** is risk management within the business divisions and functions, including the identification, assessment, monitoring, reporting and escalation of risks.
- **Line 2** is the independent risk management and compliance functions that develop risk and compliance frameworks and policies and oversee and challenge risk management in Line 1. This includes the Enterprise Risk and Enterprise Compliance functions that report to the CRO.
- **Line 3** is the Internal Audit function, providing independent assurance over key risks, controls and the effectiveness of Line 1 and 2.

Figure 2 Graphical representation of the Three Lines of Defence within the ASX organisational structure



The identification and assessment of risks relating to the resilience, reliability, integrity, and security of DCS are addressed as part of this overarching risk management framework.

Internal Audit

Internal Audit is an independent assurance function. Its role is to provide the ASX Limited Board, CS Boards and management with assurance that ASX has effective, adequate and efficient internal controls in place to support the achievement of its objectives, including the management of risk. It also provides advice on ASX's internal controls and business processes.

The Internal Audit function provides regular reports to management, the ARC and the CS Boards on key findings from internal audits and the implementation status of agreed internal audit recommendations. Management remains responsible for risk management and the operation and enhancement of internal controls, as well as for implementing agreed internal audit recommendations.

The General Manager, Internal Audit reports to the CFO for administrative purposes and has a direct reporting line to the Chair of the ARC in relation to the performance of the Internal Audit function. The General Manager, Internal Audit also has direct access to the CS Boards.

The Internal Audit function has its own charter that sets out its objectives, role, responsibilities, authority and accountability. The charter is published on the ASX website.

Regulatory Governance

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

6 / Overview of DCS environment

ASX Clearing Corporation assists ASX participants to more effectively undertake their clearing activity by reducing systemic risk, minimising counterparty risk, and by increasing capital efficiency and operating efficiency. This is achieved through ASX Clearing Corporation's wholly owned subsidiaries, ASX Clear Pty Limited (ASX Clear) and ASX Clear (Futures) Pty Limited, which operate clearing facilities and provide central counterparty facilities.

ASX Clear Pty Limited (ASX Clear) operates a clearing facility and provides central counterparty (CCP) services for financial products traded on the ASX market, including equities, warrants, interest rate securities and equity related derivatives (exchange traded options), equities traded, warrants quoted and traded on the Cboe market.

ASX Clear is authorised to clear transactions for certain customers located in a number of jurisdictions, including the EU and the United States.

ASX Clear is currently the sole provider of clearing services for Australia's equity markets.

Regulation

ASX Clear 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, 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.

DCS

ASX Clear operates the Derivatives Clearing System (DCS) to register and clear equity related derivative products and the Clearing House Electronic Subregister System (CHESS) to register and clear cash equities, interest rate securities and warrants. A separate assurance report is available for the CHESS system.

DCS consists of two primary components. The first component is used by ASX Clear and consists of a number of modules; the main module being the Central Clearing Controller (CCC). This component maintains clearing information such as open positions, financial details such as margin information for each participant's accounts, details of trades, allocations, give-ups, take-ups, parameters and all other required information.

Other modules within this component include the Derivatives Pricing System (DPS), Stock Lodgement System (SLS) and Product Factory.

DPS captures real-time price related data from the trading platform. This data is analysed throughout the day to maintain a record of 'deemed' market prices. These prices are used to establish end-of-day settlement prices and for intra-day risk assessment. DPS also includes a client application that allows parameter maintenance functions to be performed and results to be reviewed.

SLS provides functionality to manage physical non-cash collateral. Collateral may be lodged to cover a specific account (omnibus or individual customer) or shared amongst multiple accounts. SLS interfaces to the securities depository system (CHESS).

Product Factory provides the listing function for exchange traded options and also provides a mechanism by which corporate actions can be processed. The processing of corporate actions adjusts the exchange traded options series and also affects the existing open interest.

Margins for equity related derivative products are calculated in CME Span® 4.0, using position information contained within DCS on both an end-of-day and intraday basis. The end-of-day (EOD) margin calculations are sent back to DCS and reported as part of the participant's EOD settlement obligation. In addition, settled intraday margin amounts are included in the participant's EOD settlement obligation.

The second component is the Member Clearing Module (MCM) and is provided to participants. This component records information relating only to the relevant participant; it does not store any sensitive information relating to any other participants. MCM serves as the participant's interface to the clearing system and provides functionality to maintain account information and to perform position maintenance inclusive of allocations, transfers, give-ups, take-ups, match-outs and exercises.

Transaction processing

DCS captures reported trades from the ASX Trade platform and disseminates them to the relevant participants in near real-time. If a trade did not have allocation details specified at the time of order entry in ASX Trade, the participants can send an allocation transaction in DCS to allocate the trade to one or more accounts. Alternatively, the participant can “give-up” the trade to another participant. In this event, the corresponding participant would then “take-up” the trade. Any unallocated trades at the end of the day are allocated to the default house account of the participant.

The system is closed at 7:00 pm each day so that end of day processing can commence. The key purpose of end of day processing is to determine each participant's settlement obligation. This comprises of premium due, fees and commissions and calculated margin less existing cash balance and collateral valuation. The calculated cash settlement obligations are sent to Austraclear for settlement. These settlement obligations are required to be matched by the participants in Austraclear by a specified time to confirm the details of the settlement instructions. Details of the daily settlement process in Austraclear are covered in a separate assurance report.

Additional processing takes place to exercise relevant positions and randomly assign them to counterparties. Any equities trades resulting from the expiry process are automatically reported to ASX Trade.

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

Reporting

DCS automatically provides a number of reports to participants, including:

- financial reports (current account statements, interest statements, fee statements, daily margin summary, daily financial statement, commissions, margin prices, theoretical prices, price averaging, price warning)
- collateral reports (activity statements, holding statement)
- position reports (open positions, daily position activity, exercise activity, allocation listing, give-ups, transfers)
- exercise and expiring contracts reports, and
- reconciliation reports.

7 / Overview of DCS operations

The primary division that has direct control over the operational governance of DCS is the Markets Line of Business (LoB). The Operations team within the Markets LoB is responsible for the day-to-day processing of trading, clearing and settlement transactions. The Markets Technology team and the technology shared services teams within ASX Technology, and the IT Service Management team in the Enterprise Customer and Operations division, are responsible for the IT support and development of DCS.

The DCS operational environment includes processes and controls in the following areas:

- transaction processing
- error resolution and escalation, and
- security and operational resilience
- system operations
- change management
- security, and
- system resilience.

The Markets Line of Business is headed by the Group Executive, Markets, ASX Technology is headed by the Chief Information Officer, and the Enterprise Customer and Operations division is headed by the Chief Operating Officer.

The following sections provide an overview of business and IT controls.

Daily settlement in DCS and Austraclear

Each weekday, DCS sends the calculated cash settlement obligations to Austraclear for settlement through the predefined settlement process in Austraclear. In order to ensure this process is completed successfully, Clearing Operations performs a number of daily checks. These include:

- Verification of amounts being posted from DCS to Austraclear to the calculated amount presented in the daily financial statements available for the participants.
- Monitoring of participants trade matching and cash settlement status in Austraclear. If participants do not complete the matching process or if the settlement is not completed within the predefined timeframe, Clearing Operations follows a predefined escalation process.
- Reconciliation of total amount settled in Austraclear with the calculated amounts across different margin systems, including DCS.

On a regular basis, reconciliation of the ASX provided settlement obligation between DCS to Participants' internal records should be performed by the Participants. Where variances are noted, ASX should be notified. ASX follows an established incident management process to track these variances to resolution.

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 underlying databases relevant to DCS. 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 DCS follow the enterprise-wide change management process that requires all changes to be logged in a centralised IT Service Management (ITSM) 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 DCS 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 DCS and scenario(s) are tested at least yearly. 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. Disaster refers to events including, but not limited to - ‘Loss of Access’, ‘Loss of Site’, ‘Loss of Systems’ and excludes technology malfunction events.

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 User IDs, passwords, digital certificates and VPN.

IT processing

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

- System backup: DCS application data is replicated to the secondary data centre in accordance with established policies and procedures. 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. System 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 DCS. The status of the batch processes is monitored to ensure they are successfully completed. Changes to the schedules require approval prior to being implemented.
- Incident management: DCS related incidents are logged and tracked to resolution following the ASX enterprise-wide incident management process, which contains specific SLAs (Service Level Agreement) for information technology incidents.

System Change

During the period, there were changes made to the DCS environment as part of usual management and support, however there were no changes in processes and controls described above.

Control Objectives and Control Procedures

Set out in this report are the control objectives relevant to DCS. The controls listed in Section 9 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 DCS.

Complementary User Entity Controls

Achievement of control objective 7 as set out in Section 9 are also 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 participants' auditors should consider whether the following CUEC is operating.

Ref	Control Description	Relevant control objectives in section 9
CUEC 1	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

8 / Requirement for the report

The requirement for and scope of the independent audit is mandated in the ASX Clear Operating Rules. The following table provides the requirements under section 1.22 of the ASX Clear Operating Rules.

Rule Ref	Title	Content
1.22.1	ASX Clear to conduct annual review	ASX Clear must require an independent auditor to conduct an annual review of the Clearing System and that review must comprise the matters specified in the Procedures.
1.22.2	Copy of audit certificate to be provided to Participant	If a Participant requests that ASX Clear provide a copy of any audit certificate arising from an annual review under Rule 1.22.1, ASX Clear must, without charge, provide a copy of the audit certificate to the Participant within 1 calendar month of: (a) ASX Clear receiving the audit certificate or (b) the request whichever is the later.
1.22.3	Participant may request other review of the Clearing System	If a Participant gives notice to ASX Clear requesting an audit certificate in relation to any review of the Clearing System other than an annual review under Rule 1.22.1: (a) the Participant must in the notice undertake to pay any fee for that service which ASX Clear may notify to Participants from time to time and (b) ASX Clear must request an independent auditor to conduct the requested review and supply an audit certificate in relation to the review to the Participant as soon as reasonable practicable.
1.22.4	No other right to inspect ASX Clear records	Except as expressly provided in these Rules, no Participant has any right of access to, or right to inspect, ASX Clear's Records.
1.22.5	Participant to accept review by auditor	Each Participant must accept and treat a review conducted by ASX Clear's auditor under this section as if that review were conducted by the Participant's own auditor.

The following provides the requirements under section 1.22.1 of the ASX Clear Operating Rules – Procedures:

The review will comprise:

(a) reviewing ASX Clear's information processing facilities and the integrity of the Clearing System including:
  (i) maintenance of security and confidentiality over the data of Participants
  (ii) security over the physical operation of the Clearing System
  (iii) backup and disaster recovery procedures and
  (iv) Clearing System access controls.

(b) assessing the integrity and accuracy of information generated by the Clearing System including:
  (i) internal controls over data input by ASX Clear and
  (ii) processing and reporting of transaction data.

9 / Control objectives and related control procedures

This section sets out the control objectives identified and developed by ASX for DCS and the associated control activities, which are in scope for PricewaterhouseCoopers's (PwC) independent assurance report. Any references made to the ASX network, application, operating system and database are specific to DCS.

Following the description of control activities is a summary of tests performed by PwC to determine that the control activities in place were designed and operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives specified were achieved during the period 1 July 2024 to 30 June 2025. Where exceptions have been identified, these have been noted under 'Results' in the table below.

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) is documented and 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 was documented and outlined the principles for restricting access to the network, application software, operating systems and underlying databases and was available to all staff.	No exception noted.
1.2	New and modifications to user access to the ASX network, application software, operating systems and underlying databases are approved prior to access being provisioned.	**Inspection** For a sample of new and modifications to user access, verified through inspection that access to the ASX network, application software, operating system and underlying databases was approved prior to access being provisioned.	No exception noted.
1.3	Termination of user access to the ASX network, application software, operating systems and underlying databases is performed in a timely manner. Terminated employees' Active Directory access is automatically removed or deactivated on last day of service as recorded in the HR system.	**Inspection** For a sample of terminated users, verified through inspection that access to the ASX network, application software, operating system and underlying database was revoked in a timely manner in accordance with the ASX Identity and Access Management Policy.	Exception noted. For the period 24 March 2025 to 2 June 2025, following a change in process, the Active Directory termination process was not designed effectively for 'Maximum Term' employees (i.e. contractors). During this period the process was configured to remove a Maximum Term employee's access on the last day of their contract (end employment

Description of controls		Test performed by PwC	Results
		Observation Verified through onscreen observation that an automated deactivation process was in place to disable terminated staff network access on the last day of service as recorded in the HR system. **Inspection** For a sample of terminated users throughout the period, verified through inspection that their ASXProd account (ASX network access) was automatically deactivated on the last day of service as recorded in the HR system.	date), instead of their last day of service (termination date). PwC performed a review of all Maximum Term employees that were terminated during the impacted period. For 3 out of 13 users (full population) identified, their access was not removed on their last day of service. Access was removed within 1 business day of their last day of service. Testing identified that access was not used post termination.
1.4	Access to the ASX network, application software, operating systems and underlying databases is authenticated and restricted through the use of password controls in line with policy requirements or a valid exemption for the deviation exists.	**Inspection** Verified through inspection at the time of testing that password parameters at the ASX network, application software, operating system and underlying database layers were in line with the ASX Identity and Access Management Policy requirements. **Inspection** Where the password parameters were not in compliance with the ASX Identity and Access Management Policy requirements, validated through inspection that a current exemption for the deviation exists.	No exception noted.
1.5	Regular reviews of user access to the application software, operating systems, underlying databases and source code repositories are performed to confirm currency and appropriateness of access. Follow up actions are completed in a timely manner.	**Inspection** For a sample of application software, operating system, underlying database and source code repository user access reviews, verified through inspection that the reviews were performed to confirm currency and appropriateness of access. **Inspection** Verified through inspection that all follow up actions resulting from the sampled user access reviews were completed in a timely manner in accordance with ASX Identity and Access Management Policy.	No exception noted.

Description of controls	Test performed by PwC	Results
1.6 Documented procedures and network security measures, i.e. firewalls, intrusion detection software, patching, anti-virus software and incident response process, are in place for safeguarding against the threat of malicious attacks.	**Inspection** Verified through inspection of the documented policies and procedures (including playbooks) that principles for safeguarding against the threat of malicious attack were outlined. Relevant policies and procedures (including playbooks) that PwC inspected were as follows: - Vulnerability and Patch Management Policy - Malicious Code Standard - Cyber Incident Response Plan - Incident Response Playbooks **Inspection and Observation** Verified through inspection of network documentation and onscreen observation that firewalls, intrusion detection software and anti-virus software were in place at the time of testing. **Inspection** For a sample of monthly patching meetings, verified through inspection that the available patches were evaluated and, where required, tracked for implementation in line with the Security Patching Policy. *For incident response process testing, please refer to control 5.7.	No exception noted.
1.7 Remote access to the ASX network, application software, operating system and underlying databases is restricted by User IDs, passwords, digital certificates and VPN.	**Observation** For a sample user, verified through onscreen observation that User IDs, passwords, digital certificates and VPN access, were required to access the ASX network remotely. **Inspection** Verified through inspection of the ASX Mobility and Remote Access Standard that remote access to the ASX network is restricted via the use of VPN and digital certificates.	No exception noted.

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 DCS production environment are authorised, tested and managed appropriately.*

Description of controls		Test performed by PwC	Results
2.1	Documented change management procedures are in place. The policy is available to all relevant staff.	**Inspection** Verified through inspection that the ASX ITSM Change Management Policy was documented and outlines the procedures to handle standard, normal and emergency changes and was available to all relevant staff.	No exception noted.
2.2	Changes (excluding emergency changes) to the application software, operating systems and underlying databases have testing performed with testing results recorded, tracked and signed off prior to implementation.	**Inspection** For a sample of changes to the application software, operating system and underlying databases, verified through inspection that testing results were recorded, tracked and signed off prior to implementation.	No exception noted.
2.3	Changes (excluding emergency changes) to the application software, operating systems and underlying databases are authorised by Technology and/or the Business prior to implementation.	**Inspection** For a sample of changes to the application software, operating system and underlying databases, verified through inspection that each change was authorised by Technology and/or the Business prior to implementation.	No exception noted.
2.4	Segregation of development, test and production environments is in place.	**Observation** Verified through onscreen observation that segregated development, test and production environments existed at the time of testing.	No exception noted.
2.5	Emergency changes are authorised prior to or as soon as practical after implementation with documentation and testing performed as soon as practical upon implementation.	**Inspection** For a sample of emergency changes, verified through inspection that each change was formally authorised, tested and documented according to the ASX ITSM Change Management Policy.	No exception noted.

Description of controls	Test performed by PwC	Results
2.6 Segregation of duties between developers and migrators of changes is enforced through periodic review of access at the source code repositories and operating systems. Follow up actions are completed in a timely manner.	Refer to control 1.5 above.	Refer to control 1.5 above.

Physical Security

Control Objective 3: *Controls provide reasonable assurance that physical security prevents unauthorised access to the ASX primary data centre and ASX-controlled areas in the secondary data centre.*

Description of controls	Test performed by PwC	Results
3.1 Documented physical security policies and procedures relating to the ASX primary data centre and ASX-controlled areas in the secondary data centre are in place. This includes site visitation procedures (i.e. sign-in process, and the requirement to be accompanied by an authorised individual) for each category of access. The policy is available to all relevant staff.	**Inspection** Verified through inspection that documented physical security policies and procedures relating to the ASX primary data centre and ASX controlled areas in the secondary data centre were in place and available to all relevant staff. Relevant policies and procedures that PwC inspected were as follows: - National Facilities Physical Security Policy - ASX Physical Security Standards - Australian Liquidity Centre Operating Procedure	No exception noted.
3.2 Access to the ASX primary data centre and ASX-controlled areas in the secondary data centre is restricted and monitored through the use of electronic security devices and other arrangements (i.e. locked doors, security cameras, 24x7 operation). Identification badges are required for staff, visitors, contractors and customers.	**Inquiry and Inspection** Verified through inquiry with management and noted through inspection that documented physical security policies and procedures exist governing restricted access to the ASX primary data centre and ASX-controlled areas in the secondary data centres, and 24x7 operation. Relevant policies and procedures that PwC inspected were as follows: - National Facilities Physical Security Policy - ASX Physical Security Standards - Australian Liquidity Centre Operating Procedure **Observation** Verified through observation at the time of testing that the ASX primary data centre and ASX-controlled areas in the secondary data centres that access was restricted and monitored through the use of electronic security devices and other arrangements, including: - locked doors	No exception noted.

	Description of controls	Test performed by PwC	Results
		- security cameras **Observation** Verified through observation at the time of testing that staff, visitors, contractors and customers were required to wear identification badges.	
3.3	Access requests to the ASX primary data centre and ASX-controlled areas in the secondary data centre are approved prior to access being granted.	**Inspection** For a sample of access requests to the ASX primary data centre and ASX-controlled areas in the secondary data centre, verified through inspection that access was approved prior to access being granted.	No exception noted.
3.4	Access is removed in a timely manner for employees who no longer require access to the ASX primary data centre and/or ASX-controlled areas in the secondary data centre.	**Inspection** For a sample of terminated employees, verified through inspection that access to the ASX primary data centre and/or ASX-controlled areas in the secondary data centres was removed in a timely manner.	Exception noted. For 1 out of the 3 users sampled by PwC for access to the primary and secondary data centre, we noted that access was removed 10 business days after the user was terminated. Testing identified that access was not used post termination. The user's access was reviewed and removed as part of the monthly user access review process.
3.5	Regular access reviews are performed to confirm currency and appropriateness of access to the ASX primary data centre and ASX-controlled areas in the secondary data centre. Follow up actions are completed in a timely manner.	**Inspection** 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 primary data centre and ASX-controlled areas in the secondary data centre. **Inspection** Verified through inspection that no follow up actions (access removals) were identified for the sampled user access reviews.	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 DCS 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 and tested on a regular basis with an appropriate level of oversight.	**Inspection** Verified through inspection that a documented Disaster Recovery Plan for the system was in place, tested on a regular basis and test results are communicated and approved by relevant management.	No exception noted.
4.2	A documented Business Continuity Plan is in place and reviewed on a periodic basis. Scenario(s) are tested at least yearly, results are reviewed, approved and updates are made to the Business Continuity Plan as required.	**Inspection** Verified through inspection that the Business Continuity Plan (BCP) was in place and was reviewed periodically. Inspected that BCP scenario testing was performed at least annually, results reviewed, approved and updated as required.	No exception noted.

IT Processing

Control Objective 5: *Controls provide reasonable assurance that DCS 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. The policy and procedure documents are available to all relevant staff.	**Inspection** Verified through inspection that DCS back up policy was documented and was available to all relevant staff.	No exception noted.
5.2	Application data is backed up on a regular basis. Failures are identified and tracked to resolution.	**Inspection** Verified through inspection of the configuration setting that incident tickets are raised for backup failures. **Inspection** For a sample of days, verified through inspection that backups were completed successfully. **Inspection** For a sample of incident tickets raised due to backup failures, verified through inspection that they were resolved in a timely manner in line with policy.	Exception noted. PwC noted via inspection of the configuration setting in place for incident tickets being raised upon backup failure, that incident tickets were only raised in the event of a complete backup failure. PwC understands from Management that for partially successful backups an alert is sent to the backup team for appropriate action, but no incident tickets are raised. This configuration was not subject to audit procedures. For all partially successful backups identified for in-scope servers throughout the period, PwC performed additional testing to demonstrate that successful backups, where relevant (e.g. the server contains production data), were completed the following day.
5.3	Backed up data is stored in an offsite location and restricted to authorised personnel.	**Inspection** Verified through inspection of the agreement with the third-party service provider that backed up data was taken and stored in an offsite location. **Inspection** For a sample of days, verified through inspection that sign-off was provided by an authorised representative when backup tapes were taken off-site for storage. **Inquiry and Inspection**	No exception noted.

Description of controls		Test performed by PwC	Results
		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.	
5.4	Automated system monitoring tools are in place. Exception reporting is used to alert staff of operational failures.	**Observation** Verified through onscreen observation that automated system monitoring tools were in place at the time of testing. **Inspection** Verified through inspection that exception reporting functionality alerted staff of operational failures at the time of testing.	No exception noted.
5.5	Job schedules are in place for batch processing. Failures are identified and tracked to resolution.	**Inspection** Verified through inspection that job schedules were in place for batch processing. **Inspection** For a sample of days, verified through inspection that the job schedules results were documented and reviewed. In the event of any failures, these were identified and tracked to resolution.	No exception noted.
5.6	Changes to job schedules are tested and approved prior to implementation.	**Inquiry** Verified through inquiry with management that no changes were made to the scheduled jobs for DCS during the period 1 July 2024 to 30 June 2025. **Inspection** Verified through inspection of relevant job scheduler screenshots and confirmed that no changes were made to the scheduled jobs for DCS during the period 1 July 2024 to 30 June 2025.	There were no changes made to the scheduled jobs for DCS during the period 1 July 2024 to 30 June 2025. Therefore, the operating effectiveness of this control could not be tested, and our procedures were limited to inquiry only.
5.7	Documented incident management procedures are in place and available to relevant staff. Incidents are logged and tracked to resolution in accordance with procedures.	**Inspection** Verified through inspection that the ASX IT Incident Management Process was documented and outlined the incident management process and was available to all relevant staff.	No exception noted.

Description of controls	Test performed by PwC	Results
	Inspection For a sample of incident tickets, verified through inspection that the incidents were logged and tracked to resolution in accordance with ASX IT Incident Management Process document.	

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
6.1 The data centres contain the following environmental mechanisms - fire detection and suppression systems - air conditioning systems - uninterruptible power supplies, and - water detection systems.	**Observation** Verified through observation at the time of testing that the ASX primary data centre and ASX-controlled areas in the secondary data centre contained the following environmental mechanisms: - fire detection and suppression systems - air conditioning systems - uninterruptible power supplies, and - water detection systems. **Inspection** For the ASX-controlled areas in the secondary data centre, for a sample of months, verified through inspection that management received and reviewed a report which included information on these relevant environmental mechanisms.	No exception noted.
6.2 A schedule of maintenance is performed on a regular basis to assist in preventing operational failure of the above environmental mechanisms.	**Inspection** Verified through inspection of the data centre maintenance schedules that maintenance of the above environmental mechanisms was performed on a regular basis. **Inspection** For ASX primary data centre, verified though inspection of a sample of maintenance reports that the preventative maintenance occurred in accordance with the schedule. **Inspection** For the ASX-controlled areas in the secondary data centre, verified through inspection that management had performed a monitoring check to ensure maintenance for environmental mechanisms relevant to ASX had been completed in accordance with the pre-defined schedule.	No exception noted.

DCS

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
7.1 Checklists for reviewing the process of sending daily settlement inputs from DCS to Austraclear are completed and reviewed on a timely basis. Exceptions are actioned in a timely manner.	**Inquiry and Inspection** Verified through inquiry with management and inspection that checklists for reviewing the process of sending daily settlement input from DCS to Austraclear exist. **Inspection** For a sample of daily checklists, verified through inspection that they were completed and reviewed on a timely basis and any exceptions were actioned. **Inquiry** Based on our inquiry with ASX Participants Compliance team, there were no instances of participants who failed to settle margin calls prior to pre-defined cut-off time.	No exception noted.
7.2 Incidents logged with regards to a discrepancy in the settlement obligations are tracked to resolution.	**Inspection** Verified through inspection that a documented ASX IT Incident Management Process is in place for incident management. **Inquiry and Inspection** Based on our inquiry and inspection, there were no incidents logged with regards to a discrepancy in settlement obligations during the period.	No exception noted. There were no incidents logged with regards to a discrepancy in the settlement obligations during the period 1 July 2024 to 30 June 2025. Therefore, the operating effectiveness of this control could not be tested, and our procedures were limited to inquiry only.

Get in touch

asx.com.au

ASX
OfficialASX
ASX_official
@ASX
ASXLtd