

# ASX CHESS

## **Special Report of ASX Clear Pty Limited and ASX Settlement Pty Limited**

April 2023

# Contents

Special Report Structure	4
<b>1. Executive Summary</b>	<b>5</b>
1.1 Overview .....	5
1.2 Background .....	6
1.3 Recent History and Investment in CHES	6
1.4 Developing the CHES Roadmap to Address Risks .....	7
1.5 Summarised ASX's response to ASIC Requirements.....	8
<b>2. Scope of the Report</b>	<b>16</b>
2.1 Summary of ASIC Requirements .....	16
2.2 The CHES Architecture .....	16
2.3 The CHES Application .....	17
2.4 CHES Dependency on CORE .....	17
2.5 Scope of Technology Components.....	17
<b>3. Governance and Risk Arrangements</b>	<b>18</b>
3.1 ASX Governance Arrangements in Relation to CHES	18
3.2 Roles and Responsibilities of the ASX Group Boards.....	19
3.3 Roles and Responsibilities of Management .....	21
3.4 Three Lines of Defence.....	23
<b>4. Structure of ASX Response</b>	<b>25</b>
<b>5. Operation</b>	<b>29</b>
5.1 Risk Identification and Assessment / Management and Monitoring ....	29
5.2 Product Management .....	41
5.3 Scalability, Availability and Performance .....	45
5.4 IT Asset Management .....	52
5.5 Testing and Change.....	55
<b>6. Security</b>	<b>59</b>
6.1 Security Strategy, Governance and Risk Management .....	59
6.2 Identity and Access Management .....	68
6.3 Data Security.....	72
6.4 Systems Security .....	76
6.5 Threat and Vulnerability Management .....	81
6.6 Security Monitoring and Response .....	84
<b>7. Continuity</b>	<b>87</b>
7.1 Business Continuity.....	87
7.2 IT Disaster Recovery (DR) and Service Continuity .....	90
7.3 Monitoring of Backups and Incidents.....	92
7.4 Restoration of Backups .....	94

<b>8</b>	<b>Governance</b>	<b>95</b>
8.1	Governance Structure and Supporting Processes .....	95
8.2	Operating Model – Resources and Vendor Support.....	110
8.3	Controls Monitoring.....	113
<b>9</b>	<b>Detailed Roadmap</b>	<b>117</b>
	<b>Appendices</b>	<b>121</b>
	Appendix A – Introduction to ASX and CHES.....	121
	Appendix B – CHES Risks .....	132
	Appendix C – Glossary of Key Terms, Acronyms and Abbreviations .....	153

## Table of Figures

<i>Figure 1.4.3.4.A</i>	<i>CHES Roadmap .....</i>	<i>15</i>
<i>Figure 2.2.A</i>	<i>CHES Ecosystem.....</i>	<i>17</i>
<i>Figure 3.1.A</i>	<i>ASX Governance Structures Overview of CHES.....</i>	<i>19</i>
<i>Figure 3.4.A</i>	<i>Graphical Representation of the Three Lines of Defence within the ASX organisational structure .....</i>	<i>23</i>
<i>Figure 4.A</i>	<i>ASIC Requirements.....</i>	<i>25</i>
<i>Figure 4.1.2.A</i>	<i>Key Elements of the ASX Enterprise Risk Framework (Reference: ASX ERM Framework).....</i>	<i>30</i>
<i>Figure 5.3.A</i>	<i>CHES Processing Cycle .....</i>	<i>46</i>
<i>Figure 6.1.2.A</i>	<i>Cyber Security Team - Organisation Structure.....</i>	<i>61</i>
<i>Figure 8.1.A</i>	<i>ASX Management and Governance Structures Overview for CHES .....</i>	<i>96</i>
<i>Figure Appendix A.A</i>	<i>ASX Group Structure Relevant to CHES.....</i>	<i>121</i>
<i>Figure Appendix A.B</i>	<i>ASX Business and Support Divisions .....</i>	<i>122</i>
<i>Figure Appendix A.C</i>	<i>Relationship between CHES and Australia's Cash Equities, Trading, Clearing and Settlement Services .....</i>	<i>124</i>
<i>Figure Appendix A.D</i>	<i>CHES Actual Service Availability vs Availability Target .</i>	<i>127</i>
<i>Figure Appendix A.E</i>	<i>CHES Ecosystem .....</i>	<i>129</i>

## List of Tables

Table 1.5.A	ASX Statements .....	8
Table 4.A	ASIC Requirements Mapped to the Report Section .....	25
Table 5.1.4.A	CHES Risks Mapped to the four ASIC Scope Areas .....	33
Table 5.1.5.A	Monitoring Forum Groups for CHES Specific Risks.....	38
Table 5.4.3.A	Reports generated for Technology Aged Assets .....	53
Table 9.A	Key Initiatives in CHES Roadmap.....	117
Table Appendix B.A	Extract of ASX ERM system of the CHES Related Risks..	132
Table Appendix C.A	Glossary of Key Terms, Acronyms and Abbreviations used in the Special Report .....	153

## Special Report Structure

The purpose of this report is to outline how ASX is maintaining Australia's clearing and settlement system (CHES) for cash equities and it also provides a response to the requirement from Australian Securities and Investments Commission (ASIC) under s823B of the Corporations Act for a Special Report on the support and maintenance of CHES by ASX Clear and ASX Settlement and referenced in *Structure of ASX Response*.

The key sections of this report are as follows:

- **Executive Summary** – A summary of the history of CHES, and its operations, security, continuity, governance and the CHES roadmap covered in this report.
- **Scope of the Report** – A summary of the scope of this special report, the report sections covered with respect to CHES, its operating performance, architecture, and the technology components.
- **Governance and Risk Management** – Overview of the governance and risk management arrangements that are in place to govern and manage the operation of CHES and associated risks.
- **Detailed Report** – Details the specific ASX responses to the ASIC requirements, as grouped by the Report Sections.

The four report sections cover:

- **Operation** – Risk Identification and Assessment / Risk Management and Monitoring; Product Management; Scalability, Availability and Performance; and IT Asset Management.  
(For further details, refer to *Section 5 Operation*)
- **Security** – Security Strategy, Governance and Risk Management; Identity and Access Management (IAM); Data Security; Systems Security; Threat and Vulnerability Management; and Security Monitoring and Response.  
(For further details, refer to *Section 6 Security*)
- **Continuity** – Business Continuity (BC); IT Disaster Recovery (DR) and Service Continuity; Monitoring of Backups and Incidents; and Restoration of Backups  
(For further details, refer to *Section 7 Continuity*)
- **Governance** – Governance Structure and Supporting Processes; Operating Model – Resources and Vendor Support; and Controls Monitoring.  
(For further details, refer to *Section 8 Governance*)
- **Appendices** – Contains the detailed content for the introduction to ASX and CHES, the CHES Related Risks, Glossary of Definitions, Key Terms and Acronyms and a summary of the structure of the report.

*The information contained in this report is current as at the date of this report. It may change over time, including as a consequence of further developments or assessments.*

*This report has been prepared for the purpose of responding to the written notice issued by ASIC under s823B of the Corporations Act as outlined in this report. It has been published for information purposes only and should not be used or relied on for any other specific purpose.*

*© Copyright 2023 ASX Limited ABN 98 008 624 691. All rights reserved. This report must not be modified, copied, reproduced, republished, stored in a retrieval system or transmitted in any form, whether in whole or in part, without the prior written permission of ASX Limited or its subsidiaries.*

## 1. Executive Summary

### 1.1 Overview

ASX established CHES in 1994 as the electronic system to replace the manual process of clearing and settling transactions in the cash equities market. At the time, it was considered unique and industry-leading largely due to its ability to track direct ownership of listed securities through the Holder Identification Number (**HIN**) mechanism. For the past 29 years, CHES has demonstrated that it can operate reliably and efficiently to meet market needs and satisfy regulatory obligations. More recently, as ASX has worked on a project to replace CHES, a need emerged to conduct a longer term evaluation of support for CHES as it has become evident that it will now need to remain in operation for longer than initially anticipated.

In August 2022, ASX confirmed it was unlikely CHES would be replaced before the end of 2024 and a more detailed review of CHES was undertaken to understand the longer term maintenance requirements. The review confirmed CHES is supported to 2025 and also highlighted risk areas that need to be addressed given the extended timeline for replacement. These included potential capacity constraints when faced with very high volumes of trading, IT components that could come out of vendor support and the ability to maintain human resources with the right technical skills for the legacy product.

Given the longer timeframe under consideration a plan was developed to address these risks, and this was further reviewed and augmented following a request from the Australian Securities and Investments Commission (**ASIC**) to evidence plans to maintain and support CHES until it is replaced. Subsequent to this, ASIC requested ASX to consider plans for CHES to run to 2032.

This report captures ASX's current approach and plans. It notes a number of risks, most of which map to the four themes raised by ASIC which are: operation, security, continuity and governance. Broadly, the findings in this report, highlight the following key risk areas:

- CHES currently has a maximum tested capacity of 10 million trades per day and more work is needed to enhance ASX's forecast models to better cater for unprecedented drivers of trading volumes, such as the peak of 7 million trades per day during COVID-19.
- Subject to the forecast modelling, CHES may require application or infrastructure changes before the CHES Replacement project is completed which could require industry testing by CHES users.
- CHES has a dependency on a critical associated internal system that has capacity constraints.
- As CHES is legacy technology there is a risk that some IT assets may not be fully supported by vendors before the CHES Replacement project is completed. Ongoing maintenance will be required to maintain appropriate levels of support.
- The growing scarcity of engineers, technicians and other specialists required to operate and maintain legacy technologies requires prudent workforce planning.

While many of these risks had already been considered within work plans for CHES, they have been consolidated and catalogued into a roadmap that addresses the longer term support and maintenance requirements. The roadmap contains 27 key initiatives focused on ensuring that the risks are managed appropriately. Indicatively, most of these are expected to complete by the end of 2025. The roadmap will continue to evolve beyond 2025 and there will be further support and maintenance activities until 2032 or such time as the CHES system is replaced.

When reflecting upon the current status of CHES and the work plan underway, ASX makes two key statements in response to ASIC's letter:

**ASX considers that its existing governance, investment, and management arrangements for CHES are commensurate with its role in providing critical financial market infrastructure.**

**ASX has and will continue to invest in and enhance CHES to support the long-term interests of Australia's financial markets and meet applicable regulatory requirements, including the FSS. ASX has a program of work to enhance CHES to ensure it remains operationally reliable until a new solution is implemented.**

These statements are at the core of ASX's response and a summarised view of the evidentiary elements sitting behind them can be found at *Section 1.5 Summarised ASX's response to ASIC Requirements*.

ASX understands its privileged position in providing clearing and settlement services and CHES is at its core. Having done the work to understand the risks, ASX is implementing its action plan. Yet even as these risks are addressed there remains a point at which current CHES technology will not be sufficient to meet the scalability and flexibility features available from more modern architecture and design. This underscores the importance of the continued work on the CHES replacement project, where ASX is working towards announcing the design solution in the final quarter of the 2023 calendar year.

## 1.2 Background

ASX Clear Pty Limited (**ASX Clear**) and ASX Settlement Pty Limited (**ASX Settlement**) are licensed clearing and settlement (**CS**) facility operators under Part 7.3 of the Corporations Act 2001 (Cth) (**Corporations Act**) and are also wholly owned subsidiaries of ASX Limited (**ASX**). Under the Corporations Act, ASX Clear and ASX Settlement are required, among other things, to the extent that it is reasonably practicable to do so to comply with the Financial Stability Standards (**FSS**) published by the Reserve Bank of Australia (**RBA**) and do all other things necessary to reduce systemic risk, ensure the CS facility's services are provided in a fair and effective way (to the extent that it is reasonably practicable to do so) and have adequate arrangements for supervising the facility.

ASX Clear and ASX Settlement are also required to have adequate arrangements for handling conflicts between the commercial interests of the licensee and the need for the licensee to ensure that the facility's services are provided in a fair and effective way. This includes having a 'CS Lead Executive' accountable to the CS Boards for the operation of the cash equities CS facilities, whose responsibilities include ensuring that any conflicts of interest between the CS subsidiaries and other ASX Group companies are identified and managed appropriately. The CEO is accountable for ensuring that sufficient resources are made available for the operation of the CS facilities.

The Clearing House Electronic Subregister System (CHES) is the system used by ASX Clear and ASX Settlement to facilitate clearing, settlement and other post-trade services for the Australian cash equities market. It is a critical piece of national financial market infrastructure and provides services to multiple Approved Market Operators (**AMOs**). The services that ASX Clear and ASX Settlement provide enable the management of clearing and settlement risks in the cash equities market and allow for the record of title to be maintained.

## 1.3 Recent History and Investment in CHES

CHES was established in 1994, replacing a predominantly paper-based process by electronically recording security holdings and managing the settlement of securities transactions. It remains a critical system in Australia's financial markets and has supported significant market changes including the dematerialisation of equities, shorter settlement cycles, changes to asset classes, the clearing and settlement of trades from AMOs, and the introduction of electronic CHES holding statements.

The steady operational performance of CHES is underpinned by resilient architecture and a program of ongoing investment, support, and maintenance. CHES has exceeded its target availability levels over the last ten years, achieving up time of 99.997%, and it has also had no major incidents or failed changes in the past twelve months.

While CHES had been delivering high service levels to its users for more than 20 years, there were factors emerging that led ASX to begin considering options to replace CHES. These included changing business needs (e.g., emergence and increasing use of global messaging standards), greater adoption of digital capabilities, and the shifting market dynamics requiring greater performance and scalability of CHES. At the same time, ASX was made aware that the vendor providing the operating system underpinning CHES couldn't confirm support for the product beyond 2020. While this vendor issue was resolved, ASX began considering options to replace CHES around 2015. Even as the CHES Replacement Project progressed, there remained commitment and focus for the continued investment to support and maintain the high performance and availability of CHES.

The process to evaluate replacement options for CHES came at a time when Distributed Ledger Technology (**DLT**) was emerging as a credible platform solution that could provide the kind of innovation and longevity which allowed CHES

to be world-leading when it was first introduced in 1994. By April 2018, following a two-year proof of concept process, ASX began an industry consultation process to assess business requirements for a DLT-based solution to replace CHES. In 2019, ASX confirmed it was targeting a go-live date for CHES Replacement of April 2021.

A key metric for CHES related to capacity planning is peak number of trades per day over specific periods including quarterly, annual and historical look back. Currently, to satisfy the capacity metric, ASX requires a headroom capacity of 100% over and above the peak number of trades. During 2019, ASX observed some periods of increased trading levels that triggered further work to expand capacity. In December 2019, a CHES database upgrade was completed, which when tested confirmed an expanded capacity of 7 million trades per day. In March 2020, as COVID-19 began taking hold, ASX witnessed an unprecedented increase in trading volumes sparked by pandemic driven market volatility. This period saw peak daily trade volumes increase from 3.3 million to 7 million. CHES experienced some delay in processing this increased activity at the time, highlighting the need for further capacity and performance improvements. Against this backdrop, ASX established a project to upgrade the underlying hardware of CHES to process increased trading volumes. By May 2021, CHES had increased its capacity to process 10 million trades per day which remains the current capacity.

While the COVID-19 period of increased volatility and unprecedented trade volumes drove a need to re-examine capacity for CHES, these same factors were also driving a re-evaluation of the performance requirements for CHES Replacement which in turn contributed to the re-baselining of the project plan and a revised go-live date of April 2023.

#### 1.4 Developing the CHES Roadmap to Address Risks

At an enterprise level, the management of risk is core to ASX's licence to operate. Risk is identified through rigorous and consistent practices across ASX with controls identified and improvement actions put in place to effectively mitigate risk to an acceptable level. Regular reporting of key risks, including CHES specific risks, occurs on a regular basis to the Boards, and ASX Management through established governance mechanisms.

By August 2022 the CHES Replacement Project confirmed it was unlikely to reach a go-live date before late 2024. Given this development, ASX undertook a significant review of the support and maintenance requirements of CHES. The assessment confirmed CHES could be supported through to 2025 as long as the key initiatives were put in place to manage specific risks. These findings were reported to ASX and CS Boards in September 2022, and the Technology Committee in November 2022.

Within the review, the risk assessments covered:

- Internal and external support capacity and capability.
- Technology asset obsolescence.
- System capacity and performance scalability.

The assessment determined that CHES could be supported and maintained and would meet ASX's requirements through to 2025, as long as some assumptions were maintained, and actions were taken.

The assumptions identified were daily trades per day processed by CHES did not exceed 10 million and an upgrade to the Hardware Security Module (**HSM**) devices would be compatible with CHES encryption algorithm.

The two key actions were upgrades to specific hardware and software and closing out actions from the review of CHES against ASX Security Standards.

In addition, the assessment determined that there was also scope for CHES to be supportable through to 2028, and this would be dependent on further analysis and improvements to system capacity, extended external hardware support and work to address any known or emerging risks.

ASX has already implemented various initiatives including hardware upgrades against the September 2022 assessment. This program of work was again reviewed in November 2022 when ASX confirmed it would pause the CHES Replacement Project without a defined timeframe for go-live. This collective program of work that commenced in September is referred to as the CHES Roadmap.

The CHES Roadmap has since been refined following the letter from the Australian Securities and Investments Commission (**ASIC**) received in December 2022. Among the requirements requested by ASIC was for ASX to consider the support and maintenance of CHES through to 2032. This lengthier planning horizon (**Extended Period**) now forms part of the CHES Roadmap, as discussed in this report.

Broadly, ASIC's letter requested information about how ASX is managing risks on the support and maintenance of CHES as it relates to four key areas: operation, security, continuity and governance. Following work undertaken as part of the risk assessment from last September and having regard to ASIC's request, ASX has identified a number of CHES risks which have been mapped to the 27 initiatives within the CHES Roadmap (For further details on the CHES Roadmap, refer to *Section 1.4.3 CHES Roadmap Summary* and further details on CHES risks, refer to *Appendix B – CHES Risks*). The majority of these risks, and therefore the focus of many of ASX's initiatives, centre on capacity and performance, as well as the fact that CHES is an aged asset. These initiatives are grouped under ASIC's theme of operation, to which ASX has aligned 16 initiatives. Of the remaining initiatives, six relate to security and five to continuity. No specific initiatives are called out for governance as these form part of ASX's Business As Usual (**BAU**) frameworks and processes (For further detail, refer to *Section 8 Governance*)

The CHES Roadmap initiatives have been identified through detailed risk assessments, which include a review of the application and solution architecture with a future outlook. Collectively the initiatives are designed to maintain ASX's low risk appetite for matters related to CHES. Each initiative maps back to a specific CHES risk which is recorded in ASX's enterprise risk management system and will enable ASX to address risks in relation to maintaining the operational reliability of CHES. The initiatives identified in this report are based on our current assessment of CHES risks. ASX's ongoing assessment of those risks will inform new initiatives in the CHES Roadmap over time.

## 1.5 Summarised ASX's response to ASIC Requirements

In responding to ASIC's requirements, the following sections summarise ASX's response:

**Table 1.5.A ASX Statements**

Section	ASX Statement
Support and maintenance of CHES	<b>ASX considers that its existing governance, investment, and management arrangements for CHES are commensurate with its role in providing critical financial market infrastructure.</b>
Future/Ongoing Investment in CHES	<b>ASX has and will continue to invest in and enhance CHES to support the long-term interests of Australia's financial markets and meet applicable regulatory requirements, including the FSS. ASX has a program of work to enhance CHES to ensure it remains operationally reliable until a new solution is implemented.</b>

### 1.5.1 Support and Maintenance of CHES

**ASX considers that its existing governance, investment, and management arrangements for CHES are commensurate with its role in providing critical financial market infrastructure.**

#### 1.5.1.1 Risk Management Practices

**CHES is underpinned by robust risk management processes and governance structures.** Risk management activities are integrated across all areas of CHES. Robust risk management processes are in place to identify, assess, manage, and monitor risks, drawing from across business divisions and at different levels of management and oversight. Key CHES risks, including mitigations, are reported regularly to the Securities & Payments (**S&P**) business unit, executive management and the ASX Group Boards. Controls addressing risks are evaluated and initiatives are put in place to address risks outside tolerance.



**ASX has adopted a layered approach to controls and monitoring.** At each level within the Three Lines of Defence, there are various assessments and activities that are undertaken to measure, assess and continually improve and assure the ongoing resilience, reliability, integrity, and security of CHES. These include risk self-assessments, security audits, project delivery assurance, Line 2 risk challenges, and framework audits. The outcomes of these internal assessments feed into continuous improvement work and into the overall risk management and reporting mechanisms up through to executive management and the ASX Group Boards to refine risk management and the view of controls effectiveness at ASX. These internal views are supplemented by an annual independent external ASAE 3402 Assurance Report on Controls at a Service Organisation for CHES, which covers control objectives around logical access, changes to CHES, physical security, recovery, and daily processing. The external auditor has issued unqualified opinions for the last 5 years.

#### 1.5.1.2 Operation

**ASX has mature practices in place to ensure that CHES functionality continues to meet regulatory requirements and broader market needs.** Underpinning this practice is a product management process executed via the *ASX Delivery Governance Model* to ensure that the functionality of CHES continues to meet the needs of the markets, our customers and the regulatory requirements. Appropriate review, prioritisation, approval and funding are achieved via the various ASX Governance forums and delivery via the *ASX Delivery Framework*. ASX engages with stakeholders through various channels to support the process of identifying any modification or introduction of functionality required to CHES. Engagement activity includes meetings with Participants, Share Registries and AMOs, formal consultation processes, and involvement in industry forums and associations.

ASX also regularly engages with its regulators ASIC and RBA on CHES and its functionality, for example, through regularly scheduled staff-level meetings and periodic supervisory assessments conducted by the regulators. ASX is expected by the RBA to achieve a number of specific outcomes regarding the functionality of CHES in the short term, which are covered in *Section 5.2 Product Management*.

**CHES's architecture is resilient and reliable, as evident from its historical performance.** CHES, though legacy in nature, is built on a highly resilient architecture that ensures data and transactions are not lost during any incidents. This includes the use of distanced primary and secondary data centres and architectural components which incorporate redundancy and facilitate failovers between these sites.

**CHES continues to meet or exceed availability service level objectives.** Over the last 10 years, CHES has exceeded its target availability SLA of 99.80%, achieving 99.997%, with no major incidents and no failed changes in the last twelve months. ASX utilises a range of Key Performance Indicators (KPIs) to monitor the ongoing performance of CHES. The key areas monitored, measured, and managed through performance reporting and system monitoring tools include KPIs over the availability of services, capacity planning, change management, and incident management.

Maintaining service availability, efficient management of resources, and optimisation of system performance by forecasting future performance and capacity requirements ensures the service meets future needs.

**CHES has the capacity to meet market demand with headroom for growth based on current forecasting methods.** Operationally, CHES capacity is closely monitored, and modelling is in place to forecast capacity and manage headroom. The purpose of managing availability and capacity is to ensure that the CHES service achieves agreed and expected availability, performance, and capacity requirements to meet current and future business needs.

ASX continues to make upgrades to the infrastructure and components of CHES to uplift headroom capacity. The impacts and learnings, both internal and external to ASX, from the record peak day trading volume in March 2020 caused ASX to make further upgrades to the CHES infrastructure and software components throughout 2020 to 2021 to immediately increase the headroom capacity. Post these upgrades, CHES has been tested and validated to process 10 million trades per day. Based on current modelling<sup>1</sup>, forecast trades per day are expected to reach a peak of 5 million transactions by February 2025 and 10 million transactions by April 2030. The current rolling daily peak trading volume over 24 month period is 4.8 million trades, and the rolling daily peak volume over 3 month period is 2.3 million

---

<sup>1</sup> Modelling conducted in February 2023

as of February 2023. ASX recognises the forecast modelling requires greater sophistication and this is on the CHES Roadmap.

**CHES is supported by operational capabilities to maintain the system through the Extended Period.** CHES is an in-house developed application supported by internal ASX teams, including the Technology and Operations team in the Securities & Payments (**S&P**) division and teams in the Technology & Data division. The S&P Operations and Technology teams have extensive experience and operate under frameworks, practices, and policies to support their business and technology operations.

The majority of capabilities supporting CHES reside internally within ASX. Internal resourcing needs are managed via a structured set of processes to forecast the investment required in human capital to ensure the ongoing maintenance and support of CHES. These processes forecast resourcing needs based on the skills, capabilities, and capacity required. Given the Extended Period, additional capabilities have been recruited to support CHES.

Given the Extended Period, initiatives are in place or underway to review support and operational performance capabilities, including the extent to which additional vendor and/or supplementary external support capabilities are required.

**Structured processes are in place to manage changes to CHES and avoid obsolescence.** Material changes to CHES are subject to formal change management processes, including the application of the *ASX Delivery Framework*, requirements for formal change assessment, appropriate testing, controlled release processes, and approvals. Internal and external communication mechanisms are in place to ensure that impacted stakeholders are informed of changes.

ASX aligns its IT Asset Management processes with the *COBIT 5 framework* by planning, acquiring, deploying, maintaining, and disposing of aged assets to avoid technology obsolescence, reduce operational risks, and improve operational efficiency. The process involves tracking and monitoring IT assets relating to configuration management, asset end of life, and roadmap activities to maintain support for CHES.

### 1.5.1.3 Security

**ASX has deployed a 'defence in depth' strategy in the management of security risk, with controls implemented at various levels of the technology stack.** These layered controls comprise both enterprise controls that are common across the organisation and controls that are specific to the CHES environment. The controls are designed to achieve the objectives of security risk management: the identification, protection and detection of security threats and the response and recovery from security incidents.

**The ASX 'defence in depth' approach has been employed across the security control domains, ensuring there are multi-layered controls in place to address security** as it relates to access management, data security, systems security, threat and vulnerability management, and security monitoring and response.

**ASX considers cyber security to be one of the organisation's top three risks and has adopted a risk management strategy that is commensurate with this assessment.** When assessing the risks associated with cyber security, the Cyber Security team consider a range of factors, including the business objectives, key information assets, business and technology strategy, cyber trends, and the evolving cyber threat landscape. Cyber risk is managed in accordance with the *Enterprise Risk Management (ERM) Framework*.

**The security controls at ASX including those applicable to the CHES environment have been grouped into six domains and oversighted and implemented by an enterprise security function:**

- Security Strategy, Governance and Risk Management Controls.
- IAM Controls.
- Data Security Controls.
- Systems Security Controls.
- Threat and Vulnerability Management Controls.
- Security Monitoring and Response Controls.

These six domains address the key dimensions of cyber security, i.e., Confidentiality, Integrity, and Availability of CHES and the underlying data and help ensure CHES is resilient to unauthorised access or disruptions due to cyber events.

**There is Board and Board Technical Committee level oversight and approval of the *Cyber Security Strategy* to ensure it remains commensurate with the overall risk environment.** The strategy is developed through consultation, analysis, and assessment of a number of information sources, including an assessment of the risks to the ASX environment, analysis of the current and future threat environment, industry research, consultation with SMEs, results of audits and penetration tests, overall ASX business strategy and an analysis of incidents and KRIs. It is formally reviewed and approved annually by ASX Limited and CS Boards, and funding is provided to support the delivery of cybersecurity initiatives.

**Multi layered access controls are in place for internal and external users of CHES.** CHES is contained within a closed network, not exposed to the internet, and accessible only to known participants who interact with CHES via their own systems via the message-based interface. There are internal controls in place around identity management, passwords and use of multi-factor authentication, privileged user access management and logging of access for internal ASX CHES users. Participants who connect to the CHES environment are authenticated and authorised using a number of identification attributes that are designed to uniquely identify and authenticate communication between the CHES and participant systems. The assignment of these attributes follows a standard onboarding approval process. Participant user management is performed by the participant.

**A layered 'defence in depth' approach is in place to maintain the confidentiality, integrity, and availability of CHES data throughout the information lifecycle.** Control domains around data security include governance, data lifecycle management, data classification, and security of data (including physical, logical, and system and network security). These domains are applied to ensure that data is secured throughout its lifecycle and as it passes through various layers of the technology stack.

**Security controls and procedures are also implemented in a layered approach to ensure sufficient controls exist from the ASX perimeter to the back-end infrastructure.** The ASX Security Team, which operates on an enterprise level, is responsible for assessing the security requirements and overseeing the management and maintenance of the security controls and procedures. These include perimeter and email controls, operational and access management controls, end point controls, network controls, policies and procedures, network, hardware, and operating system security, as well as user training and awareness.

**Threat and vulnerability management is in place across ASX and the CHES environment.** Threats and vulnerabilities are identified through a number of sources. Threat assessment and analysis is performed centrally, and remedial activity is performed by the relevant teams. In line with the organisation's patching policy, ASX has implemented processes, standards, and technology to proactively prevent, detect, and remediate vulnerabilities.

**Enterprise wide capabilities are in place that enable continuous monitoring of systems and infrastructure, including CHES.** A centralised Security Information and Event Management (SIEM) solution has been deployed that monitors and correlates logs/security events from multiple sources to proactively identify early indicators of security incidents. This technology is complemented by detailed incident response processes and run books to help with timely detection and security incident response. In addition, monitoring of operational activity is performed by the application support teams.

**The effectiveness of the security controls is monitored via a combination of internal and external assurance activities.** Internally, these include the overall monitoring of controls addressing CHES risks as part of the *ASX ERM Framework*, periodic threat hunting exercises, regular red/purple teaming exercises to validate the efficacy of preventative and detective security controls, participation in external forums (e.g., Australian Cyber Security Centre (ACSC) 'Capture the Flag' and 'Scenario Testing'), team discussion and awareness activities and facilitated specialist incident simulations. Externally, this includes engaging ASX's external auditors to provide an annual ASAE 3402 Assurance Report on Controls at a Service Organisation for CHES, which covers control objectives around logical access, changes to CHES, physical security, recovery, and daily processing.

#### 1.5.1.4 Continuity

**Recognising the importance of CHES as a critical system in Australia's financial market infrastructure, CHES is built on highly resilient architecture, which ensures that data and transactions are not lost during any incidents.** The performance of CHES continues to be reliable, stable, and resilient, where actual availability over the last ten years is at 99.997%, exceeding the target of 99.80%. Notwithstanding, there have been individual isolated incidents where users of the system have experienced connectivity interruptions, but these do not affect overall system availability, which is what is captured by the availability KPI.

The key resiliency related components of CHES architecture include Dual Site Data centre, like-for-like hosting and configuration across both the primary and secondary sites enabling takeover by the second site should there be a failure. Within the hosting infrastructure, a number of components are designed to support resilience, ranging from front-end servers, messaging middleware, back-end application nodes, database, log servers, and application control servers.

CHES resiliency is further enabled by:

- **Load Balancers** – Distribute message traffic across CHES front-end components and assist in redirecting traffic to the secondary data centre in the event of a disruption scenario.
- **Storage** – Enterprise storage arrays provide the required storage processing power for both the primary and secondary data centres and support the synchronous replication of data [REDACTED] from the primary site to the secondary site.
- **Network Connectivity** – High speed shared network is available across both the primary and secondary data centres for data traffic and supporting data replication. The networks consist of redundant devices that allow continuity of operations during failures.

**ASX has an enterprise-wide Business Continuity Management Framework (BCMF) which guides the specific approach to business continuity planning, testing and backups and recovery.** The approach is aligned with international best practices and considers response and recovery processes for events that could cause the unavailability of CHES. The BCMF consists of four pillars covering the approach and oversight of Business Continuity Management (BCM), which includes crisis management, Business Continuity (BC), business resumption, exercise and awareness. Specific BC and technology Disaster Recovery (DR) plans for CHES and relevant internal systems have been defined and tested. This is supported by regular backup and recovery processes to ensure systems, data and access can be re-established following a disruption event.

**ASX performs annual BC and DR testing for CHES to test ASX's ability to respond and deliver critical operations in the event of technology disruption.** The CHES application is failed over and operated from the secondary data centre site for a week before reverting to the primary site. Permanent dual-site operational teams are based at both the primary and alternate operations sites (including the use of remote working arrangements), which effectively tests backup operational processes on a continuous basis and ensures that the alternate site can always be fully operational.

**Scenario based risk assessments are also performed to confirm that the BC model remains appropriate.** Scenario risk assessments are conducted to consider potential crisis/disaster incident scenarios, evaluate event likelihood factors and test the current control environment in place. The *Business Continuity Scenario Risk Assessment* details example scenarios for each site (primary and secondary) grouped under relevant risk event scenarios. The relative likelihood is then considered by assessing various factors that may increase or decrease the likelihood of an incident. These assessments are in addition to the existing vulnerability and threat assessment activities covered as part of managing security over CHES.

#### 1.5.1.5 Governance

**Governance arrangements provide visibility of CHES service performance, including availability, resilience and risk.** Detailed governance and oversight arrangements are in place with clearly defined roles and responsibilities. This ensures the ongoing monitoring and management of any risks to the performance and operation of CHES and provides

visibility of the availability of its services and adequacy of financial, technological, and human resources (including external parties and outsourced services).

**Regular CHES performance reporting against KPIs and SLAs is provided to executive management and the ASX Group Boards.** Regular monitoring of key metrics and KPIs is in place, which covers IT Service Management (ITSM) performance, capacity reporting, open risk items, open audit actions, resource pipeline, current upgrades, upcoming upgrade projects, and future projects. This allows for the monitoring, measurement and management of service availability, capacity planning, change management and incident management as it relates to CHES.

**Risk management forms a key part of governance oversight.** An ERM framework and an ASX Project Risk Management Framework guide the identification, assessment, management, and monitoring of risks across ASX, including risks associated with CHES. Risk is assessed at an enterprise, business unit, system, and project level through regular reviews. ASX adopts a Three Lines of Defence model, which provides a clear organisational structure and clarifies roles and responsibilities for managing risks and controls across the business. Regular risk reporting is provided to executive management and the ASX Group Boards.

**CHES is adequately supported from a financial, technological, and human capital perspective based on current projections of future growth.** The financial support requirements of CHES, outside of any future major upgrade, are well defined and included in the annual capital expenditure and operating expenditure budgets for ASX and are subject to internal review and approval. Technologically, CHES is stable, fully supported, and able to meet market demands. It has also been assessed as having sufficient headroom to accommodate projected future growth. Work is underway as part of the CHES Roadmap to ensure CHES continues to be stable, secure, fully supported and able to meet the required levels of forecasted support and capacity.

From a resourcing perspective, ASX has a structured set of processes and governance structures in place to forecast the investment required in human capital to ensure the ongoing maintenance and support of CHES. This is underpinned by a set of processes and practices to forecast resourcing needs based on the skills, capabilities and capacity required. The majority of capabilities to support CHES reside internally within ASX, while external capabilities are leveraged through services, tools, and licences to supplement as required. Based on the CHES Roadmap, the proposed human capital investment is expected to be in line with current resource capacity requirements.

### 1.5.2 Future Investment of CHES

**ASX has and will continue to invest in and enhance CHES to support the long-term interests of Australia's financial markets and meet applicable regulatory requirements, including the FSS. ASX has a program of work to enhance CHES to ensure it remains operationally reliable until a new solution is implemented.**

The CHES Roadmap is regularly updated to ensure it evolves to meet the applicable regulatory requirements, including under the FSS and continues to meet the demands of the market. The CHES Roadmap defines the key initiatives that are driving CHES capability uplifts and actions to address gaps and risks across people, processes, and technologies.

The implementation of certain roadmap initiatives commenced in November 2022, as outlined in this report (For detailed roadmap descriptions, refer to *Section 9 Detailed Roadmap*). For other initiatives, further planning is being conducted. The CHES Roadmap reflects these planning initiatives and key decision dates and will be regularly updated to reflect implementation activities post planning.

While the planning horizon for the CHES Roadmap runs to 2032, and the CHES Roadmap initiatives covered in this report go up to 2025. The reasons for this include:

- Most known key initiatives will be delivered by the end of 2025.
- Many suppliers providing products for CHES do not have their own roadmap beyond 2025. (There are dependencies on product vendor(s) where the roadmap has limited visibility to 2032).
- Some initiatives are in the planning stage and the CHES Roadmap will be updated once planning is completed, which may extend the delivery timeline beyond 2025.
- The roadmap contemplates future (currently unknown) business needs and requirements, which will be reflected in the roadmap once industry consultation on these needs has been completed.

The CHES Roadmap remains a 'living' document and will be updated to reflect new initiatives as they are identified/needed. Any addition or removal of initiatives, as well as the finalisation of the scope of the initiatives will be governed by the Strategic Guidance Group (SGG).

ASX will update its policies and frameworks that apply to CHES as applicable standards evolve and will take into account industry best practices in this regard.

The Group Executive, S&P has been identified as the 'CS Lead Executive' accountable to the CS Boards for the operation of the cash equities CS facilities. The CS Lead Executive has endorsed the CHES Roadmap and briefed the CS Boards on the details of the deliverables. Management will continue to update the CS Boards and regulators on progress.

ASX will closely track the progress of these initiatives as per the existing ASX Delivery and Project Governance processes and frameworks. Management and the Boards will be appraised on the progress and risks regularly. In cases initiatives require further contingency planning, additional measures will be initiated, reported and monitored via the CHES Roadmap governance. Based on ASX's progress to date, there is no contingency planning required at this time for the existing CHES Roadmap initiatives.

ASX will provide appropriate transparency to market stakeholders through regular updates using standard communication channels and undertake assurance activities over the roadmap progress via ASX Internal Audit and/or independent external audits. While not explicitly identified on the roadmap, an assurance program regarding the completion (or non-completion) of each of the identified initiatives will be developed and then implemented to ensure the initiatives are meeting their risk objectives.

### 1.5.3 CHES Roadmap Summary

The CHES Roadmap currently contains 27 key initiatives which link to specific CHES risks, including Reliability, Availability, Resourcing, IT Asset, Compliance, Performance, Capacity and Security. Each initiative is allocated to an owner within the relevant business division that is responsible for delivery, with sub-owners supporting more complex initiatives. Additionally, the 27 initiatives are also grouped across four themes from the ASIC requirements: Operation (16 initiatives), Security (six initiatives), Continuity (five initiatives) and Governance (initiatives delivered through BAU activities).

#### 1.5.3.1 Operation

ASX has defined 16 CHES operational enhancement initiatives with the following themes:

- **Capacity, Availability and Performance** – develop and imbed a more predictive trade forecasting model, improve the capacity management framework, conduct a stress test for over 10 million trades per day to identify breakpoints, assess and develop possible capacity and performance uplifts and remove dependency from internal upstream dependent system.
- **IT Asset Management** – provision and uplift of assets and services required to meet all obligations in accordance with defined CHES operation requirements and service levels. This involves software and infrastructure upgrades to address obsolescence and maintain supportability.

#### 1.5.3.2 Security

The current roadmap includes six key security initiatives to improve policies and procedures and to facilitate ongoing awareness and monitoring of threats in line with industry best practices and ASX's internal risk assessments.

#### 1.5.3.3 Continuity

Five initiatives have been defined to ensure CHES and its underlying systems are tested to enhance and expand on various disruption scenarios. This includes initiatives to review and refine CHES scenario testing, [REDACTED]

#### 1.5.3.4 Governance

Governance based initiatives have not been depicted in the roadmap.

## CHES Roadmap



NOTE: Risk & Governance based initiatives have not been depicted in the above roadmap as they are considered ongoing and business as usual in nature.  
 O-12 [REDACTED] this initiative falls outside the roadmap calendar range (target date is Dec 26). \*These initiatives contain multiple phases. Please refer to the initiatives list for further details.  
 ▲ Indicative implementation dates ▲ Completed initiatives

Figure 1.4.3.4.A CHES Roadmap

## 2. Scope of the Report

### 2.1 Summary of ASIC Requirements

ASIC's requirements for ASX to respond with respect to CHESS are grouped into the four themes of Operation, Security, Continuity and Governance. For detailed mapping of ASIC Requirements to ASX Responses, refer to *Section 4 Structure of ASX Response*)

- **Operation** – Details how ASX will identify, assess, manage, and monitor any risks to the resilience, reliability, integrity and security of CHESS; how ASX will ensure CHESS has the appropriate functionality and the safe and secure implementation of material changes; and identifies how ASX will ensure the necessary upgrades to avoid technology obsolescence and ensure it can support the scalable capacity and performance of CHESS to accommodate current and future trading volumes.
- **Security** – Details how ASX will ensure the confidentiality, integrity and availability of information and implement a system of security controls to ensure CHESS is resilient to unauthorised access of CHESS data or disruptions due to cyber events.
- **Continuity** – Details how ASX will implement, test, and maintain continuity plans to ensure disruptions scenarios are periodically tested, including regular backup and recovery, and resources that are required to engage with such plans are across the training and familiar with their responsibilities.
- **Governance** – Details how ASX will ensure that there is a system of controls, governance arrangements and frameworks to monitor the risks that may impact the performance and operation of CHESS, including resourcing and vendor support; how ASX ensures it has the requisite skills and capabilities, and the system of controls and monitoring in place to measure, assess and continuously improve and assure the ongoing resilience, reliability, integrity, and security of CHESS.

ASX's consideration of the steps it will need to take to ensure that CHESS is adequately supported and maintained until the go-live of the CHESS Replacement System, as described in this report, has not been restricted to the matters described in the four themes identified above.

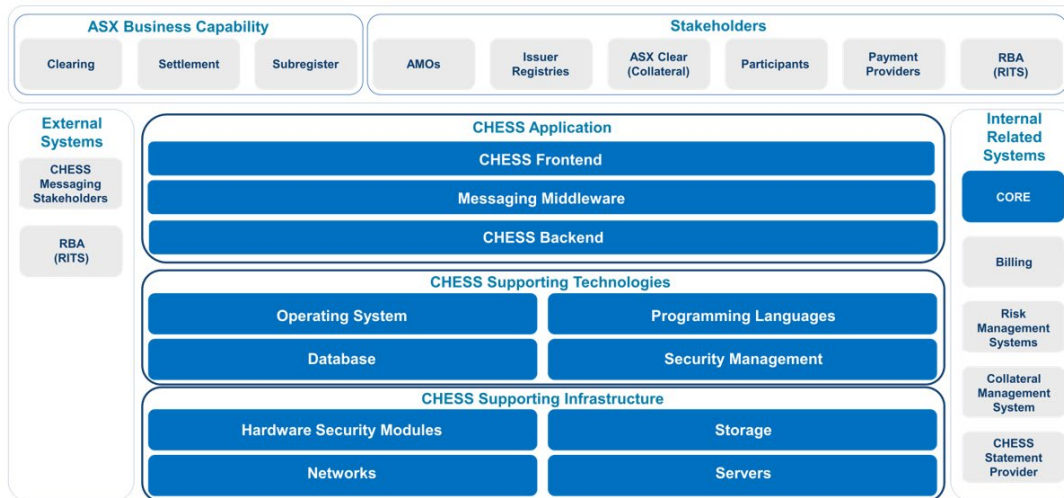
### 2.2 The CHESS Architecture

CHESS operates within an ecosystem *Figure 2.2.A CHESS Ecosystem* represents a visual summary of the ecosystem, including the Clearing, Settlement and Subregister business capabilities, the stakeholder groups and CHESS users, the CHESS application and the associated technology stack, and the key internal and external systems that CHESS interacts with. The boxes coloured blue are considered in the scope of this report.

For the purposes of this report, CHESS is defined as comprising of CHESS Application, CHESS Supporting Technologies and CHESS Supporting Infrastructure.

External Systems and Internal Related Systems (other than CORE) as identified in *Figure 2.2.A CHESS Ecosystem* are not included in the scope of this report.





**Figure 2.2.A CHESSEcosystem**

### 2.3 The CHESSEcosystem Application

The CHESSEcosystem application is made up of three logical components the “front-end”, the messaging middleware, and the “backend”.

- The “front-end” is responsible for managing secure CHESSEcosystem messaging sessions. CHESSEcosystem users establish CHESSEcosystem messaging sessions and while they are logged on, they can send and receive encrypted messages conveying information about settlement obligations, accounts, holdings, and other transactions. CHESSEcosystem messaging is always available except for part of the CHESSEcosystem overnight processing and where CHESSEcosystem is taken offline for backups.
- The messaging middleware is a purpose-built store and forward message broker that provides a loosely coupled persistent interface between the front-end and the functional backend processing.
- The “backend” is comprised of distinct functional components that specialise in particular aspects of CHESSEcosystem processing and maintenance of the associated data in CHESSEcosystem.

### 2.4 CHESSEcosystem Dependency on CORE

The number of trades submitted to CHESSEcosystem by AMOs (being Cboe Australia Pty Ltd (**Cboe**), National Stock Exchange of Australia Limited (**NSX**) and ASX Trade) for registration has a direct impact on CHESSEcosystem. Trades reported by Cboe and NSX are received into CHESSEcosystem via the CHESSEcosystem Messaging interface. However, trades received from ASX Trade are received by CHESSEcosystem via an internal middleware system called CORE. CORE is also the source of the security reference data. CHESSEcosystem, therefore, has a dependency on CORE to receive and process ASX Trade sourced market trades.

### 2.5 Scope of Technology Components

This report covers the CHESSEcosystem Application, CHESSEcosystem Supporting Technologies and CHESSEcosystem Supporting Infrastructure. Consideration was also given to whether any additional internal related systems should be included in the scope. ASX has determined that a related internal system should be included in the scope if it has the potential to materially impact the reliability and resilience of CHESSEcosystem. The CORE system meets that description and so it has been addressed in this report. The other internal systems do not.

### 3. Governance and Risk Arrangements

ASX has in place a structured and robust governance framework to ensure clarity on the different roles and responsibilities for the monitoring and management of risks relating to the performance and operation of CHES. While S&P is the sponsoring business for CHES and responsible for the external delivery of the CHES capability, the governance framework includes monitoring and managing the performance and operation of CHES.

#### 3.1 ASX Governance Arrangements in Relation to CHES

ASX's governance arrangements can be summarised into four layers – **Board Governance**, **Management Governance**, **Project Governance** and **Performance and Operations**. The governance arrangements are intended to ensure that risks, including those related to CHES, are identified, assessed, managed, and monitored.

The **Board Governance** layer focuses on the role and responsibilities of the ASX Group Boards and Board Committees relating to the ongoing operation of enterprise-wide technology and operating infrastructure and delivery of large technology projects, including delivery of the CHES Roadmap. The ASX Group Boards and Board Committees receive regular reports from management on the operation of CHES and the CHES Roadmap. These reporting mechanisms provide details on a regular basis on the status of CHES related risks and initiatives.

The **Management Governance** layer focuses on the role and responsibilities of the Chief Executive Officer (CEO) and Group Executives relating to the ongoing operation of enterprise-wide technology infrastructure and delivery of large technology projects, including the delivery of the CHES Roadmap. ASX has established a number of management committees comprised of senior executives to assist with the oversight and management of risks, including those related to the operation of CHES and the CHES Roadmap.

The third layer of governance in relation to CHES is **Project Governance** which can be summarised into three key pillars – ASX enterprise portfolio & project governance, S&P Governance and CHES Roadmap Governance. These bodies are responsible for providing governance, risk management, project delivery capability and oversight.

The fourth layer of governance in relation to CHES is the arrangements relating to **Performance and Operations**. The S&P division is responsible for managing and monitoring CHES. Within this layer resides the Technology and Data division which is responsible for supporting the security, architecture and underlying infrastructure for CHES.

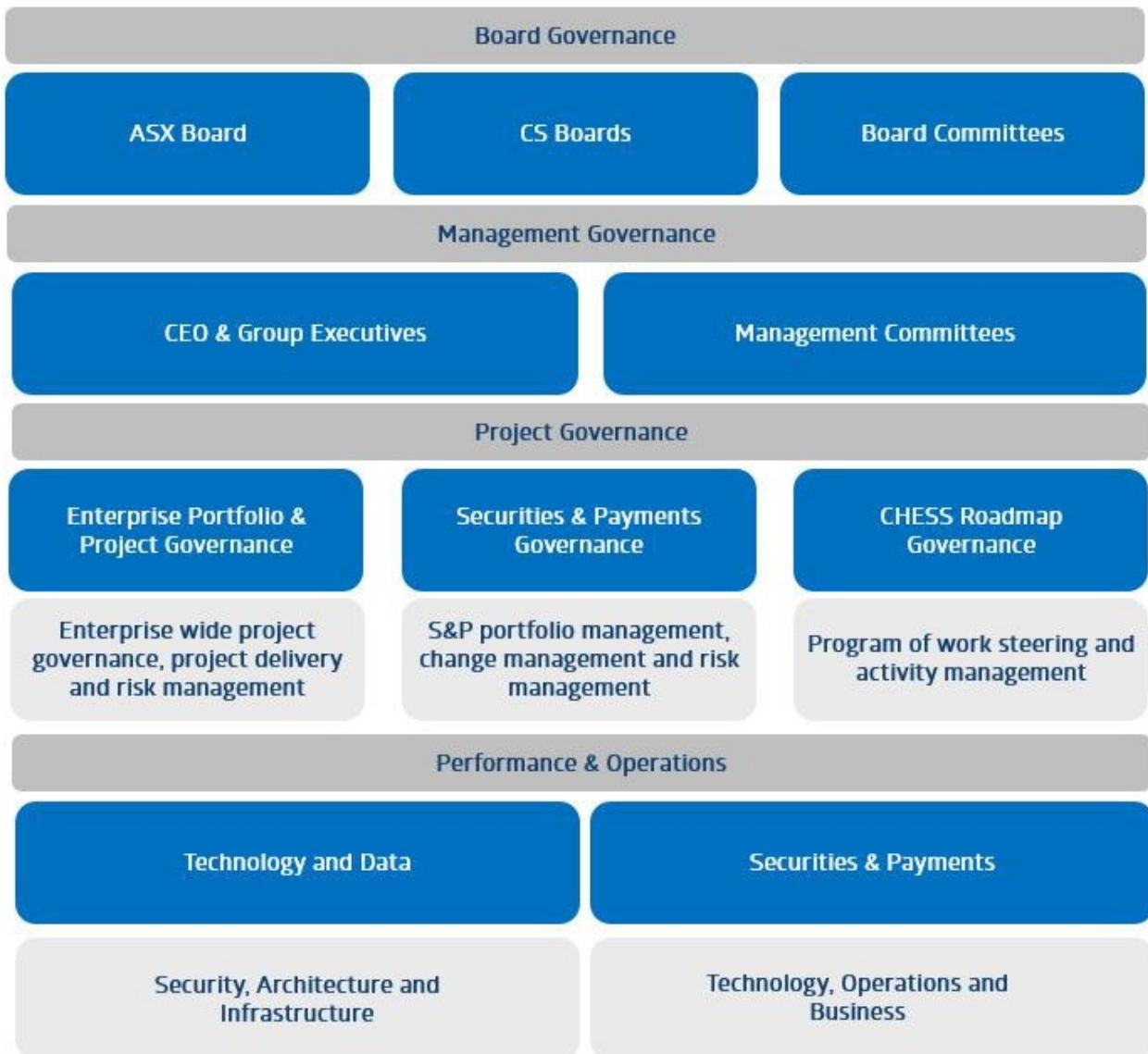


Figure 3.1.A ASX Governance Structures Overview of CHES

Section 3.2 Roles & Responsibilities of the ASX Group Boards and Section 3.3 Roles & Responsibilities of Management describe the **Board Governance and Management Governance** layers outlined above. Section 8.1 Governance Structure and Supporting Processes outlines the **Project Governance and Performance and Operation** layers.

### 3.2 Roles and Responsibilities of the ASX Group Boards

#### 3.2.1 ASX Limited Board

The role of the ASX Board is to provide leadership, guidance, and oversight for ASX Limited and its related bodies corporate (**ASX Group**), which includes ASX Clear and ASX Settlement. The ASX Board has a charter that sets out its composition, operating procedures, and the allocation of responsibilities between the ASX Board, CS Boards, Board Committees, and management. The ASX Limited Board Charter is published on the ASX Website.

The ASX Board’s responsibilities relevant to the operation and performance of CHES and the CHES Roadmap include:

- Approving the annual budget and financial plans.
- Approving major corporate initiatives, including capital expenditure.
- Setting ASX's risk strategy and risk appetite.
- Overseeing ASX's overall risk management framework and its operation by management and the processes for identifying significant risks facing the ASX Group.
- Overseeing systems of risk management and internal controls and compliance.
- Satisfying itself that appropriate controls, monitoring, and reporting mechanisms are in place.

### 3.2.2 Clearing and Settlement Boards

The role of the CS Boards is to provide leadership, guidance, and oversight of the CS operations of the CS facility licensees, which include ASX Clear and ASX Settlement. The CS Boards have their own charter that sets out their composition, operating procedures, and responsibilities. The CS Boards Charter is published on the ASX Website.

The CS Boards have broad responsibilities for the oversight of the CS facilities, including being responsible for:

- Approving the strategy developed by management to comply with the CS facility licensees' statutory and regulatory obligations and monitoring the execution of that strategy.
- Setting the operational risk tolerances for the CS facility licensees.
- Overseeing management systems and processes for the purposes of ongoing compliance with the FSS and the CS facility licensees' statutory and licence obligations.
- Reviewing and approving the risk management framework.
- Overseeing the adequacy of internal controls, systems and processes for the management of clearing and settlement risk of the CS facilities.
- Managing the CS facilities within the ASX risk appetite and operational risk tolerances set by the CS Boards.

The CS Boards regularly receive reports from management on the operation and performance of CHES. Since the decision to pause the CHES Replacement Project, the CS Boards have also received a dedicated report on CHES and the CHES Roadmap from the Group Executive S&P. The Chairs of the Technology Committee and the Audit and Risk Committee (**ARC**) also report to the CS Boards and ASX Board on matters considered by those Board Committees.

### 3.2.3 Board Committees

The ASX Board has established four Board Committees to assist it in discharging its responsibilities – ARC, Technology Committee, People and Culture Committee and the Nomination Committee. The role and responsibilities of each Board Committee is set out in a charter that is published on the ASX website. The four Board Committees also perform their responsibilities for the CS Boards.

The two Board Committees most relevant to the operation and performance of CHES and the CHES Roadmap are the Technology Committee and the ARC.

#### 3.2.3.1 Technology Committee

The Technology Committee was established as a committee of the ASX Board and the CS Boards in May 2022 to strengthen Board oversight of technology and data related strategies, operations, investments and projects, as well as technology related risks, including cyber security risks. This is the primary Board Committee with oversight of the operation and performance of CHES and the CHES Roadmap.

The responsibilities of the Technology Committee include:

- Overseeing the implementation of the ASX Group's technology, data, and cyber security strategies.
- Receiving reports from management on the performance of the ASX Group's technology systems, with a focus on those systems supporting licensed activities.
- Overseeing the ASX Group's arrangements for managing system risk associated with technology assets.
- Overseeing and reviewing annually the adequacy of the strategy for identifying, mitigating and managing the ASX Group's cyber risks.
- Overseeing the effectiveness of the ASX Group's cyber resilience risk control systems.

- Overseeing the ASX Group's strategies for mitigating and managing technology, delivery, and data risks.

The Technology Committee also assists the CS Boards in reviewing and overseeing the arrangements in place to achieve compliance by the CS facility licensees with their statutory obligations as licence holders in relation to the technological resources and human resources (with respect to technology) for operating the CS facilities.

The Technology Committee receives regular reports from the Chief Information Officer (**CIO**) on technology and cyber security risks and from the Chief Customer and Operating Officer on project and operational risks. Since the decision to pause the CHES Replacement Project, the Technology Committee has also received a dedicated report on the operation and performance of CHES and the CHES Roadmap from the Group Executive S&P.

### 3.2.3.2 Audit and Risk Committee

The role of the ARC includes assisting the ASX Board to discharge its responsibilities related to overseeing the identification of significant risks facing the ASX Group and arrangements for implementing appropriate controls, monitoring, and reporting mechanisms.

The ARC has also been appointed as the ARC of the CS Boards in respect of a number of matters, including overseeing risk matters that are outside the areas reviewed by the Technology Committee and CS Boards. ARC also oversees the preparation of the Cash Market Clearing and Cash Market Settlement Management Income Statements and the ASX internal cost allocation and transfer policy between ASX Group entities for clearing and settlement of cash equities.

The ARC also assists the CS Boards in reviewing and overseeing the arrangements in place to achieve compliance by the CS facility licensees with their statutory obligations as licence holders, with the exception of those matters carried out by the Technology Committee.

Since the Technology Committee was established in May 2022, the ARC is no longer responsible for oversight of technology risks. However, the ARC does review and provide oversight of the ASX Group's response to significant operational incidents, including those relating to technology performance.

The ARC receives regular reports from the Chief Financial Officer (**CFO**) on financial matters, the Chief Risk Officer (**CRO**) on enterprise risk matters, the Chief Compliance Officer on matters relating to the monitoring and enforcement of compliance with ASX's operating rules, as well as reports from ASX's internal and external auditors.

## 3.3 Roles and Responsibilities of Management

The ASX Board has delegated the day-to-day management of ASX and the implementation of approved strategies to the Managing Director and CEO, who in turn delegates to the executive management team subject to the financial and other limits set by the Board. The CEO is accountable to the Board for the authority delegated to all levels of management.

The CEO's key responsibilities include:

- Developing ASX's strategic objectives and strategies for Board approval.
- Executing the Board-approved strategy and achieving ASX's strategic objectives.
- Day-to-day management and operation of ASX in accordance with the risk appetite set by the Board, the policies and procedures adopted by the Board, and the implementation of processes, policies, systems, and controls that are necessary or appropriate to manage the ASX Group.
- Timely presentation of information to the Board to enable the Board to fulfil its responsibilities.

The CS Boards have also delegated day-to-day management of the CS Subsidiaries to the CEO. The CEO's key responsibilities in respect of the CS Subsidiaries include:

- Implementing the strategy and achieving the business objectives for the CS Boards.
- Day-to-day management and operation of the CS Subsidiaries in accordance with applicable policies and procedures adopted by the CS Boards and ASX Board.
- Timely presentation of information to the Board to enable the Board to fulfil its responsibilities.

The CEO has established an executive management team comprising the CEO and all Group Executives. The Executive Team meets regularly, and meetings are normally chaired by the CEO. The Executive Team operates in parallel to the formal management committees (see below) and considers business division updates, strategy, new business initiatives, non-risk related frameworks, people matters, budgets, risk, and escalation issues.

ASX has written agreements in place with executives setting out the terms of their appointment. Accountability statements have also been put in place for all ASX executives setting out the allocation of responsibilities to executives across ASX's operations.

The Group Executive, S&P has been identified as the 'CS Lead Executive' accountable to the CS Boards for the operation of the cash equities CS facilities. The responsibilities of the CS Lead Executive include ensuring that any conflicts of interest between the CS subsidiaries and other ASX Group companies are identified and managed appropriately. The CEO is accountable for ensuring that sufficient resources are made available for the operation of the CS facilities.

Resources are typically made available to ASX Group companies through ASX Operations Pty Limited, a wholly owned subsidiary of ASX. This includes financial, human, and technological resources and any other resources required by the ASX Group. This arrangement is governed by an intragroup support agreement.

ASX has established the following management committees comprised of senior executives to assist with the oversight and management of risks<sup>2</sup>: Technology Management Committee (**TMC**), Risk Committee and Regulatory Committee.

### 3.3.1 Technology Management Committee

The TMC is a senior management committee chaired by the CIO. The CIO exercises delegated authority from the CEO to oversee ASX's technology and cyber security strategies and the investments to support such strategies and is the sole decision maker on the Committee.

The key responsibilities of the TMC are to:

- Review and, as appropriate, make recommendations to the Board regarding enterprise-wide technology and cyber security strategies and significant investments in support of ASX's business strategy.
- Review and discuss technology and cyber security-related policies outside the matters carried out by the ASX Group Boards and Board Committees.
- Review major technology and cyber security risk exposures, including resources, incidents, information security and cyber security and the steps taken to monitor and control such exposures.
- Monitor industry trends that may affect the technology and cyber security strategies.
- Oversee processes in place to ensure ASX licensees can meet their relevant licence obligations.
- May recommend matters for referral to the CEO or relevant ASX Group Boards or Board Committees.

Specific to CHESS, the TMC receives a dedicated report on the support and maintenance of CHESS.

The TMC reports to the ASX Group Boards and Technology Committee as appropriate on matters relevant to those bodies. It will also review ASX's risk management and risk assessment guidelines and policies regarding technology and cyber security risks with the CRO.

### 3.3.2 Risk Committee

The Risk Committee is a senior management committee chaired by the CRO and has been established to ensure the adequacy and appropriateness of the risk management frameworks, policies, processes, and activities of the ASX Group. The CRO exercises delegated authority from the CEO to manage the framework associated with risk management of the ASX Group and is the sole decision maker on the Committee.

The key responsibilities of the Risk Committee are to:

---

<sup>2</sup> ASX has also established a Continuous Disclosure Committee to consider decisions regarding the disclosure of information in accordance with ASX's obligations as a listed public company.

- Oversee the implementation and adequacy of the ASX ERM Policy, ERM framework and risk processes, to seek to ensure risks are being managed within Board approved risk appetite.
- Monitor the effectiveness of ASX's internal control system.
- Review and approve key risk management policies, standards, and procedures. This includes clearing risk policies and procedures.
- Review key findings from internal audit reviews and ensure key risk issues are addressed on a timely basis.
- Seek to ensure that there is an adequate flow of information to the ARC and CS Boards to allow them to fulfil their remits with respect to risk management.

The Risk Committee reports to the CS Boards and ARC as appropriate on matters relevant to those bodies.

### 3.3.3 Regulatory Committee

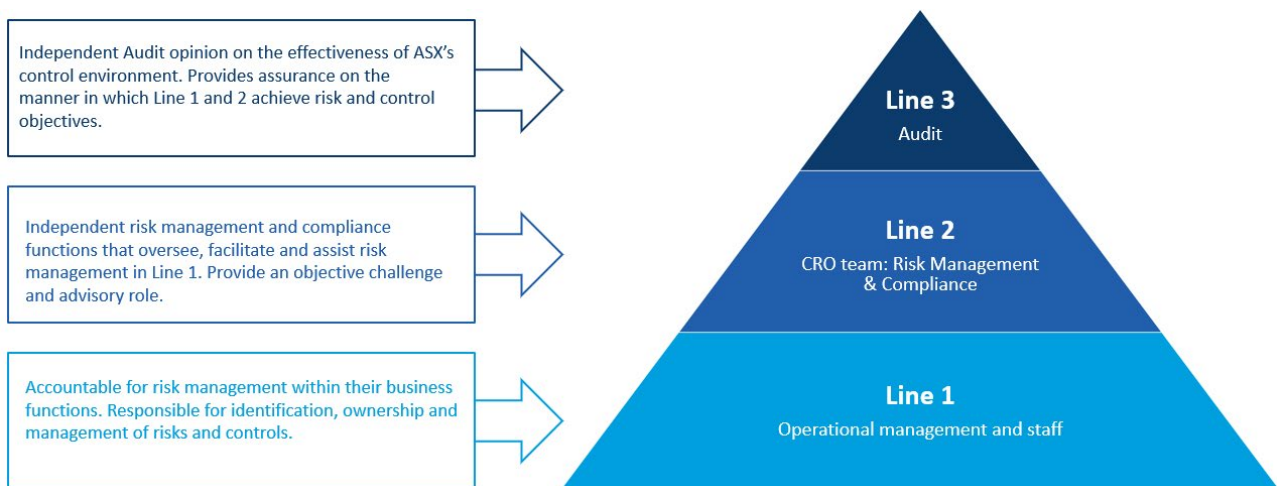
The Regulatory Committee is a senior management committee chaired by the Group General Counsel. The Regulatory Committee exercises delegated authority from the CEO to oversee policy development in relation to the operation and conduct of ASX's licensed activities, with the exception of clearing risk and settlement risk policy which is the responsibility of the Risk Committee. Decisions of the Committee are made by consensus, as determined by the Chair.

Amongst other things, the Committee receives reports from management on compliance monitoring and reporting arrangements with respect to the fair and effective licence obligations of the CS facility licensees. The Committee also determines when a matter should be referred to an ASX Board or Board Committee.

The Chair of the Regulatory Committee reports to the ASX Group Boards and Board Committees as appropriate on matters relevant to those bodies.

### 3.4 Three Lines of Defence

ASX's risk management strategy is founded on the Three Lines of Defence model, which provides a clear organisational structure and clarifies roles and responsibilities for managing risks and controls across the business. The Three Lines of Defence have been defined as follows:



**Figure 3.4.A Graphical Representation of the Three Lines of Defence within the ASX organisational structure**

- Line 1 is risk management within the business divisions. The identification, assessment, monitoring, reporting and escalation of risks begins in Line 1. For CHES, the relevant business divisions are S&P Technology, Customer, and Technology and Data.
- 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 the first line.

- Line 3 is the independent assurance function (i.e., Internal Audit).

The identification and assessment of risks relating to the resilience, reliability, integrity, and security of CHES are addressed as part of this overarching *ASX Risk Management Framework*. More details on risk management and the risk reporting structure are outlined in the detailed Operations and Governance sections of this report.



#### 4. Structure of ASX Response

ASIC has required ASX to prepare a Special Report detailing how ASX will ensure that CHES is adequately supported and maintained until the go-live of the CHES Replacement System. The scope of the report has been presented as a series of specified matters, which have been grouped thematically across four streams.

Operation	Security	Continuity	Governance
<p>2) a. With respect to the ongoing operation of CHES:</p> <ul style="list-style-type: none"> <li>i. Identify and assess, any risks to the resilience, reliability, integrity and security of CHES</li> <li>ii. Detail how the Licensee will manage and monitor any risks to the resilience, reliability, integrity and security of CHES</li> <li>iii. Detail how the Licensee will ensure CHES has the appropriate functionality, scalable capacity and performance - including to accommodate current and future reasonably expected growth in trading volumes growth in trading volumes</li> <li>iv. Identify any necessary upgrades to CHES required to avoid obsolescence of the end-to-end technology</li> <li>v. Detail how the Licensee will manage the safe and secure implementation of material changes to CHES, including testing such changes and ensuring that parties that may be impacted are adequately consulted and communicated with, and prepared for the changes</li> <li>vi. Detail the Licensee's management program (including monitoring and performance management) for any outsourced services essential to the operation of CHES and availability of its services, including all risks to resilience, reliability, integrity and security</li> <li>vii. Identify internal and external support requirements, in terms of resourcing and extendable/upgradeable vendor contracts</li> </ul>	<p>2) b. With respect to the security of CHES</p> <ul style="list-style-type: none"> <li>i. Detail how the Licensee will ensure the confidentiality, integrity and availability of information obtained, held or used by the Licensee in relation to CHES, including maintaining availability of and authorised access to data</li> <li>ii. Detail how the Licensee will implement a system of security controls, monitoring and periodic testing of controls to ensure CHES is resilient to unauthorised access or disruptions due to cyber events</li> </ul>	<p>2) c. With respect to the continuity of CHES detail how the Licensee will:</p> <ul style="list-style-type: none"> <li>i. Establish, implement, test and maintain continuity plans that include response and recovery processes for any event that would or would be likely to cause significant disruption to CHES, including (but not limited to) server or network infrastructure failures, software failures, cyber incidents, and business process failures</li> <li>ii. Ensure that disruption scenarios are periodically tested, continuity plans are continually improved, and resources (including any external parties) that are required to engage with such plans are trained and familiar with their roles and responsibilities.</li> <li>iii. Implement regular backup and recovery (from back up) procedures to ensure access can be re-established following a disruption event resulting in loss or corruption of data</li> </ul>	<p>2) d. With respect to the Licensee's governance arrangements, detail:</p> <ul style="list-style-type: none"> <li>i. What governance arrangements (including Board level oversight and management structures) the Licensee has in place to ensure ongoing monitoring and management of any risks to the performance and operation of CHES and availability of its services, and the adequacy of financial, technological and human resources (including any external parties and outsourced services)</li> <li>ii. How the Licensee will ensure it has the requisite skills and capabilities (including, where necessary, external parties) for the operational maintenance and support arrangements for CHES and for continued performance and operation of CHES and availability of its services until the Go-Live date of the CHES Replacement System</li> <li>iii. What system of controls and monitoring the Licensee has in place to measure, assess and continuously improve and assure the ongoing resilience, reliability, integrity and security of CHES.</li> </ul>
<p>2) e. With respect to governance, management, delivery and operational practices noted above, what principles, policies and frameworks (including international standards where appropriate) are to be applied to guide a comprehensive, consistent and transparent approach across these areas.</p>			
<p>3) For the avoidance of doubt and where appropriate, the special Report must detail implementation plans and specify the date by which the arrangements detailed in accordance with 2(2) will be in place.</p>			

Figure 4.A ASIC Requirements

ASX's responses to the ASIC Requirements have been similarly grouped into the four themes of Operation, Security, Continuity and Governance, recognising that consideration of Risk and Principles, Policies and Frameworks are applicable across the themes. Each ASIC requirement is broken down into component(s) and assigned a unique identifier (**Report Reference**).

Table 4.A ASIC Requirements Mapped to the Report Section

ASIC Letter	ASIC Requirement	Report Section	Report Reference
Operation a. (i)	Identify and assess, any risks to the resilience, reliability, integrity and security of CHES;	Risk Identification and Assessment / Management and Monitoring	5.1
Operation a. (ii)	Detail how the Licensee will manage and monitor any risks to the resilience, reliability, integrity and security of CHES;	Risk Identification and Assessment / Management and Monitoring	5.1
Operation a. (iii)	Detail how the Licensee will ensure CHES has the appropriate functionality, scalable capacity and performance – including to accommodate current and	Product Management Scalability, Availability and Performance	5.2 5.3

ASIC Letter	ASIC Requirement	Report Section	Report Reference
	future reasonably expected growth in trading volumes;		
Operation a. (iv)	Identify any necessary upgrades to CHESSE required to avoid obsolescence of the end-to-end technology;	IT Asset Management	5.4
Operation a. (v)	Detail how the Licensee will manage the safe and secure implementation of material changes to CHESSE, including testing such changes and ensuring that parties that may be impacted are adequately consulted and communicated with, and prepared for the changes;	Testing and Change	5.5
Operation a. (vi)	Detail the Licensee's management program (including monitoring and performance management) for any outsourced services essential to the operation of CHESSE and availability of its services, including all risks to resilience, reliability, integrity and security;	Governance – Operating Model – Resources and Vendor Support	8.2
Operation a. (vii)	Identify internal and external support requirements, in terms of resourcing and extendable/upgradeable vendor contracts;	Governance – Operating Model – Resources and Vendor Support	8.2
Security b. (i)	Detail how the Licensee will ensure the confidentiality, integrity and availability of information obtained, held or used by the Licensee in relation to CHESSE, including maintaining availability of and authorised access to data;	Security	6.1 6.2 6.3 6.4 6.5 6.6
Security b. (ii)	Detail how the Licensee will implement a system of security controls, monitoring and periodic testing of controls to ensure CHESSE is resilient to unauthorised access or disruptions due to cyber events;	Security	6.1 6.2 6.3 6.4 6.5 6.6
Continuity c. (i)	Establish, implement, test and maintain continuity plans that include response and recovery processes for any event that would or would be likely to cause significant disruption to CHESSE, including (but not limited to) server or network infrastructure failures, software failures,	Business Continuity	7.1

ASIC Letter	ASIC Requirement	Report Section	Report Reference
	cyber incidents, and business process failures;		
Continuity c. (ii)	Ensure that disruption scenarios are periodically tested, continuity plans are continually improved, and resources (including external parties) that are required to engage with such plans are trained and familiar with its roles and responsibilities;	IT Disaster Recovery (DR) and Service Continuity	7.2
Continuity c. (iii)	Implement regular backup and recovery (from backup) procedures to ensure access can be re-established following a disruption event resulting in loss or corruption of data;	Monitoring of Backups and Incidents Restoration of Backups	7.3 7.4
Governance d. (i)	What governance arrangements (including Board level oversight and management structures) the Licensee has in place to ensure ongoing monitoring and management of any risks to the performance and operation of CHES and availability of its services, and the adequacy of financial, technological and human resources (including any external parties and outsourced services);	Governance Structure and Supporting Processes	8.1
Governance d. (ii)	How the Licensee will ensure it has the requisite skills and capabilities (including, where necessary, external parties) for the operational maintenance and support arrangements for CHES and for continued performance and operation of CHES and availability of its services until the Go-Live date of the CHES Replacement System;	Operating model – Resources and Vendor Support	8.2
Governance d. (iii)	What system of controls and monitoring the Licensee has in place to measure, assess and continuously improve and assure the ongoing resilience, reliability, integrity and security of CHES.	Controls Monitoring	8.3
e.	With respect to the above, identify what principles, policies and frameworks (including by reference to international standards where appropriate) are to be applied to guide a comprehensive	Where relevant, the ASX specific policies, frameworks and principles have been called out within the responses above. These have been noted in <i>italics</i> for ease of reference. As applicable, references to any international	

ASIC Letter	ASIC Requirement	Report Section	Report Reference
	consistent and transparent approach across these areas.	standards and/or frameworks have also been noted.	
(3)	For the avoidance of doubt and where appropriate, the Special Report must detail implementation plans and specify the date by which the arrangements detailed in accordance with 2(2) will be in place.	Refer to <i>Section 9 Detailed Roadmap</i> .	

## 5 Operation

The section below details the specific ASX responses to the ASIC requirements regarding ongoing Operation of CHES.

### 5.1 Risk Identification and Assessment / Management and Monitoring

ASIC Requirement	Operation a. (i) and Operation a. (ii)	Objective	Identify and assess, any risks to the resilience, reliability, integrity and security of CHES Detail how the Licensee will manage and monitor any risks to the resilience, reliability, integrity and security of CHES
------------------	--	-----------	---

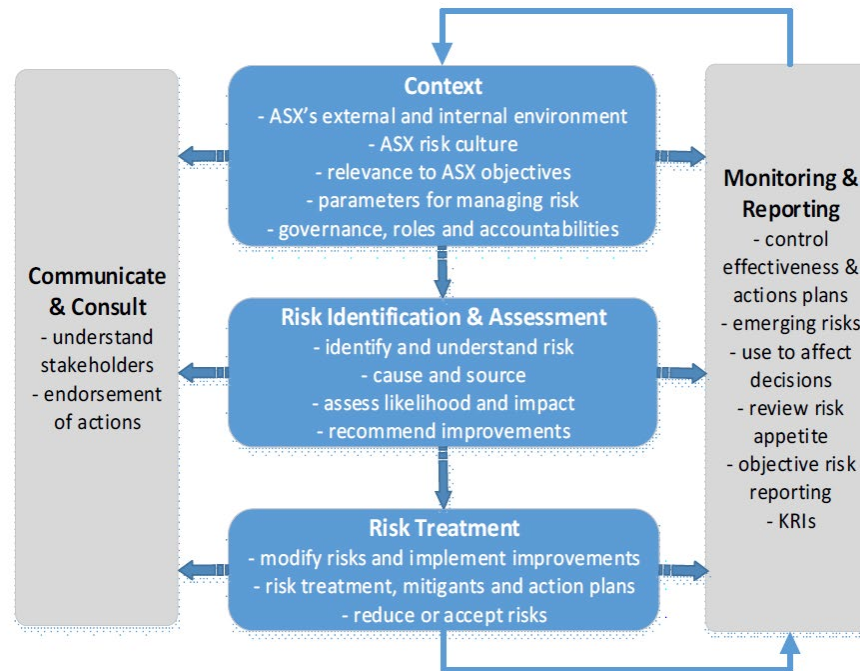
#### 5.1.1 ASX’s Risk Appetite Statement

ASX’s Risk Appetite Statement (**RAS**) is a central component of ASX’s risk management framework and describes the risk types encountered in ASX’s business, along with tolerance thresholds. Tolerance levels are expressed through KRIs that are cascaded throughout ASX to assist staff in its day-to-day management of risk. This helps ensure the whole organisation operates within agreed risk tolerance boundaries.

#### 5.1.2 ASX’s Enterprise Risk Management Framework

The *ERM Framework* has been developed with reference to leading practice global risk management standards, in particular ISO 31000:2018. It describes a number of key elements that help enable ASX to manage its key risks and supports assurance that the Group’s risk management and internal control environment is designed appropriately and operating effectively.

The core elements of the ASX *ERM Framework* are complemented by specific risk management processes and practices including establishing the context, identification and assessment, treatment, monitoring, reporting and communicating risk. This section focuses on risk identification, assessment, monitoring and reporting as it relates to CHES.



**Figure 4.1.2.A Key Elements of the ASX Enterprise Risk Framework (Reference: ASX ERM Framework)**

### 5.1.3 Risk Identification and Assessment

Risks faced by ASX are considered under seven key risk categories with the objective of providing a common risk lexicon to support business risk identification and assessment and facilitate organisation-wide monitoring, reporting and analysis of risks. The seven risk categories are Strategic, Operational, Technology, Counterparty, Financial, Regulatory and Legal, and Reputation.

Business division management (Line 1 in the Three Lines of Defence model) identifies risks in relation to business-as-usual and project-based activities, including raising management awareness, facilitating Risk Working Groups (RWGs), undertaking Project Risk assessment sessions with project stakeholders,

reviewing and analysing incidents (internal and external) along with utilisation and close monitoring of sensible risk metrics, i.e., audit actions, control improvement action plans, KRIs, incidents, problems, project risks, complaints etc. to enable proactive risk management.

Risks are broadly classified into “Delivery Risks” and “Delivered Risks”:

- Delivery Risks relate to those risks that threaten the execution/delivery objectives of a project or change initiative to be addressed within the project.
- Delivered Risks include risks introduced by the delivery of a project to a business function or service. ASX identifies and assesses CHES risks in line with the ERM Framework.

Line 1 together with Line 2 risk teams, ensure that delivered risks are actively being managed by the relevant business and technology teams. There are a number of ways the business can identify and assess delivered risks at ASX. The key methods are noted below.

#### **5.1.3.1 Risks Identified and Assessed as Part of Business as Usual (BAU) Activities**

Line 1 business teams are expected to identify risks arising from daily business activities, as well as risks pertaining to building, changing, or developing the business on an ongoing basis. The S&P business division staff and management team records and assesses risks within the ERM System. Oversight and review of these risks is performed by both by S&P Line 1 management staff and risk champions and by Line 2 Risk.

#### **5.1.3.2 Annual Risk Self-Assessments (RSA)**

At a minimum, business unit risk profiles are self-assessed annually as part of a formal Risk Self-Assessment (**RSA**) program. The review of risks and controls pertaining to CHES is encompassed as part of this annual RSA program. S&P has six business unit risk profiles which encompass risks and controls relevant to the CHES operating environment. Line 2 reviews the completeness and efficacy of these risk profiles as part of the annual RSA program, as well as active participation in the quarterly S&P and Technology & Data RWG.

#### **5.1.3.3 Project Related Delivery Risks**

The project related delivery risks are captured in the Enterprise Issue and Project tracking tool based on the project risk management framework and include the Risks, Assumptions, Issues and Dependencies register.

#### **5.1.3.4 Project Related Delivered Risks**

Any relevant delivered risks are also identified, managed, and captured by project teams in the Enterprise Issue and Project Tracking tool and transferred (once formally accepted by the Risk Owner) to the ERM system. The ERM system is the core repository for all risks, issues, controls, and action plans across ASX, including risks and controls specifically related to the integrity, resilience, reliability, and security of CHES.

### 5.1.3.5 System Operations Risk Assessment

System operations risk assessments are performed biannually (twice a year) for a subset of systems that have been identified as critical to ASX's operations, including CHES. These risk assessments are performed against the following 8 categories:

- Availability.
- Capacity.
- Disaster Recovery.
- Incidents and Problems.
- IT Security.
- System Age.
- System External Support.
- System Internal Support.

System Owners are responsible for recording any findings that arise from these assessments as issues in the ERM system. These issues will be linked to an associated risk either where one already exists or if a new risk is identified, this will be added to the existing risk repository in the ERM System.

### 5.1.3.6 Security Risk Assessments

The Security Team performs regular risk assessments of the ASX environment, including the CHES environment. A security risk assessment may be triggered by the annual strategy process, a major project or upgrade implementation, the identification of an emerging risk or issue, or a request from the business. These risks are discussed at the appropriate various business forums and escalated as required.

### 5.1.3.7 Problem Management Risks

Problems are identified, assessed, investigated, solutions proposed and agreed upon and then implemented within the ITSM platform.

When it is determined that a Problem Investigation should no longer be investigated further, the Problem Lead can propose that the risk be accepted for the Service Owner to evaluate. When accepted, the problem is moved to a state of "Closed" with "Risk Accepted" as the closure code, and, if applicable, an entry is made into the ERM system, referring to the problem record.

## 5.1.4 CHES Risks

Risks associated with CHES are identified through the mechanisms listed above and assessed as part of multiple risk profiles within the S&P business. In addition to the existing risk profiles, ASX intends to maintain a CHES specific risk view for central visibility and ease of management.



There are 31 CHES risk that have been identified and assessed as part of the above processes, which map to 26 ASX risk themes per ASX’s enterprise risk library. Those that relate to resilience, reliability, integrity and security are listed below (21). These risks (and the associated descriptions) have been extracted directly from ASX’s ERM system. The risk descriptions have been developed as a plain-language summary of risk exposures (and associated obligations) for use by Line 1 staff in risk monitoring and reporting in relevant business units.

**Table 5.1.4.A CHES Risks Mapped to the four ASIC Scope Areas**

ASIC Risk Category	ASX Risk Theme *	CHES Risk
<p><b>Resilience</b> The ability to avoid/recover from incidents or events</p>	<p>Outage or unavailability of critical systems or services due to a natural disaster or another unexpected event</p>	<p>[Redacted]</p>
<p><b>Reliability</b> The ability of the system to function and perform consistently</p>	<p>Outage or unavailability of critical systems or services due to a software or hardware defect</p>	<p>[Redacted]</p>
	<p>Critical tasks are not completed promptly or not completed at all due to skill or resource unavailability</p>	<p>[Redacted]</p>

---

Market Outage and/or Business disruption due to system malfunction/failure

Non-compliance with contractual obligations with third parties - Technology

Non-compliance with regulatory obligations or relief

		[Redacted]
	Inflexible and inefficient technology environment	[Redacted]
	Ineffective or inefficient process design or manual execution	[Redacted]
<b>Integrity</b> System integrity – the ability of the system to function as intended, free from unauthorised manipulation of the system.	Outage or unavailability of critical systems or services due to an internal procedural error	[Redacted]
The validity and accuracy of data	Ineffective system functionality and utility (including performance and capacity)	[Redacted]
	Inefficient, untimely, and ineffective delivery of technology changes	[Redacted]
		[Redacted]



Internal fraud by management or staff (including contractors)	[Redacted]
Inadequate cyber resilience framework	[Redacted]
System or data compromised by unauthorised or malicious activity	[Redacted]

\*Predefined risk themes per the ERM system library

The full list of CHES related risks is provided in *Appendix B – CHES Risks*. Those not related to the four ASIC areas include risks related to strategy, product pricing, regulatory reporting, compliance with ASX frameworks, market position and brand and these have been classified as “Other” in *Appendix B*.

Risks are evaluated and assessed against a 5x5 risk scalar matrix to provide a consistent view of the likelihood and impact of identified risks including those related to the integrity, resilience, reliability, and security of CHES.

The risk assessment matrix is utilised to (i) assess risks consistently, and (ii) help express ASX’s risk tolerance in defining high, medium, and low levels of risk:

- Risk is assessed as a product of Impact x Likelihood, on both a qualitative and quantitative 1 to 5 scale.

- Inherent (pre-controls) and Residual (after considering control effectiveness) risk is assessed using the same scalars.

### 5.1.5 Risk Monitoring

Monitoring, management, and escalation of risk within and across the ASX begins in Line 1, by staff and management and through daily operations as well as appropriate forums, including RWGs. Oversight of the risk and control environment occurs in both Line 1 and 2, with escalation and reporting to the relevant management oversight committees, and ultimately to the appropriate Board.

ASX’s RAS is a central component of ASX’s risk management framework, and describes the risk types encountered in ASX’s business, along with tolerance thresholds. Tolerance levels are approved by the Board and expressed through KRIs that are cascaded throughout ASX to assist staff in its day-to-day management of risk.

ASX’s RAS is operationalised firstly from the bottom-up through each business division’s annual self-assessment of risk profiles as well as regular reporting on its organisational KRIs. Secondly, risks are monitored from a top-down perspective via quarterly reporting on 30 Board KRI results across seven key risk categories. Thirdly this information is supplemented using material and knowledge relevant to emerging risks, project delivery, people and culture, audit reports, compliance breaches, strategic initiatives, incidents, regulatory deliverables, and regulatory engagement. These elements culminate in the provision of an objective opinion on whether the company is operating inside or outside risk appetite, conveyed via the quarterly Chief Risk Officer (CRO) Enterprise Risk report to the ARC.

CHES specific risks are considered within the monitoring groups and forums listed in the following table. The below listed forums are part of the broader ASX Governance Forums and consider the Resilience, Reliability, Integrity, and Security risks relating to CHES (for further details, refer to *Section 8.1 Governance Structure and Supporting Processes*). The Security Operations Centre (SOC) listed below only monitors alerts on security related issues.

**Table 5.1.5.A Monitoring Forum Groups for CHES Specific Risks**

#	Monitoring forum	Short description of what it monitors	Frequency
1	S&P Technology and Operations	Oversees for daily CHES operations related risks and issues	Daily
2	SOC	Monitors for security alerts for system performance, incident management, vulnerability scanning and threat intelligence.	Daily
3	S&P Leadership Team	Oversees business divisional escalation of risks and issues	Fortnightly

4	S&P RWG	Oversees the sound operation of risk (and compliance) management in a line of business	Quarterly
5	S&P Project Working Group	Review and Endorse all S&P funding requests and updates to PGG	Monthly
6	Portfolio Governance Group	Oversees the status of various projects, including the risks that are threatening delivery of portfolio objectives. This includes the CHES Roadmap.	Monthly
7	Risk Committee	Oversees implementation and adequacy of the risk management frameworks, policies and processes to ensure risks are being managed within Board approved risk appetite.	Quarterly
8	Technology Management Committee	Oversees IT security and systems and incident management.	Quarterly
9	Board Audit and Risk Committee	Assists the ASX Board to review and oversee systems of risk management, internal control, and compliance within the ASX Group. Assists the CS Boards to oversee risk matters that are ASX Group enterprise-wide in nature.	Quarterly
10	Board Technology Committee	Assists the ASX Group Boards to oversee technology and data risks, including cyber security risks.	Quarterly
11	CS Boards	Broad responsibilities for oversight of the CS facilities, including setting operational risk tolerances for the CS facilities, and overseeing management of the CS facilities within these operational risk tolerance and ASX risk appetite, reviewing and approving the risk management framework, and overseeing adequacy of internal controls, systems and processes for clearing and settlement risk of the CS facilities.	Monthly
12	ASX Limited Board	Oversees ASX's overall risk management framework and its operation by management, and the processes for identifying significant risks facing the ASX Group. Oversees systems of risk management, internal control and compliance within the ASX Group. Approves the ASX Risk Appetite Statement.	Monthly

### 5.1.6 Control Effectiveness and Action Plans

In order to effectively manage risks, ASX ensures that all inherently High and Medium risks have at least one key control in place. Control effectiveness is self-assessed by control owners as part of the annual RSA review. Note key controls testing is scheduled to commence in FY24 to support the assurance of key control design and effectiveness as they relate to both CHES and broader enterprise risks. In the absence of or a deficiency in a key control, an issue is recorded and ASX ensures that an action plan has been assigned or a risk issue acceptance has been sought and approved via the established risk issue acceptance process. Open risk issue acceptances in place for CHES are reviewed as part of the annual RSA review program, as well as part of ongoing management and monitoring of risks and issues by Line 1 business owners in their BAU activities'.



Current and Planned Initiatives	Status of Initiatives	Theme	Indicative Date
No additional initiatives identified (Related initiatives are in other sections).			



## 5.2 Product Management

ASIC Requirement	Operation a. (iii)	Objective	Detail how the Licensee will ensure CHES has the appropriate functionality, scalable capacity and performance - including to accommodate current and future reasonably expected growth in trading volumes
------------------	--------------------	-----------	---

To ensure CHES has the appropriate functionality to meet market needs, ASX adopts a delivery process that includes stakeholder engagement, divisional and enterprise prioritisation, and delivery via the *ASX Delivery Framework*. The framework sets out the governance arrangements, assurance, ownership, mandatory artefacts and deliverables, roles and responsibilities, and Responsible, Accountable, Consulted, and Informed (**RACI**) that all change initiatives (projects) follow at ASX.

The Product Management framework is summarised through three pillars within the Product Management process:

- Stakeholder Engagement.
- Product Prioritisation and Roadmap.
- Product Development.

### 5.2.1 Stakeholder Engagement

The way ASX engages with stakeholders in relation to CS services and any proposed or required changes in those services or CHES functionality considers the subject matter related to the change, the stakeholders affected and the scale of any proposed change or impact. The engagement channels to support stakeholder engagement include:

- Formal consultation, including the publication of a consultation paper, response to consultation feedback and the publication of non-confidential submissions from stakeholders. ASX would typically use this mode of engagement for changes to CS services or CHES functionality with a material impact on a wide range of users of CS services.
- Meetings of the ASX Business Committee, which comprises representatives from the CS stakeholder groups, including Participants, Share Registries and AMOs. A number of industry associations for relevant stakeholder groups are also represented on the ASX Business Committee (Australian Financial Markets Association, Australian Custodial Services Association, Australian Shareholders’ Association, Australasian Investor Relations Association, Governance Institute of Australia and Stockbrokers and Investment Advisers Association). The Business Committee is ASX’s formal

channel for regularly scheduled engagement with stakeholders on matters related to CS services and CHES system functionality. More information on the Business Committee is provided below.

- Industry forums and associations, including Issuer and shareholder associations. This form of engagement may occur through ASX's participation in conferences convened by industry associations (for example, ASX staff as presenter, panellist or attendee) or participation in meetings or discussion groups convened by industry associations (for example, ASX as a member of the industry association or an invitee).
- Bilateral discussions with customers as part of ASX's customer relationship management activities. These discussions may be initiated by ASX or by the customer.

One of the core elements of ASX's *Cash Equities Clearing and Settlement Code of Practice (the Code)* is ASX's commitment to meaningful engagement with customers and other stakeholders about the ongoing development of cash equity CS infrastructure. In the Code, ASX explicitly recognises the importance of engagement in the design and functionality of the infrastructure to ensure it continues to meet the needs of users and the market.

In ASX's Cash Market CS business, the ASX Business Committee is ASX's formal channel for regular engagement with stakeholders on matters related to CS services and CHES, including system functionality. The Business Committee is convened to assist ASX in fulfilling its commitment with respect to meeting the needs of users and the market. The Business Committee can make recommendations to the ASX CS Board on the ongoing operation and development of cash equities CS infrastructure and services. Those Boards must consider those recommendations and provide formal responses to the Business Committee. The Code also requires ASX to consult with the Business Committee on its investment decisions in relation to the design, operation and development of new cash equities CS infrastructure and services. The Business Committee meets quarterly and is governed by the Business Committee Charter.

ASX also has formalised procedures (*Access Procedures for AMOs*) in place for AMOs to request an enhancement or expansion of the Trade Acceptance Service (**TAS**).

ASX engages with ASIC and RBA on CHES and its functionality regularly, for example through regularly scheduled staff-level meetings and periodic supervisory assessments conducted by the regulators. ASX is expected by RBA to achieve a number of specific outcomes with respect to the functionality of the current system in the short term. Those specific outcomes include, among other things, an explanation of the CS facility licensees' plans for implementation of system features that are required for compliance with the FSS and that were planned as part of the CHES Replacement, assessments of the feasibility of implementing intraday margining and a segregated house/client account structure for cash market positions in the current system, and enhancements to ASX's periodic reporting of cash market CS data to the RBA.

### 5.2.2 Prioritisation and Product Roadmap

Any proposals to introduce new functionality in CHES or to modify existing functionality (whether originated through stakeholder engagement or by ASX internally) are raised via a formal process and must be approved by the Group Executive, S&P via the bi-weekly meeting of the S&P Leadership Team. Any

material changes to CHES functionality that cannot be funded and resourced from within the S&P business will be escalated for enterprise prioritisation, funding, and resource allocation.

Prioritisation of change initiatives is assigned initially by the S&P team based on a prioritisation framework that considers the type of change, the urgency of the change and its impact. Any proposal to introduce new functionality in CHES, or to modify existing functionality, would be classified in the appropriate 'type of change' category. These categories include (in descending order of priority) 'Licence to Operate', Regulatory, Process Improvement, and New Product Development. More information on these categories is contained in the *Backlog Prioritisation Framework*. Prioritisation is further informed by both "Urgency" and "Impact"; change initiatives with high impact and urgency will be prioritised over items with low impact or urgency.

Once prioritised by S&P (or where re-prioritisation is required of an already approved initiative), a change initiative is raised to the ASX Governance forums for further organisational prioritisation and approval, including the release of funding and resource allocation. The ASX Governance forums, including the SGG, Portfolio Working Group (**PWG**) and PGG each have responsibilities with regard to prioritisation, including (but not limited to):

- Approve the commencement of new projects by authorising funds and resources (PGG).
- Provide a governance mechanism for the commitment of resources, clarification of necessary resource capacity, to commence new projects, and endorse any recommended change to or re-prioritisation of initiatives as required (PWG).
- Help balance priorities (e.g., help prioritising work, resourcing, scope and objectives, resourcing, budget, customers) (SGG).

(For further details on governance forums, refer to *Section 8.1 Governance Structure and Supporting Processes*)

All approved changes form part of the Product Roadmap, which contains all change initiatives, their respective priority and planned delivery dates. These initiatives are communicated to stakeholders via the below mechanisms (where appropriate):

- Annual Cash Equity CS Services Developments Report, including delivered initiatives and future planned enhancements.
- Technology Upgrade Release Notices (**TURNS**), published via ASX Online.
- The Business Committee.

### 5.2.3 Product Development

Based on the inputs from stakeholder engagement, and the proper prioritisation and planning of the product roadmap for CHES, development of changes to CHES follow the *ASX Delivery Framework* (for changes delivered via a project) supported by the Software Change Request (**SCR**) process. (For further details, refer to *Section 5.5 Testing and Change*)



The current functional and non-functional solution baseline against which changes are raised are expressed in the *ASX Procedure Guidelines (APG)*, External Interface Specifications (**EIS**) and other sources including architecture requirements and designs. ASX will, over time, formally express these into functional and non-functional requirements for CHES, including a traceability matrix for major ongoing and future changes.

Current and Planned Initiatives	Status of Initiatives	Theme	Indicative Date
No additional initiatives identified (Related initiatives are in other sections).			

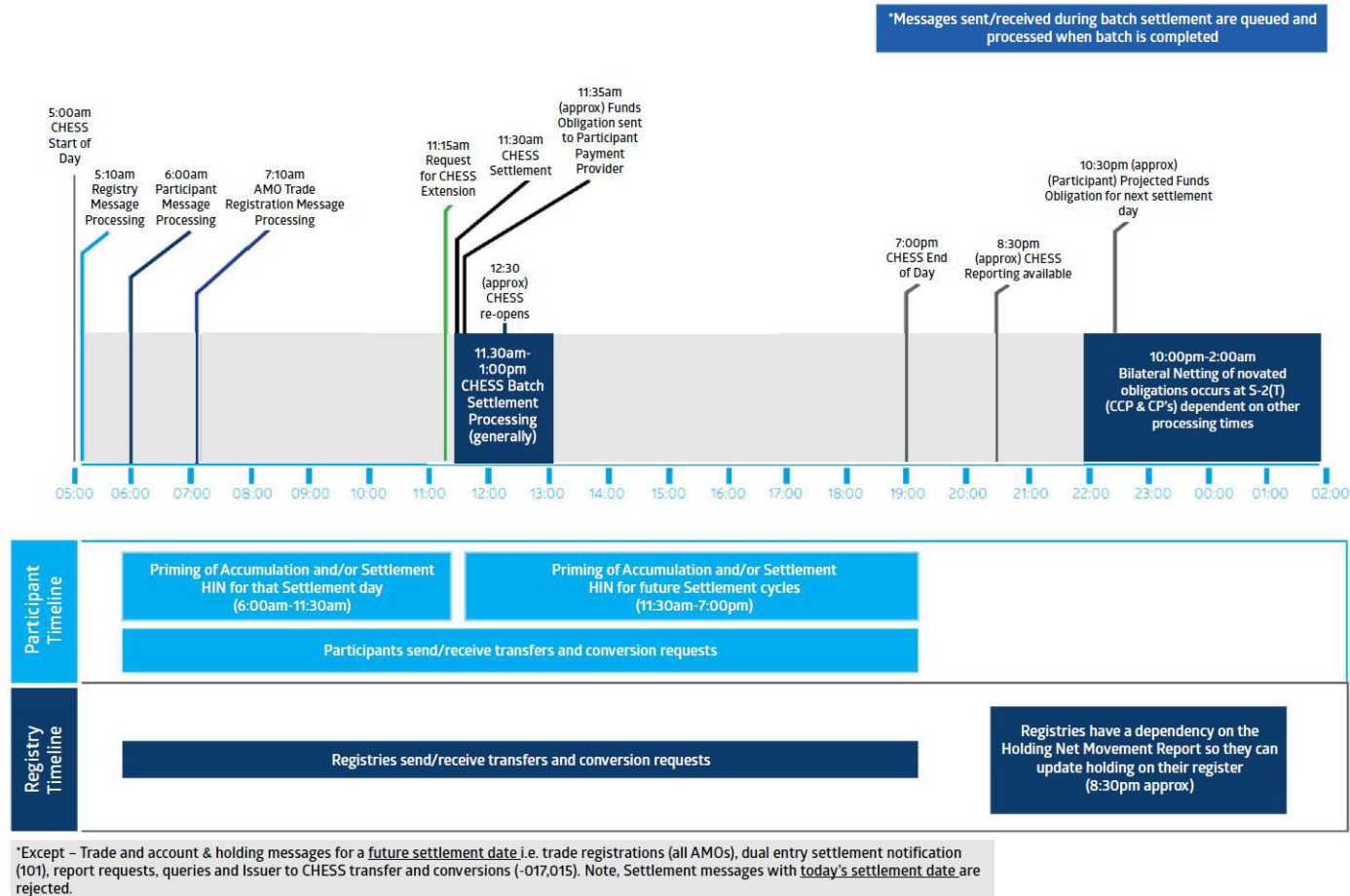
### 5.3 Scalability, Availability and Performance

---

ASIC Requirement	Operation a. (iii)	Objective	Detail how the Licensee will ensure CHES has the appropriate functionality, scalable capacity and performance - including to accommodate current and future reasonably expected growth in trading volumes
------------------	--------------------	-----------	---

---

ASX aligns with the *COBIT 5* process framework for service delivery, including the approach to “Build, Acquire & Implement” services and the “Manage Availability and Capacity” processes. A typical day in the CHES processing cycle is shown below.



**Figure 5.3.A CHES Processing Cycle**

ASX manages the availability and capacity of CHES to achieve agreed and expected availability, performance, and capacity requirements to meet current and future business needs. Maintaining service availability, efficient management of resources, and optimisation of system performance through prediction of future performance and capacity requirements in a timely manner ensures the service meets future needs.

The critical performance metric that is used to monitor and manage CHES capacity is “Trades per day”.

Availability and capacity management can be categorised into the following streams:

- **Availability Management** – Ensures that CHES Technology services meet the current availability needs of the business in a timely manner (Service Level Objectives).
- **Business Capacity Management** – Focuses on future changes to service requirements by informing ASX on market demand and forecast of trade volumes that are inputs to the CHES Service.
- **Service Capacity Management** – Focuses on monitoring live CHES Services and gathering information data to identify trends in order to prevent a performance or availability impact on the CHES service.
- **Component Capacity Management** – Focuses on the performance utilisation and capacity of individual technology components, e.g., hard disk storage, and hardware computing power.

### 5.3.1 Availability Management

ASX Availability Management for CHES is the process responsible for ensuring that Technology services meet the current availability requirements in a timely manner. Availability management defines, analyses, plans, measures, and improves all aspects of the availability of Technology services, and ensures that Technology infrastructure, processes, tools, and roles are appropriate for the agreed service level targets for availability.

Component availability is monitored through software and hardware monitoring tools. CHES utilises multi-site synchronous storage and multi-site redundant hardware to provide the resilience needed for the system to withstand incidents such as hardware failure and site loss within Service Level Objectives. (For further details on continuity and resilience, refer to *Section 7 Continuity*)

ASX use the Service Availability Reporting (**SAR**) process to record and report on CHES availability metrics and inform regulators such as ASIC and RBA on the availability of market facing services.

CHESS Service Level Agreements (**SLAs**) and availability are measured and recorded in the KPI report. This report provides the baseline and service level targets for availability and is presented to the ASX Board and used for internal management by the ARC. The data from KRI is used as input for the CHESS Technology Performance Summary Dashboard and to identify risks and required actions for managing risks.

### 5.3.2 Business Capacity Management

ASX has three performance metrics to monitor and report on the capacity and performance of CHESS:

- Trades per day (Cash Market) includes ASX, Cboe and NSX Trades minus Cboe Crossing Settlement Information Trades.
- Novated and Non-Novated Settlements.
- Netted Transactions per day.

The number of trades submitted to CHESS by AMOs for registration are the major driver of CHESS capacity requirements, given that trades make up most of the daytime transaction volumes. Trade volumes can be subject to spikes caused by market events. CHESS resources are consumed proportionally to the increases in trade volumes.

Trades reported by Cboe and NSX are received into CHESS via the CHESS Messaging interface. However, trades received from ASX Trade are received by CHESS via an internal middleware system called CORE. CHESS, therefore, has a direct dependency on CORE to receive and process the majority of market trades.

In 2018 and 2019, the daily CHESS peak trade volume ranged from 2.7 to 3.3 million respectively. In early 2020, global markets experienced increased trading volatility and volumes related to the COVID-19 pandemic. On 13 March 2020, CHESS had a record peak day volume of 7 million trades. This prompted ASX to make upgrades to the CHESS infrastructure and software components throughout 2020/2021 to immediately increase the headroom capacity.

Post upgrades, testing of the CHESS environment was conducted, and it was validated that CHESS was able to process 10 million per day. The test results, along with additional considerations, were presented to the relevant executives and associated governance bodies for approval and to set CHESS capacity limitation at 10 million trades per day.

The current rolling daily peak over the preceding 24 month period is 4.8 million trades, and the rolling daily peak volume over 3 month period is 2.3 million as of February 2023. The ASX S&P Technology Team uses an exponential forecast model to assist in capacity requirements planning by extrapolating from historical monthly peak trading volume data. Based on this exponential model<sup>3</sup>, daily trades are forecasted to reach 5 million by February 2025 and 10 million by April 2030.

---

<sup>3</sup> Modelling conducted at February 2023



ASX has the following plans in place for CHES in 2023:

- Develop application breakpoint test that would determine the practical capacity limitation for the CHES and identify the maximum number of daily trades that would result in the system failing to meet SLAs.
- Work with AMOs and regulators to develop potential options to manage incoming transactions during unplanned/outlier events.
- Identify solutions that would allow CHES to move to an alternate method for ASX Trade to submit trades.

In parallel, the following are plans in development that will support ongoing CHES capacity management:

- To ensure ASX forecasts future trading growth as reliably as possible, ASX is developing a revised model that would consider underlying drivers of volume increase based on historical experience of events such as market structure changes, major corporate action events, and unplanned/outlier events such as the COVID-19 pandemic.
- Improve the maturity level of the Availability and Capacity Management Framework for CHES.
- Investigate the technical feasibility to transition from a single instance of the application to multiple instances (multi-threading) of the application to process trades.
- Analyse opportunities to optimise the database to allow CHES to process more transactions per day.

### 5.3.3 Service Capacity Management (Monitoring of Performance and Capacity)

ASX actively monitors the outstanding CHES message volumes to identify if there is a backlog in the application or customer queues during a trading day. In the instance where the trade application queue backlog is becoming longer than standard operations, an investigation will take place that may trigger an incident process for escalation to address the backlog.

In the event of a high volume or high volatility trading day, the team will participate in live monitoring alongside Technology and Markets teams to monitor trading volumes and compare against prior record day throughput.

### 5.3.4 Component Capacity Management (Application, Infrastructure/System Monitoring)

ASX performs infrastructure and system monitoring to ensure CHES maintains the availability and performance to meet its licence obligations and service level requirements. The ASX teams across infrastructure, application support and database utilise a range of monitoring tools to provide 24/7 monitoring and support daily and overnight processes across hardware and technology components.

In the case of monitoring alerts that require escalation, the team receiving the alert will follow the enterprise incident management process.

### 5.3.5 Intra-day CHES Settlement Batch Process Management/Monitoring

ASX monitors the CHES Settlement Batch from commencement to completion. CHES Settlement Batch is scheduled to commence at 11.30 am each day and performs seven processes to achieve DvP (Delivery vs Payment) settlement of cash market novated and non-novated obligations. During this time, CHES suspends the processing of most settlement instruction messages and as such, it is important to monitor the activity to ensure completion in a timely manner so that CHES can resume normal processing. The team monitors prior to the commencement, during, and after the Settlement Batch is completed.

Key metrics for monitoring the progression and completion of the CHES Settlement Batch include the number of extension requests, request for ASX support during Batch and time to completion. Post batch reporting includes the percentage of scheduled settlement obligations that settle successfully during the batch (settlement efficiency) and the daily fail rate. Settlement obligations that fail are removed from batch settlement by CHES and re-scheduled for the following business day. ASX reviews the fail rate daily and may engage directly with the relevant Participants if the rate exceeds a threshold

Reporting of business activity processed during CHES Settlement Batch and settlement efficiency are prepared for the purpose of reporting to management. Key service performance metrics are also provided to the Business Committee and AMOs (for each AMOs own transactions).

### 5.3.6 End of Day Batch Process Management Monitoring

CHES performs overnight processing outside of business hours. This processing, which includes trade netting, cum entitlement (CUM) balance creation, reporting and other functions, is collectively known as the CHES End of Day (EOD) batch.

The EOD Batch must complete to meet the start of day service level hours for users of 6.00 am to 7.00 pm and 7.10 am to 7.00 pm for the users of the TAS, business days Monday to Friday.

### 5.3.7 Batch Incident Management

Incidents that occur during intra-day batch settlement or CHES EOD batch processing follow the standard enterprise *Incident Management Process* to remediate the issue. This includes the reporting of the incident to regulators where required by the process. When addressing known issues, the Application Support team follows the problem management process and leverages a repository of remediated actions for CHES.

Incidents may be resolved by S&P teams including CHES Equity Operations, CHES Application Support or Engineering. Resolution of incidents takes priority over defect fixes. All historical incidents along with the applicable workarounds and resolution methods are documented.

The initiatives below are identified to maintain the low risk appetite for matters relating to CHES.

Current and Planned Initiatives	Status of Initiatives	Theme	Indicative Date
Develop a new model for forecasting future trading growth	In Progress	Operations	Sep 2023
Improve maturity level of the Availability and Capacity Management Framework and processes based on COBIT	In Progress	Operations	Dec 2023
Stress test CHES to determine further points of failure	Planned	Operations	Dec 2023
Capacity and Performance Improvements	N/A	Operations	Mar 2025 (Phase 1)

## 5.4 IT Asset Management

ASIC Requirement	Operation a. (iv)	Objective	
			Identify any necessary upgrades to CHES required to avoid obsolescence of the end-to-end technology

ASX aligns its IT Asset Management processes with the *COBIT 5 framework* by planning, acquiring, deploying, maintaining, and disposing of aged assets to avoid unsupported technology obsolescence, reduce operational risks, and improve operational efficiency. The process involves tracking and monitoring IT assets relating to configuration management, asset end of life, and roadmap activities to maintain support for CHES.

### 5.4.1 Asset Registers

ASX utilises two enterprise asset register tools to log and monitor the end-to-end lifecycle management for software and infrastructure assets.

- ASX stores all CHES related contracts, including software licence contracts, in a centralised enterprise Contract Management capability within the ASX ITSM platform. The Contract Module stores contract metadata relevant to the management of the contract which provides contract search and reporting functionality and helps to automate certain functions such as notifying a contract owner when a contract is approaching renewal. Contracts in the ITSM platform are managed by the central Vendor Management team with support from the Contract Owner, and the Business and Finance teams. Software contracts that have licence entitlements in support of the CHES application are updated in the Software Asset module of the ITSM platform and tracked by the Contract Owner to ensure ASX complies with the licence entitlements. The *ASX Vendor Management Framework* and *Procurement Policy* document the roles and responsibilities of teams within the processes.
- Infrastructure assets are tracked in a separate asset register, which details the physical asset entitlements required to operate the CHES service including servers, routers, backup devices, storage networking and firewalls. This asset register is managed by the ASX Technology Infrastructure team and contains the infrastructure asset information relevant to maintaining the asset. A documented *Data Centre Equipment Commissioning and Decommissioning* process is in place to ensure infrastructure asset information is captured on an ongoing basis.

### 5.4.2 Technical Debt

ASX performs six-monthly System Operational Risk Assessments (**SORA**) to identify, amongst other criteria, the risks associated with legacy technology, including support, maintenance, and patching levels available for operating systems, infrastructure, and application components. Key issues and risks are captured in the ASX Enterprise RMS to enable management and visibility on the progress of the actions. ASX uses the *ASX Delivery Framework* to initiate

projects, plan and implement IT asset upgrades. The results of the CHES SORAs are reported to the S&P management team, the TMC, and the Technology Committee.

### 5.4.3 Upgrades

In September 2022, following announcements regarding delays to the CHES Replacement go-live, ASX made further assessments of the risks around the support and maintenance requirements of CHES. The assessment determined that CHES could be supported and maintained and would meet ASX's requirements through to 2025. Further, a number of initiatives were identified that would improve system capacity and external hardware support to meet ASX's requirements through to 2028. When ASIC provided ASX with its letter last December, it asked ASX to consider support and maintenance to 2032, referred to as the Extended Period. To take this into account, ASX identified additional enhancements to ensure CHES remains operationally reliable over the Extended Period.

Initiatives included in the above assessment related to Technology aged assets are reported across the organisation and actioned. The following reports are generated:

**Table 5.4.3.A Reports generated for Technology Aged Assets**

Report	Description	ASX Owner (report preparer)	Frequency
System Operational Risk Assessments	ASX enterprise risk assessment performed on selected systems and environments. Submitted to the ASX RWGs, TMC and Technology Committee, the report includes an assessment of aged assets support and maintenance for CHES	ASX Technology Security & Governance	Bi-Annually (Twice a year)
Infrastructure Quarterly Asset Report	CHES IT Asset lifecycle management on infrastructure aged assets and roadmap strategy to ensure support is maintained.	ASX Infrastructure	Quarterly
Performance Technology Dashboard	CHES technology performance dashboard containing aged asset risks presented back to ASX Executive Management.	ASX S&P Technology	Monthly

As noted above, a number of CHES components have been identified as needing attention due to the ageing of assets, including the operating system, hardware, network, monitoring, hardware security modules, shared storage array, and platform support. Additionally, ASX has identified a dependent system (CORE), as an aged asset. CORE provides the input of ASX Trade trades to CHES.

To avoid obsolescence, ASX is proactively monitoring and upgrading CHES related aged assets and seeking extended support from vendors. The CHES Roadmap has been developed, and key activities identified to be progressed through to December 2025 to uplift aged assets and ensure support of the components until CHES is safely replaced. The initiatives below are identified to maintain the low risk appetite for matters relating to CHES.

Current and Planned Initiatives	Status of Initiatives	Theme	Indicative Date
Establish a Managed Service Contract agreement [REDACTED]	In Progress	Operations	Jun 2023
Front end – OS and Hardware upgrade	In Progress	Operations	Jun 2023
CHES Access upgrade	In Progress	Operations	Sep 2023
[REDACTED]	Planned	Operations	Jun 2024
Address CORE dependencies:	Reference Data (Batch)	Operations	Jan 2024 (Phase 1)
	Reference Data (Real time)	Operations	Jun 2024 (Phase 2)
Monitoring application upgrades	Planned	Operations	Mar 2024
Backend upgrades [REDACTED]	Planned	Operations	Dec 2026
Backend upgrades [REDACTED]	Planned	Operations	July 2024
Assess alternative hardware architecture for backend servers to support CHES	Planned	Operations	Jun 2024
Customer VPN Access	In Progress	Operations	Jun 2023 (Phase 1)
HSM Device upgrade	In Progress	Operations	Nov 2023

## 5.5 Testing and Change

ASIC Requirement	Operation a. (v)	Objective	
			Detail how the Licensee will manage the safe and secure implementation of material changes to CHES, including testing such changes and ensuring that parties that may be impacted are adequately consulted and communicated with, and prepared for the changes

The CHES application is an in-house built application that follows the CHES specific SCR process, as detailed in the *CHES Application Development Change Management Release Process* document. This process is used to manage the source control, build and promotion of software between the various test environments through to production.

The management of change is governed by the overall *ASX Delivery Framework*, including the *Quality Engineering and Testing (QE&T) Capability Practice Framework* which is part of the overall *ASX Delivery Framework*.

Request for change related to CHES arising from the business, any identified Technology debt/Production software defects, operations, and other business divisions are raised using the ASX Enterprise Issue and Project Tracking tool and go through a prioritisation process. Depending on the nature of the CHES change, size and cost involved, the prioritisation process will decide whether the change will be implemented as a project, following the project *ASX Delivery framework* or as a BAU change following the CHES SCR process.

Once endorsed and prioritised, work planning and budgeting take place to manage and track delivery. (For further details on the governance structures, refer to *Section 8.1 Governance Structure and Supporting Processes*)

All Technology changes (including projects) must follow the *ASX ITSM Change Management Policy and Process Guide* when releasing IT changes into the environments under change control (e.g., external client environments, the production copy environment, and the production environment).

### 5.5.1 CHES IT Material Change Identification

Change initiatives (i.e., projects and programs) and other non-project activities for CHES can be initiated in numerous ways depending upon its nature and size. These include an *Investment Governance Framework*, a structured S&P level change initiation and triage process, and the Product Management process. (For further details, refer to *Section 5.2 Product Management*)

The materiality of Technology changes at ASX is determined by submitting the change through a risk assessment process in the ASX ITSM Platform. This assessment determines the impact of the change on the operation of CHES as well as its users, the type of change process that is required to be applied, and the level of approval required before implementing the change. Change risk is calculated according to probability and impact.

Approval is then provided by a peer reviewer, then is managed by and operated by approvers for each impacted service and then by the Change Manager, Change Advisory Board (**CAB**) and the Executive Management. Any changes to production are subject to assessment and approval via a weekly CAB meeting. For emergency changes, an emergency CAB meeting is held. The CAB operates under a Terms of Reference (**ToR**). Specific reporting of changes is submitted to the CAB for consideration, supplemented by divisional ITSM dashboards for on demand data on upcoming changes for review, and quarterly risk reporting, with updates to the Enterprise RMS, which is also incorporated in quarterly ITSM reporting.

Depending on the type of change, key artefacts have been defined that capture the following information:

1. Planned schedule dates/times.
2. Impacted Services.
3. Impacted Configuration items.
4. Business/technical justification.
5. Implementation plan (projects that are Tier 1 and 2 only).
6. Recovery plan.
7. Test plan and results.
8. Risk assessments.
9. Any additional information as required.
10. Conflict review with other ASX changes, maintenance windows, and blackout schedules.

### 5.5.2 Change Readiness Assessment

CHES changes are subject to an implementation readiness assessment to determine if they can be released into production as planned. The following assessments are conducted and reviewed with the CAB:

- Business Justification.
- Implementation Plan.
- Recovery Plan.
- Test Plan and Result – Test Summary results.
- Implementation Readiness document (projects only).



- Change Risk assessment.

CHES changes are subject to internal and external testing depending on its scope and impact which is determined by the *Quality Engineering and Testing Capability Practice Framework* which is part of the overall *ASX Delivery Framework*.

### 5.5.3 Change Testing for CHES

ASX has developed the *Quality Engineering and Testing (QE&T) Capability Practice Framework* which is part of the overall *ASX Delivery Framework*. The framework provides a set of rules, standards, controls, and guidelines that describe how to enact quality and testing for the project and technology changes. Quality and testing must be enacted at ASX for all projects and technology changes and references recognised industry frameworks such as the Test Maturing Model integration (**TMMi**) standards and the international standard ISO-IEC-IEEE-29119 Software Testing.

All CHES changes are subjected to some or all of the below tests depending on the scope and stakeholder involvement:

1. Functional Testing.
2. Non-Functional Testing (**NFT**).
3. User Acceptance Testing (**UAT**).
4. Regression Testing.
5. System Integration Testing.
6. End to End Testing.
7. Capacity Testing.
8. Performance Testing.
9. Rollback Testing.
10. Comms Test/Accreditation test plan.

A risk-based testing approach is used in finalising the test plan detailing the different types of tests conducted for the change aligned to the change risk. ASX has developed standard testing templates and processes which can be used while conducting tests and customised depending on the tests conducted. The majority of CHES test cases are automated using tools that allow for rapid and repeatable testing, a small proportion of tests are conducted manually due to integrations with upstream/downstream systems. Once testing is completed, a Test Summary Report (**TSR**) is generated that captures the test coverage, results and any metrics or defects that may have been observed as part of the test and this test report is provided as a key input into the implementation readiness process. The TSR is required to be signed off by the Head of Quality Engineering and Testing team prior to the change being deployed into production. Testing records including the TSR are retained within the Enterprise Issue and Project Tracking tool.

#### 5.5.4 Test Environments

The primary purpose of the test environment is to facilitate validation of the system/application/feature being developed.

ASX maintains test environments for both internal testing, as well as external test environments to facilitate CHES users' participation in testing.

#### 5.5.5 Change Release Process for CHES

At the completion of the agreed testing and approved test plans and results, Release notes are documented, and a change management authorisation request is raised to seek approval for promoting the change to production. This process is detailed in the *CHES Application Development Change Management Release Process* document.

#### 5.5.6 Change Communication

Per the Organisational Change Management (**OCM**) Framework, internal communication of CHES changes to impacted stakeholders occurs as part of the change management process through the involvement of relevant representation from the different teams.

For external communications, changes are communicated to external stakeholders and participants via the quarterly TURN report issued by the Enterprise Project Management Office (**EPMO**), as well as detailed Market Notices issued to CHES users and other stakeholders outlining the impacts of the relevant changes, where to find more information and go live dates.

Where external UAT is required, external communication will outline the changes made to the CHES external test environment along with steps required to be carried out by users to access the test environments and perform its own testing.

(For further details on the communication process, refer to *Section 8.1 Governance Structure and Supporting Processes*)

Current and Planned Initiatives	Status of Initiatives	Theme	Indicative Date
No additional initiatives identified (Related initiatives are in other sections).			

## 6 Security

The section below details the specific ASX responses to the ASIC requirements regarding ongoing Security of CHES.

### 6.1 Security Strategy, Governance and Risk Management

ASIC Requirement	Security b. (i) and Security b. (ii)	Objective	
			<p>Detail how the Licensee will ensure the confidentiality, integrity and availability of information obtained, held or used by the Licensee in relation to CHES, including maintaining availability of and authorised access to data.</p> <p>Detail how the Licensee will implement a system of security controls, monitoring and periodic testing of controls to ensure CHES is resilient to unauthorised access or disruptions due to cyber events.</p>

This section provides an overview of the key security controls that make up the layers of defence that protect CHES from inappropriate or unauthorised access and help to ensure it is resilient to any disruption caused by cyber events.

This section also outlines the risk management processes, governance structures and overall security strategy that underpins the control environment, providing a mature security capability in the prevention and detection of security events and recovery and resolution from security incidents.

#### 6.1.1 Security Governance - Overview

The overall goal of the Cyber Security Team is to provide a safe, secure, reliable, and adaptive security environment that meets the needs of both internal (Board, management, business) and external stakeholders (customers, participants, regulators) in the provision of cyber security services and protection of data and other technology assets.

The key objectives are to:

- Ensure the confidentiality, integrity and availability of data and services are maintained.
- Promote a security culture where staff are cognisant of security risks and are comfortable in raising and escalating security concerns.
- Provide ASX personnel with assurance they can conduct its day-to-day activities with confidence and ease through appropriate training and awareness.

- Ensure the timely communication of security matters to relevant parties.
- Adopt a risk-based approach to information security such that resources are deployed in an effective and efficient manner to meet ASX's very low technology and operational risk appetite.
- Ensure a best practice approach to security management, including being proactive in identifying security trends, maintaining continuous improvement in security tools and techniques, and complying with relevant regulatory standards and 'best practice' guides.

The assessment of cyber risk and definition of controls, policies and standards is the responsibility of the Cyber Security Team, however, the implementation and performance of cyber controls and compliance with security policies is considered an enterprise responsibility. Accordingly, teams such as Application Support and Technology Infrastructure are responsible and accountable for owning, operating, and maintaining controls within their remit.

The Technology Security and Governance team is responsible for security strategy, policy, risk management and overall control definition and governance for all ASX environments, including CHES. ASX has deployed a 'defence in depth' strategy in the management of security risk, with controls implemented at various levels of the technology stack. As such, although there are CHES specific security controls, many of the security controls that manage risks related to CHES are also enterprise controls. This is particularly relevant for overall cyber security governance and risk management.

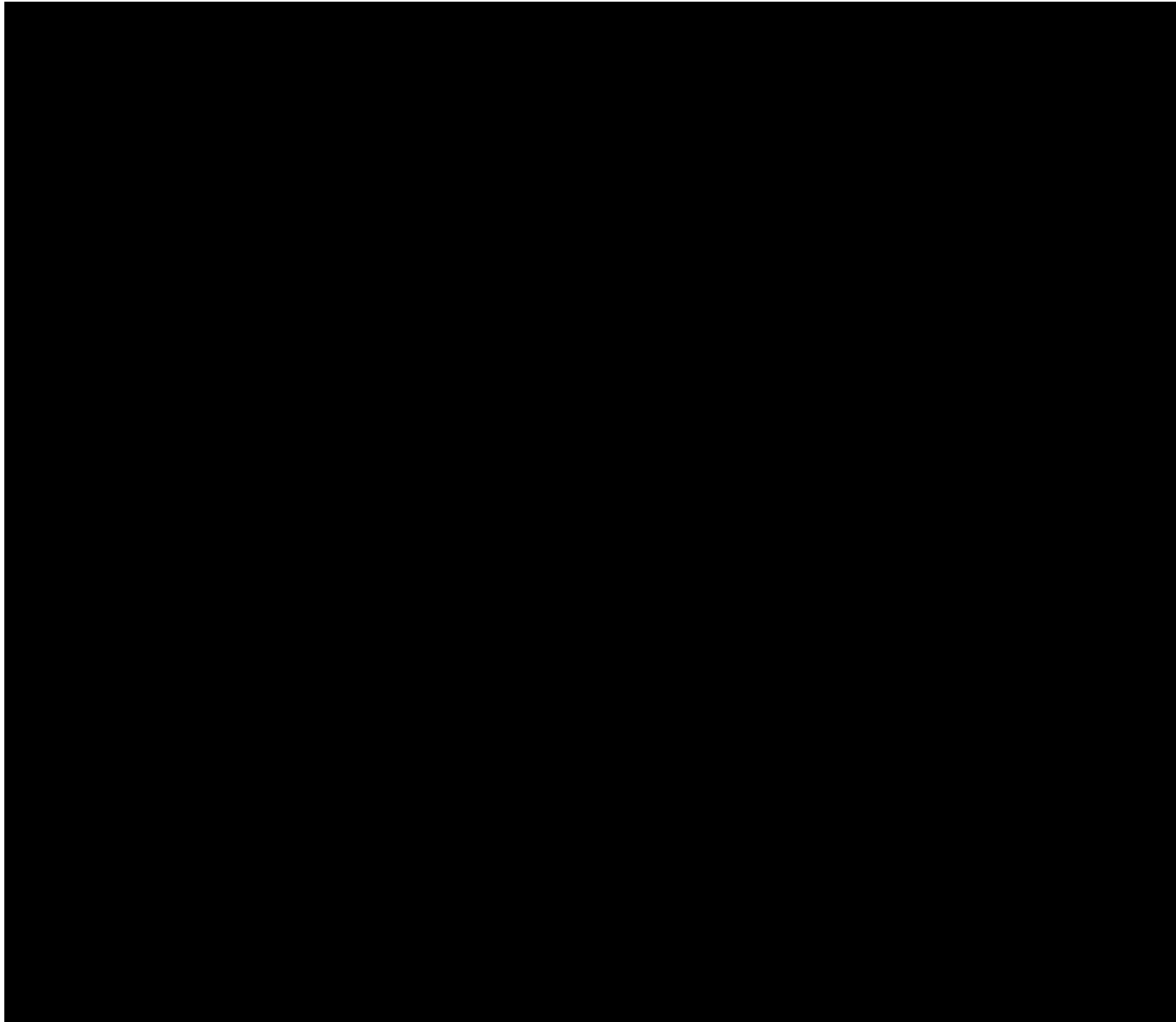
[REDACTED]

Governance of the Cyber Security function is achieved through various general and cyber specific risk forums and Executive Management and Board Committees. (For further details on governance forums and monitoring, refer to *Section 5.1 Risk Identification and Assessment / Management and Monitoring*)

### 6.1.2 Cyber Security Team Structure and Responsibilities

Cyber Security is an enterprise function centralised with the Technology Security and Governance team in the Technology and Data business division. The General Manager, Technology Security and Governance has overall responsibility for cyber security and reports to the CIO and has independent and unfettered access to the Chair of the Technology Committee. (For further details, refer to *Figure 6.1.2.A Cyber Security Team – Organisation*)

Oversight of cyber security, data governance and risk management activities are performed by a number of Board and management committees. The details of various governance committees are outlined in *Section 5.1 Risk Identification and Assessment / Management and Monitoring*. These committees consider a range of cyber and data management activities, including operational incidents, risk environment, roadmap delivery and overall cyber strategy.



The Technology Security and Governance function is composed of the following teams:

- **IAM** – The IAM team [REDACTED] is responsible for internal user access management (i.e., user access add/change/delete), managing user access reviews, integrating applications with the IAM system, administering privileged access management, and the support and maintenance of the IAM systems. [REDACTED]
- **SOC** – The SOC team [REDACTED] is responsible for security monitoring processes and procedures (e.g., playbooks), threat hunting, incident management (including analysis, investigation, response, and remediation), vulnerability scanning and threat intelligence (including threat assessment). [REDACTED]
- **Security Domain** – The Security Domain team [REDACTED] is responsible for the delivery of the security strategy and roadmap items, facilitation of priority calls, management of the security delivery budgets and reporting to the PWG. The Security Domain team works with other security teams and cross functional ASX teams to deliver the security roadmap. [REDACTED]
- **Security Architecture and Assurance** – This team [REDACTED] is responsible for overall policy and standard development, security assurance (e.g., penetration testing and red teaming), security architecture and design, consulting to other ASX projects, and product and tool evaluation. [REDACTED]
- **Technology and Data Risk Management** – This team [REDACTED] are responsible for Line 1 risk management in line with the ERM Framework. While the team does not own the risks and controls, they are tasked with providing risk management support and advice to the Technology and Data teams and also facilitate the preparation of reports to the various governance forums, including KRI reporting to Board and management. [REDACTED]
- **Data Governance** – The Data Governance team [REDACTED] is responsible for the implementation of the Data Governance Framework, assessment of data governance incidents and performance of data impact assessments and ad hoc data risk assessments. [REDACTED]
- **Vendor Management** – The vendor management team [REDACTED] is responsible for supporting the sourcing and procurement of goods and services, ensuring compliance with the procurements and vendor management frameworks, and managing the critical service provider process. [REDACTED]

The centralisation of the cyber, data and technology risk management teams facilitates strong collaboration across cyber and data security and operational risk management. In addition, Security and Governance teams work closely with the various technology and operations teams in other business divisions and

corporate functions to manage security risk. In particular, the teams work closely with the Technology Infrastructure team regarding network, hosting and data centre security, and the Application Support teams in the business divisions regarding application security (e.g., CHESS Application Support team).

### 6.1.3 Security Strategy, Budget, and Resourcing

The Cyber Security Team develops an annual *Cyber Security Strategy* that is approved by the ASX Technology Committee, ASX Limited Board and CS Boards. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]



#### 6.1.4 Risk Management

The ASX Board and management have identified cyber risk as one of ASX's top 3 three risks and views cyber risk as an enterprise responsibility. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

All risks are tracked and managed through ASX's ERM system. The key categories of risks identified in the ERM system (applicable to CHES) include:

- Malware.
- Inadequate frameworks.
- Insider risk/internal fraud.
- Strategy or roadmap delivery.
- System or data compromise.
- Ineffective change management.
- Resourcing.
- Third parties.

[Redacted]

[Redacted]

### 6.1.5 Assurance and Audit

The need for risk and control assurance is driven by a combination of internal ASX desire for control effectiveness testing and verification, external regulatory requests, and market rule requirements. Assurance is provided by a combination of internal teams (e.g., Security Team self-assessment, enterprise risk review, internal audit) and external specialists (e.g., external auditors and specialist cyber security firms).

The Cyber Security Team have developed an annual penetration testing plan and works with the business and enterprise risk, compliance, and audit teams to determine the annual audit activities.

The assurance work performed in FY22 included:

- SWIFT Customer Security Program (**CSP**) compliance.
- ASAE 3402 audit for CHES.
- ASAE 3402 audit for Austraclear System, Financial Settlement Manager (**FSM**) and Derivatives Clearing System (**DCS**).
- CHES Replacement security assessments and audits.
- Various application penetration tests.
- Perimeter and website penetration tests.
- Purple team testing (incorporating both attack and defence perspectives).
- Network penetration tests.

[Redacted]

---

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED] e
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

---



## 6.2 Identity and Access Management

ASIC Requirement	Security b. (i) and Security b. (ii)	Objective	
			<p>Detail how the Licensee will ensure the confidentiality, integrity and availability of information obtained, held or used by the Licensee in relation to CHES, including maintaining availability of and authorised access to data.</p> <p>Detail how the Licensee will implement a system of security controls, monitoring and periodic testing of controls to ensure CHES is resilient to unauthorised access or disruptions due to cyber events.</p>

IAM involves the management of internal identities and access rights and entitlements throughout ASX’s technology environment, including CHES.

ASX’s *Identity and Access Management Policy* outline the principles for managing all internal identities and service or generic accounts. The policy includes coverage of the onboarding of new users, making changes to existing users, terminating accounts, and performing user access reviews. The policy also provides an overview of key controls in regard to:

- Privileged access management.
- Stale account management.
- Principle of least privilege.
- Segregation of duties.
- Password management.

[Redacted]

### 6.2.1 Identity Management

[Redacted]

[Redacted]

- [Redacted]

For CHES, no entitlements or access rights are assigned by default. These are explicitly requested in accordance with an established process and a pre-defined/authorised entitlements master table. This enforces the principles of Segregation of Duties (SOD) and least privileges to ensure that entitlements are not more than what is required to perform a particular role. Access rights vary based on the role and the functions of the teams that access CHES for different business processes. An initiative to enhance and define the access controls at a team level is currently in progress to help document and formulate granular access.

[Redacted]

### 6.2.2 Password Security

Identities are authenticated using passwords that are in accordance with the defined and approved ASX password standards. These standards include common parameters such as minimum password length, password expiry and password history, and are applicable for all systems at ASX including CHES.

[Redacted]

### 6.2.3 Segregation of Development and Production System Access

[Redacted]

### 6.2.4 Privileged User Access Management

Privileged accounts are those identities that have administrative level access privileges for CHES. A privileged user IAM solution, [Redacted], has been implemented that allows access approval workflows, [Redacted]

[Redacted] etailed processes and guides are available for the management of such privileged user identities and its access rights.

### 6.2.5 Remote Access Management for Internal and External users

ASX permits selected users to connect to the systems remotely for business purposes in accordance with the *Mobility and Remote Access Standard*. Remote access is not granted to ASX's systems, including CHES by default. All remote access requests, beyond the usual corporate connectivity, need explicit approvals from business, security, and technology teams. Further, all remote access to systems is enabled through secured transport channels [Redacted]

[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]

### 6.2.6 Participant Authentication, Authorisation and Access Management

CHES is contained within a closed network, not exposed to the internet, and accessible only to known participants who would interact with CHES via their own systems via the message-based interface. Participants who connect to the CHES environment are authenticated and authorised using a number of

identification attributes [REDACTED]  
[REDACTED] The assignment of these attributes follows a standard onboarding approval process.

[REDACTED]

### 6.2.7 Audit Trails and Logs



### 6.3 Data Security

<p><b>ASIC Requirement</b></p>	<p>Security b (i) Security b. (ii)</p>	<p><b>Objective</b></p>	<p>Detail how the Licensee will ensure the confidentiality, integrity and availability of information obtained, held or used by the Licensee in relation to CHESS, including maintaining availability of and authorised access to data.</p> <p>Detail how the Licensee will implement a system of security controls, monitoring and periodic testing of controls to ensure CHESS is resilient to unauthorised access or disruptions due to cyber events.</p>
--------------------------------	--	-------------------------	--

Data Security involves the application of layered security controls to protect information assets. ASX has deployed a ‘defence in depth’ approach to maintaining the confidentiality, integrity, and availability of CHESS data throughout the information lifecycle.

Data Security encompasses a range of control domains, including:

- Data Governance and Management.
- Data Management Lifecycle.
- Data Classification.
- Data Security.
- Physical Security.
- Logical Security.
- System and Network Security.

These domains are applied to ensure that data is secured throughout its lifecycle and as it passes through various layers of the technology stack. The sections below provide an overview of the controls deployed.



### 6.3.1 Data Governance and Management

ASX has an overarching organisational data governance strategy to support the rollout of good data management practices with the following objectives:

- Data is originated and stored to meet user and regulatory requirements.
- Data is discoverable and consistently presented.
- Data is adequately protected against unauthorised use.
- Data is used appropriately.
- Users are properly trained and equipped to use the data

A high-level inventory of key data assets has been developed and overall data ownership assigned. While the Data Governance team are responsible for the data governance framework and strategy, the data itself is owned by the relevant business owner.

A data impact assessment process is in place to assess the risks associated with certain data activities such as the adoption of cloud services or exposing data to new systems or users. A data breach notification process is in place to assess suspected data breaches, including whether a report is required to be submitted to the Office of the Australian Information Commissioner (**OAIC**). An online reporting mechanism is in place to facilitate staff reporting of potential data incidents. These processes are managed by the Data Governance team within the wider Technology Security and Governance team. A Data Governance Group consisting of senior ASX executives has been established to oversee the activities of the Data Governance team.

### 6.3.2 Data Management Lifecycle

*Data Handling Procedures* are in place to facilitate the secure treatment of data throughout its lifecycle. The procedures provide an overview of the control's requirements, depending on the data classification, for each stage of the lifecycle from creation, use, retention, and disposal of data to ensure that the confidentiality, integrity, and availability of data is appropriately maintained.

The key steps as defined within the approved *Data Handling Procedure* include:

- Identification of a data source.
- Identification of data owner.
- Sensitivity assessment of data being handled.
- Data risk assessment.
- Application of minimal control standards as per the approval by the respective data owner and the relevant stages of the data lifecycle.

### 6.3.3 Data Classification

ASX has an internal team responsible for performing data classification assessments with the objective to apply a classification label to data within a system. The data within CHES has been classified as 'Highly Protected', the most sensitive classification as defined within the *ASX Data Handling Procedure*.

### 6.3.4 Data Security

[Redacted]

#### 6.3.4.1 Security at the Network Layer

[Redacted]

[Redacted]

#### 6.3.4.2 Security at the Application Layer

CHES data messages between ASX and participants are encrypted using secret keys. [Redacted]  
[Redacted] Industry good practices for key management (master and backup) are utilised to ensure the safety and security of keys.

### 6.3.5 Encryption of Back-ups

CHES data is backed-up [Redacted] and is stored in an off-site location. CHES backups are encrypted using industry good practice configurations. (For further details on backups, refer to *Section 7.3 Monitoring of Backups and Incidents*)

### 6.3.6 Physical Security

The infrastructure supporting CHES is hosted in secure data centre environments that provide physical and environmental controls. [Redacted]  
[Redacted]



---

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]		

---

## 6.4 Systems Security

ASIC Requirement	Security b (i) Security b. (ii)	Objective	Detail how the Licensee will ensure the confidentiality, integrity and availability of information obtained, held or used by the Licensee in relation to CHESS, including maintaining availability of and authorised access to data. Detail how the Licensee will implement a system of security controls, monitoring and periodic testing of controls to ensure CHESS is resilient to unauthorised access or disruptions due to cyber events.
------------------	------------------------------------	-----------	---

ASX employs a range of risk-based security controls and procedures and has implemented a ‘defence in depth’ approach ensuring there are layered controls at all levels from the ASX perimeter to the back-end infrastructure. The Security Team is responsible for assessing the security requirements and overseeing the management and maintenance of the security controls and procedures, including:

### 6.4.1 Perimeter and Email Controls

- [Redacted content]

#### 6.4.2 Operational and Access Management Controls

- [Redacted]

#### 6.4.3 Endpoint Controls

- [Redacted]

#### 6.4.4 Network Controls

- [Redacted]

#### 6.4.5 Policies and Procedures

- Policies and standards for communicating minimum security requirements, system hardening and security responsibilities.
- Playbooks that document the relevant procedures for performing BAU activities and responding to incidents.

#### 6.4.6 Partnerships

- Partnerships with specialist security partners and government agencies to support threat intelligence gathering, threat hunting, incident management and security roadmap delivery processes.
- Membership of peer organisations, domestically and globally, to gain access to threat, vulnerability, and other cyber-event related intelligence.

### 6.4.7 User Training and Awareness

[Redacted]

### 6.4.8 End User System Security

[Redacted]

#### 6.4.9 Hardware and Operating Systems Security

Hardware and operating systems supporting CHES are secured and configured in accordance with enterprise security standards. [REDACTED]. Further, ASX has developed a baseline configuration for the operating system based on better practices, vendor guidance and subject matter expertise within the team.

#### 6.4.10 Network Security

The infrastructure supporting CHES is hosted in a segregated segment of ASX's network that has no direct access to or from the Internet. Infrastructure controls (e.g., firewalls, routers / Access Control Lists (**ACLs**)) are designed to restrict communication to authorised usage of networks and segregate network zones/environments. [REDACTED]

[REDACTED] Access to these networks is restricted to known CS Participants that have been authorised by the business.

At the enterprise level, ASX has deployed multiple technologies to protect the network from cyber-attacks. [REDACTED]

#### 6.4.11 Security in Software Development Life Cycle (SDLC)

Software code related to CHES application is hosted and managed internally by ASX using a custom-built Code Management System (**CMS**) that supports storage, version control and general management of the code. [REDACTED]

---

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]		

---



## 6.5 Threat and Vulnerability Management

---

ASIC Requirement	Security b (i) Security b. (ii)	Objective	Detail how the Licensee will ensure the confidentiality, integrity and availability of information obtained, held or used by the Licensee in relation to CHES, including maintaining availability of and authorised access to data.  Detail how the Licensee will implement a system of security controls, monitoring and periodic testing of controls to ensure CHES is resilient to unauthorised access or disruptions due to cyber events.
------------------	------------------------------------	-----------	---

---

### 6.5.1 Threat Management

ASX Board and management recognise cyber security as one of ASX’s top risks and the ASX environment, including CHES, is subject to a range of threats and vulnerabilities. Threat management is a core function of the Security Team and includes the identification, analysis, and response to threat related information.

Threats and vulnerabilities are identified through a number of sources, including:

- Commercial threat intelligence providers.
- Industry threat intelligence providers [REDACTED]
- [REDACTED]
- Vendor notification.
- Peer networks.
- Open-source threat intelligence.
- Automated vulnerability scanning.
- Internal staff reporting through the Mimecast tool and SPAM Reporting mailbox.

The SOC is the primary team responsible for the ingestion and analysis of the threats and vulnerabilities. The threats may be received manually or ingested directly into security tools and systems [REDACTED]. The SOC is also responsible for threat hunting within the environment such as searching for reported indicators of compromise. The SOC (and other Security Teams) also has the ability to direct other ASX teams to perform analysis on its behalf (e.g., code or environment reviews by specific application support teams).

While threat assessment and analysis are primarily a SOC responsibility, remediation and response could be performed by a variety of teams depending on the nature of the threat. The SOC has the ability to perform a number of tasks [REDACTED] however, the SOC (and other Security Teams) may also request other teams to perform remedial activities [REDACTED]. Remedial actions could be focused on specific tasks [REDACTED] through to wider actions such as the implementation of or changes to overarching controls or operational procedures.

Threats are generally managed at an organisational level; however, the processes apply to the CHES environment. [REDACTED]

### 6.5.2 Vulnerability Management

Vulnerability management includes the identification, assessment, and remediation of vulnerabilities by prioritising the most critical vulnerabilities followed by appropriate risk assessment and mitigation for those vulnerabilities which cannot be remediated.

Vulnerabilities and control weaknesses are identified through a number of sources, including:

- [REDACTED]

In line with the organisation's Security Patching Policy, ASX has implemented processes, standards, and technology to proactively prevent, detect, and remediate vulnerabilities. [REDACTED]

Patch management in line with ASX's patching policy. [REDACTED]  
[REDACTED] Security patches are evaluated to determine remediation priority and follow the standard IT change management process before being deployed to the environment.

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

## 6.6 Security Monitoring and Response

ASIC Requirement	Security b (i) Security b (ii)	Objective	Detail how the Licensee will ensure the confidentiality, integrity and availability of information obtained, held or used by the Licensee in relation to CHES, including maintaining availability of and authorised access to data.  Detail how the Licensee will implement a system of security controls, monitoring and periodic testing of controls to ensure CHES is resilient to unauthorised access or disruptions due to cyber events.
------------------	-----------------------------------	-----------	---

The security team has enterprise wide capabilities in place that enable continuous monitoring of systems and infrastructure, including CHES. These are complemented by additional monitoring for operational activity performed by the application support teams.

Security monitoring is performed by the SOC and includes automated collection and analysis of logs/events that are generated by systems that support ASX environment. [REDACTED]

### 6.6.1 ASX's xChange Cyber Security Centre (XCSC) SOC Capabilities

[REDACTED]. The combined experience of the team provides a good mix of knowledge of ASX's processes, applications and technical environments, and industry experience of working in security operations. In addition, there are agreements in place with external [REDACTED] partners to support the team in engineering, analysis, and incident response as required.

The SOC has a mature set of processes and procedures documented in playbooks that, combined with the team experience and external subject-matter-expert support, underpins the security monitoring and response capability.

The SOC has a wide remit to assess, investigate and respond to events as appropriate, however, the key monitoring and response functions include:

- **Business Engagement** – Engage with business teams, technology governance and risk management team to identify areas to support the ASX strategy.
- **Security Engineering** – Help secure and monitor technology environments that support business processes by defining, selecting, and managing various security controls/tools.

- **Event Triaging** – Interpret the security events generated by systems, users or external entities and triage for analysis to identify potential security incidents for response and recovery.
- **Incident Management and Response** – Manage security incidents within the overall ASX incident management framework, including escalation and communication.

### 6.6.2 Security Incident Management and Response

Security incidents are responded to in accordance with documented policies, playbooks, and procedures, and managed in accordance with the overarching ASX Incident Management process. There are specific actions to be taken in response to a security incident, including, where appropriate, Government agency notification, internal and external escalation and specific containment, remediation, and response processes.

The security incident response process is made up of three phases:

1. Detection and Analysis.
2. Containment, Eradication and Recovery.
3. Post-incident activity.

The '*Cyber Security Playbooks*' address several scenarios based on key cyber risks identified and recorded in the ERM system. The playbooks are structured consistently to provide the response team specific guidance in responding to typical incidents/events and provide an outline of:

- Roles and responsibilities.
- External Contacts.
- Detection and Monitoring.
- Triaging.
- Investigation.
- Containment.
- Recovery.

The playbooks contain links to other ASX wide processes, including the incident and crisis management processes. (For further details on how broader BC and disaster recovery controls operate, refer to *Section 7.1 Business Continuity and 7.2 IT Disaster Recovery (DR) and Service Continuity*)

[Redacted text block]

### 6.6.3 Periodic Testing and Improvement

There are a number of activities undertaken to test and practice the threat hunting, analysis and remediation and response capabilities. [Redacted text]  
[Redacted text] These are designed to test ASX's people, process and tool capability and maturity.

[Redacted text block]

In addition, documentation, including playbooks, are periodically updated through lessons learnt and improvements identified as the team responds to different cyber events and potential security incidents.

[Redacted text block]

## 7 Continuity

The section below details the specific ASX responses to the ASIC requirements regarding ongoing Continuity of CHES.

### 7.1 Business Continuity

ASIC Requirement	Continuity (i)	Objective	
			Establish, implement, test and maintain continuity plans that include response and recovery processes for any event that would or would be likely to cause significant disruption to CHES, including (but not limited to) server or network infrastructure failures, software failures, cyber incidents, and business process failures.

Continuity plans for CHES (and CORE) have been established, implemented, tested, and maintained in line with the broader requirements of the *ASX Business Continuity Management Framework (BCMF)*.

#### 7.1.1 Business Continuity Framework

ASX has defined a BCMF to enable Executive Management and business divisions to assess, implement, monitor, and improve the effectiveness of BC procedures. The framework is aligned with the Business Continuity Institute’s Good Practice Guidelines (2018 Edition), the international standard for business continuity and recognised global best practices. In addition, emerging practices and developments (e.g., CPS 230 and recent ASIC Market Integrity Rule changes) are considered by ASX in the ongoing maintenance of the BCMF. This leading practice is also considered in reviewing the approach taken to the Business Impact Assessment, Business Continuity Plans, and testing/ maintenance activities.

The BCMF consists of four pillars covering the approach and oversight of Business Continuity Management (**BCM**), which includes:

- **Crisis management** – Management and overall direction/oversight of BC and resumption activities following a crisis.
- **BC** – Arrangements (including technology/IT incident management), which include individual Business Continuity Plans (**BCPs**) and technology Disaster Recovery Plans (**DRPs**), which enable the continued delivery of activities, products and services and recovery of key processes at alternate sites.
- **Business resumption** – The resumption of normal business activities at either the existing or new primary site following a crisis.
- **Exercise and awareness** – The regular testing of framework elements and staff’s general understanding of BCM activities.

In line with the requirements of the BCMF, individual department-level BCPs have been established based on a centrally managed template, which includes recovery processes for the unavailability of CHES. The individual department-level BCPs include the following details:

- Name and contact details of plan owner, BCP coordinator, crisis management contacts, and media and communications team.
- Employee hotline phone number for initial response.
- Scope and assumptions.
- Criticality ranking and Recovery Time Objective (**RTO**) for applications essential to market and CS facilities operations.
- High-level recovery strategies for different scenarios including the loss of access to the properties, systems, and sites as well as strategies for pandemic and potential cyber-attacks.

[REDACTED]

A quarterly Risk Committee meeting is held to discuss various risk-related topics. In the January 2023 meeting, an overall assessment of the BCM program was presented to the Risk Committee, informing them about the various initiatives currently in progress to further improve the BCM program, including KRIs and metrics.

The Risk Committee is responsible for approving, monitoring, and assessing the BCMF. Roles and responsibilities for BCM at ASX, such as the Framework Owner, Group Business Continuity Manager, BCP Analyst, Business Continuity Plan Owner, Business Continuity Coordinators/Risk Champions, and staff are captured in the BCMF.

### 7.1.2 CHES Architectural Resiliency

CHES, though legacy in nature, is built on a highly resilient architecture which ensures that data and transactions are not lost during any failures.

The key components of the CHES resilient architecture include:

1. **Data Centres** – CHES is hosted across two data centres in Australia. [REDACTED]
2. **Hosting Infrastructure** – CHES hosting infrastructure is configured in a like-for-like manner at both the primary and secondary data centres which allow the secondary data centre to take over as the primary should there be a failure. Within the hosting infrastructure, a number of components are designed to support resilience, ranging from front end servers, messaging middleware, back-end application nodes, database, log servers, and application control systems.
3. **Load Balancers** – All incoming transactions are distributed to CHES using load balancers. The load balancers assist in redirecting traffic to the secondary data centre in the event of a disaster scenario.



4. **Storage** – Enterprise storage arrays provide the required storage processing power for both the primary and secondary data centres and support the synchronous replication of data by the [REDACTED] from the primary site to the secondary site.
5. **Network Connectivity** – High speed network is available across both the primary and secondary data centres for data traffic and supporting data replication. The networks consist of redundant devices that allow continuity of operations during failures.

### 7.1.3 Scenario Testing

The *BCM Exercise Framework* includes guidelines for BC exercises and testing in accordance with the ASX BCMF. The purpose of conducting regular exercises is to verify the effectiveness of BCP, DRP and Crisis management processes. The document also covers the type of exercises which can be conducted for different scenarios. For example, a weekend internal systems DR exercise will cover scenarios such as loss of systems, loss of access, and loss of site. The framework is reviewed at least annually, and changes are incorporated as appropriate with the endorsement of the CRO. The framework is approved by the Audit & Risk Committee every three years.

In order to confirm that the BCP model remains appropriate, a *scenario risk assessment* is conducted [REDACTED]. This analysis considers potential crisis/disaster incident scenarios, event likelihood factors and the current control environment in place. The *Business Continuity Scenario Risk Assessment* details example scenarios for each site (primary and secondary) grouped under relevant risk event scenarios. The relative likelihood is then considered by assessing various factors that may increase or decrease the likelihood of an incident and the BCP is updated as appropriate.

The initiatives below are identified to maintain the low risk appetite for matters relating to CHES.

Current and Planned Initiatives	Status of Initiatives	Theme	Indicative Date
Review CHES resilience scenario testing	Planned	Continuity	Jul 2024
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

## 7.2 IT Disaster Recovery (DR) and Service Continuity

ASIC Requirement	Continuity (ii)	Objective	
			Ensure that disruption scenarios are periodically tested, continuity plans are continually improved, and resources (including any external parties) that are required to engage with such plans are trained and familiar with its roles and responsibilities.

ASX performs BC/DR planning to support operational resilience and the ability to respond and deliver critical operations in the event of technology disruption. In particular, DR planning supports the ability to manage the potential loss of critical systems (including supporting technologies, data, technology staff resources and/or data centres). The objective of DRPs is to provide detailed recovery procedures for a service to ensure that core systems, hardware and data are available at the alternate site on a timely basis, to support business activities in the event of a disruption.

### 7.2.1 BC/DR Testing

BC/DR exercises are performed annually, where the CHES application is placed in failover mode and run fully operationally from the secondary data centre site for a week before reverting to the primary site. Permanent dual-site operational teams are based at both the primary and alternate operations sites (including the use of remote working arrangements), which effectively tests backup operational processes on a continuous basis and ensures that the alternate site can always be fully operational.

The CHES Application Owner follows a document that provides detailed testing requirements, procedures and steps undertaken during the annual CHES testing. The CHES Application Owner is responsible for running the DR test for CHES to ensure it meets the annual requirement. Annual planning activities include reviewing changes (if applicable) that may have occurred since the last DR test to ensure the task list is updated and the relevant teams are ready before the agreed test date. Responsibilities are allocated for testing activities, including the execution of failover steps and the failback steps. The DR run sheet for CHES has been developed and refined over a number of years and kept up to date based on the findings from each annual test. There is a planned initiative to document a formal RACI Matrix for the annual CHES DR testing.

Teams from CHES support, hosting services, settlement operations and SWIFT support are involved in the testing activities. The test runs for a week, with the main tasks required for site reversal performed on Saturdays (non-Business days) on either side of the week.

Per the ASX BCM Exercise Framework, the DR test can be determined as successful, unsuccessful, or partially successful. The CHES Application owner determines the test's outcome, and the General Manager of S&P Technology gives the final approval to the outcome determined by the Application Owner.



The last BC/DR exercise for CHES was successfully performed in █████ 2022; the next exercise is scheduled to be performed in █████ 2023. During the CHES testing exercise, it was noted that the RTO achieved for CHES complies with the RBA recovery time requirements per the *Business Continuity and Security Standards for Reserve Bank Information and Transfer System (RITS) Members – December 2022*. The components tested included the application, database, client connectivity, batch processing and interfaces.

The last BC/DR exercise for CORE was successfully performed in █████ 2022; the next exercise is scheduled to be performed in █████ 2023. For CORE, a workbook has been established to provide a comprehensive step-by-step guide on how DR testing is performed for the CORE application. As per the last exercise, the recovery time for CORE was within the defined RTO.

### 7.2.2 Training and Awareness

ASX develops comprehensive training materials for BCP and DR teams consisting of a high-level understanding of the BCP and DR concepts, roles and responsibilities and the different scenarios of BCP. The training helps staff to understand how BC is applied, including relevant tools and templates.

Role specific, hands-on training is provided to BC Coordinators and BCP owners in relation to their BIAs and BCPs – and the functionality in relation to completing and maintaining the accuracy of those plans within the ERICA system.

The most recent iteration and release of BCM eLearning training was launched in Q3FY23 and is mandatory for all staff, including new starters. The training includes a refresher about the roles and responsibilities of Group Executives/Business division General Managers/Senior Managers, Business Continuity Plan Owners, and Business Continuity Coordinators.

### 7.2.3 Third-party dependency

Both CHES and CORE have no dependencies on any third parties for DR-level testing as both systems are maintained and managed in-house.

### 7.2.4 Reporting

The outcomes of CHES DR tests are reported to the Risk Committee and the Board ARC. There is a Board KRI related to the outcome of system DR testing.

Current and Planned Initiatives	Status of Initiatives	Theme	Indicative Date
No additional initiatives identified (Related initiatives are in other sections).			

### 7.3 Monitoring of Backups and Incidents

---

ASIC Requirement	Continuity (iii)	Objective	Implement regular backup and recovery (from backup) procedures to ensure access can be re-established following a disruption event resulting in loss or corruption of data.
------------------	------------------	-----------	---

---

#### 7.3.1 Security Incident Management and Response

The *ASX Daily Backup and Restoration Policy* is the overarching document that applies to the production environments, detailing the minimum requirements for backup and restoration of backups. The policy provides guidance on the requirements of performing risk assessment for systems (to support the determination of backup requirements) and also provides other guidance for the backup and restoration process, including responsibilities, the backup schedule, guidance on backup media available, storage and transportation requirements, retention periods, restoration testing guidelines, disposal, and security of backup media. There is a planned initiative to review and update backup policies more frequently.

Backups and backup media are encrypted in accordance with the *ASX Daily Backup and Restoration Policy* which requires that “Backups must be subject to access control and other security and integrity mechanisms (e.g., encryption) to protect the backup from modification or unauthorised access”.

This third-party service provider is also responsible for the secure destruction of physical media. ASX has a defined *Secure Deletion and Disposal Standard* to guide the approach to media destruction. ASX has also defined a *Media and Hard Disk Drive (HDD) Disposal Procedure* that details the process of securely destroying media.

#### 7.3.2 Monitoring

The *ASX Daily Backup and Restoration Policy* mandates that the backup teams verify the backups' performance and completion. Robust monitoring processes are in place, operated by the Hosting and Operations team, to ensure backups occur and any issues are quickly identified and resolved.

An enterprise backup and recovery solution are used for managing backups. The backup system uses Technical Policies that implement the scope of backups (to disk and tape), the schedule, retention, and off-site tape retention.

[Redacted text block]

### 7.3.3 Third-Party Support

[Redacted text block]

Current and Planned Initiatives	Status of Initiatives	Theme	Indicative Date
No additional initiatives identified (Related initiatives are in other sections).			

## 7.4 Restoration of Backups

ASIC Requirement	Continuity (iii)	Objective	Implement regular backup and recovery (from backup) procedures to ensure access can be re-established following a disruption event resulting in loss or corruption of data.
------------------	------------------	-----------	---

### 7.4.1 Restoration of Backups

Restoration requirements are detailed in the *Business Continuity and Security Standards for RITS Members - December 2022* as issued by the RBA, ASX is required to comply with these requirements. The standard provides guidance on the restoration requirements of secure backups. CHES is currently compliant in relation to the offline tapes backups which meet all requirements. [REDACTED] Restoration testing from backups is currently being performed for the CHES application. The current restoration testing procedure is aligned with *Section 5.5 Testing and Change of the ASX System Backup Policy CHES* which requires that backups be restored on demand. There is a planned initiative to align the backup restoration requirements with *Business Continuity and Security Standards for RITS Members - December 2022*. A similar initiative will be undertaken for CORE.

A documented procedure for restoring the CHES database from tapes and online backups has been created, and requests can be submitted as service requests to the internal helpdesk.

The initiatives below are identified to maintain the low risk appetite for matters relating to CHES.

Current and Planned Initiatives	Status of Initiatives	Theme	Indicative Date
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
CHES - Review backup and restore processes	Planned	Continuity	Mar 24
CORE - Review the backup and restore processes	Planned	Continuity	Mar 24

## 8 Governance

The section below details the specific ASX responses to the ASIC requirements regarding ongoing Governance of CHES.

### 8.1 Governance Structure and Supporting Processes

---

ASIC Requirement	Governance d (i)	Objective	
			What governance arrangements (including Board level oversight and management structures) the Licensee has in place to ensure ongoing monitoring and management of any risks to the performance and operation of CHES and availability of its services, and the adequacy of financial, technological and human resources (including any external parties and outsourced services)

---

ASX has in place a structured and robust governance framework to ensure clarity on the different roles and responsibilities and monitoring and management of any risks to the performance and operation of CHES. ASX's governance is summarised into four layers – *Board Governance, Management Governance, Project Governance and Performance and Operations* in order to manage risks to the performance and operations of CHES.

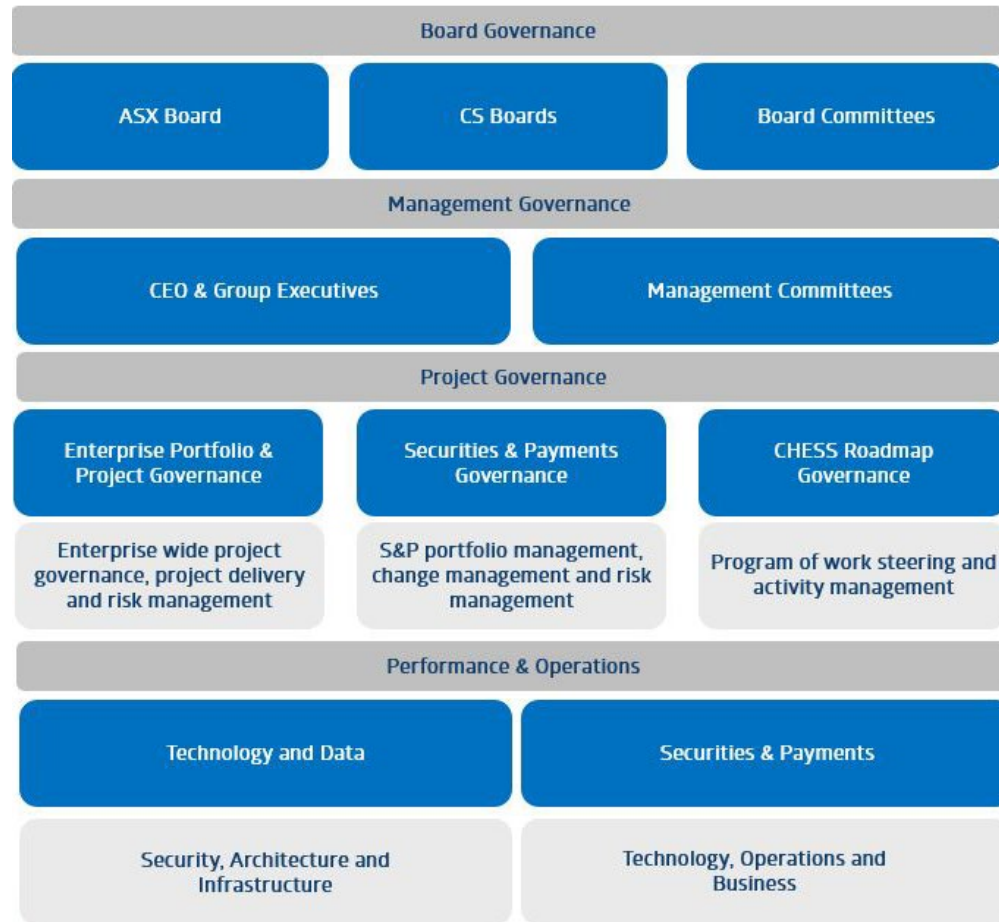


Figure 8.1.A ASX Management and Governance Structures Overview for CHES



### 8.1.1 Board Governance

The Board governance layer consists of ASX Board, CS Boards, and the Board Committees. (For further details on Board level Governance, refer to *Section 3.2 Roles and Responsibilities of the ASX Group Boards*)

### 8.1.2 Management Governance

This governance layer consists of the Executive Management structures relevant to CHES. (For further details on Board level Governance, refer to *Section 3.3 Roles and Responsibilities of Management*)

### 8.1.3 Project Governance

This section outlines the different governance bodies and frameworks which are responsible for governing the performance, risk management and operation of CHES for both BAU change and projects.

#### 8.1.3.1 Enterprise Portfolio & Project Governance

##### 8.1.3.1.1 ASX Delivery Framework

The *ASX Delivery Framework* provides the process/tools/deliverables for the successful execution of projects/programs within a Portfolio/ Business division. The ASX Delivery Framework is made up of the following sub-components: Project Management, Business Analysis, Enterprise Architecture, Solution Engineering, Quality Engineering and Testing, Organisation Change Management, and Project Delivery Assurance.

#### Project Management

The ASX EPMD is responsible for the following:

- Delivery of Policies & Standards.
- Delivery of Methods, Tools, and Guidelines.
- Delivery of compliance measurement and insights.
- Delivery Methodology continuous improvement.
- Preparation of reporting to governance bodies.

The EPMO maintains the Delivery Governance Model and provides integrated, sustainable, and pragmatic project support services, tools and frameworks that enable ASX projects and practitioners to safely deliver successful business outcomes. The EPMO supports Delivery Governance & Reporting, PWG and PGG support and advisory, quality control and review of documents, Risk, Assumptions, Issues and Dependencies (**RAID**) and risk management support and project tooling.

Change initiatives that meet the definition of a project are delivered via the enterprise wide *ASX Delivery Framework*. The framework sets out the governance arrangements, assurance, ownership, mandatory artefacts and deliverables, roles and responsibilities, and RACI that all project change initiatives follow at the ASX. It combines the disciplines of business analysis, project management, engineering, architecture, organisational change management, testing and assurance together into a consolidated view. It is mandatory for all projects to comply with the ASX Delivery Framework.

Only change initiatives that meet the ASX definition of a 'Project' are delivered via the *ASX Delivery Framework*, the extent of governance is then driven by the allocation of a Tier which is determined through an objective Complexity and Risk assessment conducted by the project team and validated by the EPMO. Any future major project related activity for CHESS would be managed through this process and aligned to the ASX Scaled Project Management Framework and ASX Delivery Framework.

### **Business Analysis**

Frameworks and processes for capturing and translating the requirements throughout the delivery lifecycle.

### **Solution Engineering**

Solution architecture, solution engineering, solution design, frameworks, and processes to deliver working code that meets the requirements specified by the business analysts.

### **Quality Engineering and Testing**

Testing frameworks and enabling capabilities for quality engineering and testing to ensure business requirements are being met. The framework sets the standard and provides the means for quality to be proactively managed and embedded throughout the delivery of projects.

### **Organisational Change Management**

Framework and processes by which organisational change management is executed throughout the delivery lifecycle.

## Project Delivery Assurance

For further information on ASX Project Delivery Assurance Framework (PDAf), refer to Section 8.3 Controls Monitoring.

## Delivery Governance

The ASX Delivery Governance model is a structure of relationships and processes that provides guidance for monitoring, decision making and escalation to enable Projects / Portfolios to achieve their planned outcomes. Some of the groups below are in addition to the mandatory requirements set out in the ASX delivery governance model e.g., S&P leadership team. These are listed below to provide a comprehensive view of CHES related delivery governance.

### 8.1.3.1.2 Portfolio Governance Group

Change initiative delivery is governed by the PGG. This is a governance group chaired by the CCOO with membership consisting of Executive Management members, and senior leaders with responsibility for delivery. This governance body is charged with overseeing the commencement and execution of priorities endorsed by the ASX Executive Management via the strategic planning process and in-line with the Board approved budget. The PGG provides the approval mechanism for the release of funds and commitment of resources for Executive Management agreed priorities, and acts as the escalation point for the line of business portfolios in relation to these.

Decisions are reached by broad consensus within the delegated authority from the Managing Director and Chief Executive Officer. There is no right to vote by any member. Where approvals exceed delegated authority (as set out in Finance Policy), this group will make recommendations to the ASX Board as required.

The primary function of the PGG is to discharge the responsibilities as set out below:

- Approve the commencement of new projects through the authorisation of funds and resources.
- Review and consider validity of Change Requests in the context of delivering benefits required to achieve objectives.
- Consider and take action for early termination of projects that can no longer deliver expected benefits.
- Monitor the health and progression of projects and program through to and including benefits realisation.
- Monitor group project spend, both Capital Expenditure (Capex) and Operating Expenditure (Opex), ensuring alignment to group targets.
- Monitor project and portfolio resourcing at a group level.
- Resolve issues and agree mitigation options for risks escalated through from the Line of Business Portfolios or those that impact enterprise wide.
- Endorse and provide feedback on material changes to the delivery frameworks and ways of working as they relate to projects.
- Approve requests to draw down on project contingencies.

All CHES related projects are governed by the PGG.

#### 8.1.3.1.3 Architecture and Design Authority

ASX aligns to TOGAF<sup>4</sup> as the enterprise architecture framework for CHES (as with all architecture at the ASX), and operates under a two-tier governance model:

- Design Authority.
- Architecture Community Meeting.

#### 8.1.3.1.4 Design Authority (DA)

The DA focuses on technology strategy and architecture. DA must approve technology solution designs with a focus on managing the high-level design concept and its ability to meet business goals, needs, and specifications relative to the EA Roadmap (Enterprise and Line-of-Business).

The Design Authority meets at least monthly and is the highest level of architectural governance at the ASX. It comprises the CTO (Chair), CIO, CCOO, Head of Enterprise Architecture, as well as various General Managers across the technology domain including the CISO. The Design Authority ensures that technology decisions are aligned with the ASX technology strategy, architecture, process and data design principles, and business strategies. Qualifying architecture to CHES are passed through this governance forum according to the terms of reference of this forum and the ASX delivery framework.

#### 8.1.3.1.5 Architecture Community Meeting

The Architectural Community Meeting meets weekly and is a forum that reviews, agrees, and approves architectural solutions, technology initiatives, and innovations that are presented as a precursor to the Design Authority. It is chaired by the Head of Enterprise Architecture who is solely responsible for any recommendations made by the Architectural Committee Meeting. For architecture decisions around extending existing capability, decisions have been delegated from the Design Authority to the Architecture Community. Qualifying architecture changes to CHES are passed through this governance forum according to the terms of reference of this forum and the ASX delivery framework.

---

<sup>4</sup> The Open Group Architecture Framework (TOGAF) is an industry framework used for enterprise architecture, that provides an approach or designing, planning, implementing and governing an enterprise information technology architecture.

### 8.1.3.2 Securities and Payments Governance

The S&P Governance structure connects with governing bodies at both the Enterprise and the CHES program level. It is responsible for S&P related governance for both BAU and projects and ensuring that directives and guidance provided by the Enterprise PGG flow through to the relevant BAU and Project related committees and forums.

The S&P business is responsible for ensuring the appropriate levels of governance and operational delivery capability is in place for the ongoing monitoring and management of risk to the performance of CHES.

#### 8.1.3.2.1 S&P Senior Leadership Team (SLT)

The S&P SLT is the management forum that meet on a weekly basis to update the S&P leaders on CHES related opportunities, risks, stakeholder insights and general business updates across finance, HR, and risk.

#### 8.1.3.2.2 Portfolio Working Group

The PWG's are currently in place for every portfolio in the business division (e.g., S&P, the portfolio of which CHES is a component) and are senior management governance groups, occurring each month and chaired by each portfolio executive sponsor. They are in place for both 'running the business' (BAU) or 'changing the business' (projects) set per the strategic plan endorsed by the Executive Management.

The purpose of each PWG is to provide direction and oversight as agreed in the annual strategic planning cycle, governance of initiatives in scope to ensure strategy, objectives and benefits are aligned and achieved, consider resourcing and capacity, sequencing and prioritisation within the portfolio, act escalation point for projects in the portfolio and a gate through to PGG.

The PWG connects with the ASX Enterprise PGG at the Enterprise level for strategic alignment, BAU and project related governance and at both the SGG and Program Working Group level (where they exist) for programs of work such as the CHES Roadmap.

In relation to CHES specifically this governance body is responsible for providing the direction and oversight for the CHES Roadmap, including strategies for managing risk to the ongoing performance of CHES.

#### 8.1.3.2.3 S&P Risk Working Group

The S&P RWG focuses on risks, controls, KRIs and actions relating to:

- S&P Operations and Technology, Business Management & Planning and Product & Client Relationships, Equity Post Trade, Debt & Collateral, Payments and Issuer Services

- operational processes and systems and projects owned by the S&P business

The Chair of the S&P RWG is the Group Executive, S&P. The General Managers (GMs) reporting to the Group Executive S&P own the risks relating to their areas of responsibility and are members of the S&P RWG.

Relevant elements and/or outcomes of the RWG are escalated as necessary and/or consolidated into formal risk reporting to Risk Committee, ARC and/or Board as appropriate.

In relation to CHES specifically this governance body is responsible for the oversight of the CHES Roadmap, including managing the risks related to the ongoing performance of CHES.

#### 8.1.3.2.4 S&P Front Door Process

An S&P Front Door Process has been defined to initiate work. (For further details, refer to *Section 5.2 Product Management*)

#### 8.1.3.3 CHES Roadmap Governance

The CHES Roadmap is supported by a governance structure with program level governance and oversight, program delivery, change management and risk management. Underpinning this structure is a focus on the monitoring and management of any risks to the performance of CHES, which in turn is then managed by the Performance and Operations layer of capability supported by the Oversight and the Management committees.

##### 8.1.3.3.1 Strategic Guidance Group

The SGG is the Executive/Senior Leader Group chaired by the Program sponsor with the core purpose of providing ongoing direction for the program. It provides a forum to escalate risks that may impact the successful delivery of the program outcomes and ensure outcomes stay aligned to achieving the program objectives. Delivery risk is underpinned by ASX's project risk management framework and the day-to-day execution management by project teams. There is a SGG in place to govern CHES related projects.

ASX governance is based on the allocation of a Tier to a project, which is determined through an objective complexity and risk assessment conducted by the project team and validated by the EPMO. At the execution level there are two classes of governance groups that may be employed to oversee and guide a project or program.

- All Tier 1 and/or high-risk projects (as determined by the outcomes of the Complexity, Project Risk Assessment and Tier Allocation Process) require an SGG to be established. Where a program exists, the SGG will reside at the program level rather than the individual projects within the program.
- A project that has a vendor delivering a major component of the project requires a Joint Steering Group (JSG) to be established.

- A project that has a major external sponsor or contributing external party should also consider a JSG.
- All other projects will generally be governed via the project team organisation structure (as per the roles and responsibilities of the Sponsor and Owner), reporting into a business division Portfolio.

All Tier 1 project artefacts (incl. CHES related projects), such as business cases and Change Requests (**CRs**) must be endorsed by the SGG and the S&P PWG before being submitted for approval by PGG.

#### 8.1.3.3.2 Program Working Group (PgWG)

The CHES Roadmap is governed by the SGG and delivered and managed through the PgWG. Chaired by the Program Manager meeting on a weekly basis the PgWG consists of Project/Delivery/Stream Leads, Product Owner, Operations Leadership, Leadership from impacted systems, Business Analysis, Architecture, Engineering, Testing Leadership and Security, and Risk & Assurance.

This working group oversees the delivery and governance of all CHES related activity which includes:

- Program Status Reporting.
- RAID Management.
- Scope Management.
- Schedule Management.
- Resourcing and Budget Management.
- Escalation Management.
- Vendor Management.
- Delivery Process Governance.

#### 8.1.4 Performance and Operations

The operational delivery of the ongoing monitoring and management of risks to the performance of CHES is summarised in the Performance and Operations layer. This layer oversees the availability of services and the underpinning adequacy of financial resources, technological resources, and the human capital (including external parties).

Performance and Operations is governed by the following two pillars:

1. The Technology and Data division is responsible for the ongoing monitoring and management of risks relating to the underlying infrastructure which is utilised by CHES and the design and build services relating to CHES. This capability is delivered through four key pillars – Data centres, Workplace Technology, Network Services and Hosting, which are in turn underpinned by a number of external vendors supporting CHES.
2. The S&P Business division is the sponsor for the CHES CS solution, delivering safe, secure, and resilient infrastructure to Australia’s financial markets. The S&P Technology and S&P Operations teams are responsible for the technical support and maintenance of CHES and associated projects.

#### **8.1.4.1 Technology and Data**

The Technology and Data pillar within the Performance and Operations layer is responsible for supporting the Security, Architecture, and underlying infrastructure for CHES. The Technology and Data team provides design and build services to trusted and innovative technology platforms, and comprises four pillars: Data centres, Workplace Technology, Network Services and Hosting.

Underpinning these capabilities are a range of enablers covering technology governance and risk, Centres of Excellence, and technology pillar specific expertise.

##### **8.1.4.1.1 ASX Technology Leadership Team**

The ASX Technology Leadership Team holds a fortnightly meeting comprising the ASX Technology General Managers, CTO, CIO, General Manager Infrastructure and General Manager Technology Security and Governance. In addition, the Senior Manager, Tech and Data Risk Management and the Heads of Enterprise Architecture, Quality Engineering and Testing and Engineering usually attend.

It is a forum where discussion of emerging technology risks, as well as list of approvals of changes to systems, and systems risk assessment processes occurs. CHES is not discussed as a regular agenda item within this meeting and would only be discussed if there is a specific emerging risk or a CHES related project. Note that this meeting is currently weekly due to the volume of activity occurring across ASX.

#### **8.1.4.2 Securities and Payments**

As the sponsoring business for CHES, S&P is ultimately responsible for the ongoing monitoring and management of risks to the performance of CHES, the availability of services and the underpinning adequacy of financial resources, technological resources, and the human capital.

##### **8.1.4.2.1 CHES Business, Technology and Operations**

Financials, resourcing, technology, and availability of CHES related services (including those that are outsourced and managed through third parties) are reviewed with appropriate controls applied through the remit of each delivery arm.

Within S&P, primary oversight of CHES from a technical and operational standpoint falls under the responsibility of the General Manager S&P Technology, General Manager S&P Operations and General Manager S&P Business.



- **General Manager S&P Technology** – Responsible for the technical support of CHES across Application Support, Software Engineering and Testing.
- **General Manager S&P Operations** – Responsible for the operations and non-technical support of CHES, as well as the management of CHES users (e.g., participants, share registries, and others) and issuer/financial product lifecycle management.
- **General Manager S&P Equity Post Trade and Payments (Business)** – Responsible for the strategy and service development and execution. They are responsible for the ongoing monitoring and management of risk to the performance of CHES. This includes the adequacy of technological, financial, and human capital resources.

The following sections outline the management structures and underpinning practices utilised to meet these responsibilities.

#### 8.1.4.2.2 Ongoing Monitoring and Management of Risks to the Performance of CHES

The ongoing monitoring and management of risks to the performance of CHES and availability of services is summarised through the following key Performance and Operations capabilities:

- Technology Performance Reporting, including Service Management Reporting.
- Inflight and BAU Reporting.

#### Technology Performance Reporting

The S&P Technology team has in place reporting via the ASX ITSM platform to report upon KPIs and associated metrics across the service management framework. The Senior Manager ITSM and BCP Change Manager are responsible for collecting and reporting upon ITSM data, these are then consolidated into the Technology Summary Performance dashboard which covers the following:

- ITSM Performance.
- Capacity reporting.
- Open Risk items.
- Open Audit items.
- Resource Pipeline.
- Current Upgrades.
- Upcoming Upgrade Projects.
- Future Projects.

As outlined in the Technology Performance Summary report, ASX utilises a range of KPIs to monitor the ongoing performance of CHES. The majority of KPIs are associated with Capacity which utilises several measures of capacity (e.g., rolling monthly, three monthly, 24 monthly), total available capacity measures (the headroom to full capacity) is then assessed.

The key areas monitored, measured, and managed through the Technology Performance reporting are as follows:

- **Availability of Services** – ASX use the Service Availability Reporting (SAR) process to record and report on CHES availability metrics and inform regulators such as ASIC and RBA on the availability of market facing services.
- **Capacity Planning** – ASX Capacity management for CHES is the process to manage trade volumes to accommodate current and future demands.
- **Change Management** – The S&P Change Initiation and Triage process is used to initiate all changes; changes are then tracked in the ASX Project Management tool and managed through the weekly CAB. These changes are reported on to the CAB and as part of the Technology Performance summary report.
- **Incident Management** – Incidents are reported via dashboards in the ASX ITSM platform and are available on-demand. Incident data is also reported via the ‘Technology Performance Summary Dashboard’ that shows incidents for the current calendar year with status per quarter, and incident trends showing annual peaks, and averages

### In-flight and BAU Reporting

In addition to the Technology Summary Performance Dashboard, there are various reports that are produced within the ASX for the reporting of BAU (both technology and operations) and change initiatives for Enterprise and Board oversight. This level of reporting is collated manually from various sources to provide a centralised views of the CHES Program and other BAU initiatives, S&P Portfolio level data, as well as information of interest to the ASX Board and Sub-committees.

### CHES Support Model

CHES is used by both internal and external users. To ensure its continued availability, it is supported by a matrix of internal and external service support teams and a CHES Service desk which is available to external CHES users to provide tiered levels of support:

- **1st level support** – performs support for basic customer issues such as solving usage problems and fulfilling service desk request that require IT involvement.
- **2nd level support** – performs technical support; incident diagnostic and resolution for both incidents and problem management. Deploys changes to production.

- **3rd level support** – develops changes to the CHES software according to the nature and requirements of a business request. Assists 2nd level support in incident and problem management.

#### 8.1.4.2.3 Financial Adequacy

As a critical asset the financial support requirement of CHES, outside of any future major upgrade, are well defined and included in the annual Capital Expenditure (**CAPEX**) and Operating expenditure (**Opex**) budgets. Capex and Opex budgets are determined in accordance with the five-year plan, which is then re-baselined and re-prioritised each year, and includes a capital buffer at both the ASX entity and ASX Group level for any unforeseen operational business risk. Through the period of the CHES Replacement Project, the financial support was focused on maintaining the operational performance of CHES within predefined system tolerances, critical system upgrades and supporting important regulatory/business imperatives, as required during this period.

With the recent decision to pause the CHES Replacement Project, management have commenced reviewing CHES to identify and implement necessary upgrades required to ensure the functionality, infrastructure and support is in place through to 2032. This activity is still in progress including the assessment of technological risk stage gates and forecasted Capex for required software and infrastructure upgrades. Required upgrade costs will be prioritised and approved through ASX's existing financial budgeting processes.

Outside of extraordinary events such as the impact of pausing of the CHES Replacement Project, ASX's annual budgeting process involves ASX business owners preparing a base budget that forecasts for the following financial year. Annual budgets and proposed initiatives are discussed and agreed between the Executive Management based on priority (aged assets and regulatory projects take priority).

As a listed entity, the ASX provides market guidance on Capex for the future year, with ASX publishing details of in-flight as well as new initiatives. If additional Capex is required, then the Capex guidance will be adjusted accordingly.

Change requests for project funding may occur and are reviewed and approved on an as required basis. Post Executive Management approval, the annual budget for Capex is provided to the Board for its approval.

The forecasted cost of running CHES is encapsulated within the internal governance arrangements, such as the PWG and ASX Enterprise PGG and the associated strategic priorities and investment planning activities they contain. The CHES program is currently being planned at the Project level and as such costs are not yet consolidated at the program level. Funding for the delivery of CHES program, including the longer-term CHES Roadmap, will be addressed through existing approval mechanisms (e.g., change requests, budgetary cycle).

#### 8.1.4.2.4 Technology Adequacy

CHES is stable, fully supported, meeting market demands and assessed as being able to process up to 10 million trades per day and assessed as having sufficient headroom to accommodate current projected future growth. With the pausing of the CHES Replacement Project there is the requirement to

continue to update the CHES IT Assets to ensure CHES continues to be stable, secure, fully supported and meeting required levels of forecasted support and capacity. Work in this area is underway as part of the CHES Roadmap, a summary of which is provided below.

The CHES Roadmap outlines the upgrades required to extend support and increase capacity, there are several stage gates which will require the assessment of technical delivery risk and technology related investment uplifting IT Assets. (For further details on the initiatives planned, refer to *Section 9 Detailed Roadmap*)

#### 8.1.4.2.5 IT Asset Upgrades

(For further details on IT Assets related to CHES, refer to *Section 5.4 IT Asset Management*)

As per the CHES Roadmap the obsolescence of the core technology stack [REDACTED] is being managed through a series of planned upgrades.

The capacity of the current stack has been tested up to 10 million trades. Further testing will be performed in 2023 to test the maximum volume of trades CHES can process before performance degradation, to understand peak capacity, forecast processing time required and assess any impacts on next day opening times.

#### 8.1.4.2.6 Extended Support and Run

The current available upgrade paths provide support through to 2025 at a minimum, and in some instances through to 2030. These dates will potentially extend further as new upgrade paths are announced by the external service providers. Software and hardware providers typically provide full support over a three-four-year period and then extension options with reduced levels of support removing elements such as vulnerability testing. Typically, providers only release its planned upgrades one to two years in advance, reducing the ability to forecast upgrades that have not yet been announced.

#### 8.1.4.2.7 Extension and Risk Acceptance

The end of extension support, and the associated risks, risk assessment and mitigation will be assessed by ASX at key check points, as outlined in the CHES IT Asset plan.

#### 8.1.4.2.8 Human Resource Adequacy

Based on known work, proposed human capital investment for CHES support is expected to be in line with current capacity requirements. Key technological changes to the system will have flow through impacts to the cost of development resources and factored into the budgeting process when key change decisions are made.



[Redacted content]

Current and Planned Initiatives	Status of Initiatives	Theme	Indicative Date
No additional initiatives identified (Related initiatives are in other sections).			

## 8.2 Operating Model – Resources and Vendor Support

<p><b>ASIC Requirement</b></p> <p>Governance d (ii)</p> <p>Operations a (vi)</p> <p>Operations a (vii)</p>	<p><b>Objective</b></p> <p>How the Licensee will ensure it has the requisite skills and capabilities (including, where necessary, external parties) for the operational maintenance and support arrangements for CHES and for continued performance and operation of CHES and availability of its services until the Go-Live date of the CHES Replacement System.</p> <p>Detail the Licensee’s management program (including monitoring and performance management) for any outsourced services essential to the operation of CHES and availability of its services, including all risks to resilience, reliability, integrity and security.</p> <p>Identify internal and external support requirements, in terms of resourcing and extendable/upgradeable vendor contracts.</p>
--	--

To ensure that ASX has the requisite skills and capabilities for the continued performance and operation of CHES and the availability of its services, ASX has in place a range of practices to forecast and align resources. This includes resourcing categorisation and forecast utilisation, capacity assessment, and tracking the availability of required skills within ASX in the event of a high priority and urgent request or incident for relevant systems.

These practices inform the internal operational structure, the identification of any gaps, and inform the external support requirements, ensuring ASX has the required levels of human capital.

Specifically, CHES is primarily supported using internal resources, and the critical skills are related to the CHES programming languages and operating system skills.

[REDACTED] The current human capital coverage the ASX has in place for CHES provides the required level of coverage within its current operating parameters.

### 8.2.1 Operational Structure

CHESS is an in-house developed application supported by internal ASX teams including S&P Technology, S&P Operations and Technology & Data. The S&P Operations and Technical teams have extensive experience and frameworks, practices, and policies to support its business and technology operations.

The General Manager of S&P Technology has responsibility for business-as-usual technical support and the maintenance of CHESS as well as projects (via the engineering and testing teams) and is supported by the Senior Manager for Application Support, Software Engineering Manager, Test Manager, and its respective teams.

The S&P Technology team interfaces internally with the S&P Operations team and the broader business. Senior members of the Technology team (e.g., General Manager S&P Technology) also attend operations meetings with external stakeholders such as the RBA.

This structure is aligned with the skills and capabilities required to support the operational maintenance and support of CHESS until the go-live date of the CHESS Replacement System.

#### 8.2.1.1 Internal Resourcing

ASX has a structured set of processes and governance structures in place to forecast the investment required in Human Capital to ensure the ongoing maintenance and support of CHESS. This is underpinned by a set of processes and practices to forecast resourcing needs based on the skills, capabilities and capacity required.

Resourcing is determined by comparing to prior year baselines and adjusting. Resourcing to support CHESS has been considered for the next one to two years and will be revisited on an ongoing basis. Emergent risks are also considered, and a process is in place to address these in relation to the capacity of the service desk and other support for CHESS and to ensure that all activity is accounted for over this period. Any delivered risks are captured in the ASX Enterprise RMS to ensure ongoing monitoring and appropriate mitigations.

The current resource forecasting is focused on the delivery and support of CHESS within its current technology architecture and within the parameters of current functionality. This includes:

- Resource capacity for core business hours including the ability to support when factoring items such as leave entitlements projected out for the year.
- The resource skills to support CHESS have been established with ASX staff and its associated skills and skill grading recorded so that these can be mapped to what is required to support CHESS and identify if there are any resourcing gaps.
- On call coverage and weekend support to support CHESS are under consideration.
- The support team prioritises any CHESS incidents over project work to ensure that CHESS operations are fully supported. If any resources are working on projects when an incident occurs, those resources will stop work on projects and switch to resolving incidents until resolved.



A resourcing skills matrix has been defined for the roles supporting CHES to enable an analysis of the required skills to support CHES.

The ASX Systems key support matrix is used to monitor and forecast the capacity required to support each of the ASX systems, the databases, and the infrastructure. Its purpose is to monitor skills availability and identify any gaps based on:

- The availability of required skills within ASX in the event of high priority and urgent requests or incidents for relevant systems, and
- The availability of required skills for ongoing maintenance and development of the relevant systems.

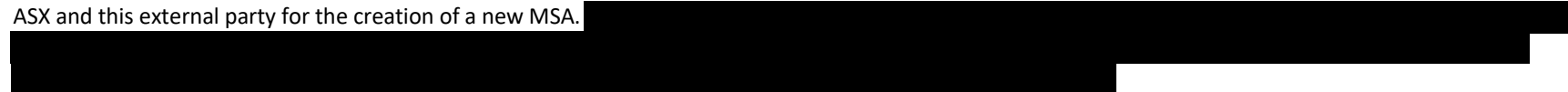
Within these parameters, the current human capital coverage the ASX has in place for CHES provides the required level of coverage within its current form.

This does not however provision for the human capital requirements of new functionality or major upgrades (hardware and software), these would need to be accounted for at the time of planning.

**8.2.1.2 External Parties**

ASX applies its *Vendor Management Framework* which defines the minimum standards and accountabilities applicable for managing Vendors and Partners. It is aligned to the ASX Procurement Principles designed to enable and support the ASX business to undertake appropriate procurement while ensuring the proper controls and risk management are in place.

The majority of internal capabilities supporting CHES reside within ASX. The external capabilities are leveraged through services, tools and licenses across operating system, database, monitoring tools, hardware, storage, and infrastructure. ASX currently has a key external partner who is contracted under an existing MSA to provide operating system support and to assist in resolving software defects and incidents. Discussions are currently underway between the ASX and this external party for the creation of a new MSA.



Current and Planned Initiatives	Status of Initiatives	Theme	Indicative Date
No additional initiatives identified (Related initiatives are in other sections).			



### 8.3 Controls Monitoring

ASIC Requirement	Governance d (iii)	Objective	
			What system of controls and monitoring the Licensee has in place to measure, assess and continuously improve and assure the ongoing resilience, reliability, integrity and security of CHES.

ASX has adopted a layered approach to controls and monitoring. At each level within the Three Lines of Defence, there are various assessments and activities that are undertaken to measure, assess and continually improve and assure the ongoing resilience, reliability, integrity, and security of CHES.

#### 8.3.1 Line 1 Controls Monitoring

ASX has implemented a set of 171 controls (Operation - 72, Security - 41, Resiliency - 10, and Governance – 48) in order to actively manage risks related integrity, resilience, reliability, and security of CHES. A summary of those controls against each risk is included in Appendix B – CHES Risks.

Where a control gap or deficiency exists, these are defined as “issues” and managed in line with ASX’s Risk Issue Management Framework. Risk issue management facilitates Line 1 risk ownership and accountability through self-identification and remediation of operational risk issues. All issues must be linked to one or more risks (in the ERM system), and one or more associated control improvement action plans unless accepted.

Once the control gap or deficiency has been addressed by closure of the issue, reassessment of the control environment and the residual risk is performed. All risks, controls, issues, and action plans are maintained and monitored within the ERM system, and action plans are then tracked in the various RWGs and through relevant governance forums. (For further details on governance forums and monitoring, refer to *Section 5.1 Risk Identification and Assessment / Management and Monitoring*)

Line 1 conducts the following activities as part of its control monitoring.

##### 8.3.1.1 Controls Self-Assessment

Currently, self-assessment of controls is performed as part of the formal company-wide annual RSA process, as well as on an ad-hoc basis, and/or when there is a material change to the process, risk, or control environment.

A formal control testing framework is scheduled for rollout across ASX in the latter half of the calendar year 2023. This will focus on key controls and will support the assurance of key control design and effectiveness as they relate to both CHES and broader enterprise-wide risks.

### 8.3.1.2 Security Audits

ASX is subject to several regulatory driven and external technology and security focused audits/reviews that assist in providing assurance on technology/security controls and in identifying areas that need improvement. In addition, security risks are considered every six months as part of the CHES risk assessment process. Such risk assessments are conducted at least every six-months and/or as required based on changes to the environment. These assessments assist in identifying control risks, non-compliances, and/or exceptions for consideration. Risks identified through these external or internal exercises are recorded in the ERM system and are tracked for risk mitigation in accordance with the ERM framework.

The PDAf forms part of the ASX Delivery Framework and aims to provide an independent and objective assessment of change initiatives. It is risk based, outcome focused and facilitates effective and continuous communication with the Executive Management, Program Sponsor, Executive Leadership team, Delivery teams, and key stakeholders about the health of the Program and/or Project. The PDAf helps ensure that sufficient governance and controls are in place, it identifies and highlights risks and makes recommendations to be actioned, it also supports continuous improvement and effective decision-making.

Project delivery assurance activities are tailored to the complexity, risk and size of the project or program. The PDAf covers the CHES Roadmap.

### 8.3.1.3 Line 2 Challenge

One of the key objectives of Line 2 is to continue to improve the effectiveness of ASX's control environment (i.e., minimise control failure), support assurance that business is being performed in accordance with risk appetite, and to enable effective risk-based decisions. Enterprise Risk acts in a Line 2 oversight role to provide independent advice and to review and challenge the risk management and decision-making management activities of Line 1. Factors that support and enable Line 2 challenges include, but are not limited to:

- ERM review and challenge of the Line 1 risk profile, i.e., risks, key controls, issues, action plans, with provision of Line 2 review/commentary for risk self-assessment purposes.
- Active participation at Line 1 RWGs, with a focus on review/challenge of risks above target, emerging risks, organisational KRI results (including remediation), and control improvement action plans.
- All Tier 1 projects are required to engage Line 2 to support appropriate project management activities through reviewing and challenging risks, issues, assumptions, and dependencies and ensuring delivered risks are appropriately managed and transitioned into the business after a project has been delivered.

The activities above would include consideration of any risks and controls relevant to the CHES operating environment.

Line 2 also provide an objective assessment of ASX's overall risk posture against risk appetite through quarterly CRO Risk reporting to the Risk Committee and the ARC which includes assessment against seven key risk categories, underpinned by the results of 30 Board level KRIs.

#### **8.3.1.4 Line 3 Assurance**

The third line of defence provides the independent assurance and assessment of the effectiveness of activities undertaken by Line 1 and Line 2.

#### **8.3.1.5 Framework Audits**

The system of internal control and risk management across the organisation is reviewed by ASX's Internal Auditors. The General Manager Internal Audit has a direct reporting line to the Chair of ARC in relation to the performance of the functions of Internal Audit, and to the CFO for administrative purposes. The General Manager Internal Audit presents an Internal Audit Plan and quarterly audit findings to the ARC.

#### **8.3.1.6 ASAE 3402 Assurance**

ASX engages external auditors (PWC) to provide an annual ASAE 3402 Assurance Report on Controls at a Service Organisation for CHES for the financial period, which covers the following control objectives:

- 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.
- Controls provide reasonable assurance that all changes relating to the application software, operating system software and underlying databases within the CHES production environment are authorised, tested, and managed appropriately.
- Controls provide reasonable assurance that prevents unauthorised access to the ASX primary data centre and ASX-controlled areas in the secondary data centre.
- Controls provide reasonable assurance that in the event of a disaster, measures are in place to enable CHES to resume effective operations within two hours.
- Controls provide reasonable assurance that CHES is backed up, and system processing and performance is monitored.
- Controls provide reasonable assurance that environmentally controlled data centres exist to facilitate continuity of data processing operations.

- Controls provide reasonable assurance that the process of daily settlement is complete and accurate.
- Controls provide reasonable assurance that the securities holdings recorded and maintained by CHESSE are complete and accurate.
- Controls provide reasonable assurance that transactions submitted to CHESSE by ASXS, participants or registries are processed completely and accurately.

No exceptions were identified in the preceding financial period 1 July 2021 – 30 June 2022.

Current and Planned Initiatives	Status of Initiatives	Theme	Indicative Date
No additional initiatives identified (Related initiatives are in other sections).			

## 9 Detailed Roadmap

The table below details the CHES Roadmap which contains the 27 key initiatives across four themes from the ASIC requirements: Operation (16 initiatives), Security (six initiatives), Continuity (five initiatives) and Governance (initiatives delivered through BAU activities).

**Table 9.A Key Initiatives in CHES Roadmap**

Pillar	ID	Status	Indicative Date	Initiative Name	Description
Operations	O-1	In Progress	Sep 23	Develop a new model for forecasting future trading growth	Initiative to develop a new model to forecast future trade growth that would consider underlying drivers of volume increase based on historical experience of events such as market structure changes, major corporate action events, and unplanned/outlier events such as the COVID-19 pandemic.
Operations	O-2	Planned	Dec 23	Improve maturity level of the Availability and Capacity Management Framework and processes based on COBIT	Establish an enterprise 'Availability and Capacity Management Framework' to align with COBIT. Includes Availability Management, Business Capacity Management, Service Capacity Management and Component Capacity Management across Critical services that S&P will then imbed for CHES.
Operations	O-3	Planned	Dec 23	Stress test CHES to determine further points of failure	Perform CHES stress test to determine further points of failure.
Operations	O-4	Planned	Mar 25 (Phase 1)	Capacity & Performance Improvements	Remediate short-term points of failure and assess options for further performance improvements to address the outcomes of the CHES stress test and develop a plan for remediation.
Operations	O-5	In Progress	Jun 23	Establish a Managed Service Contract agreement	
Operations	O-6	In Progress	Jun 23	Front-end – OS and Hardware upgrade	Upgrade of the CHES front-end hardware and operating system to the latest version. The initiative will ensure continued vendor support key to the operational resiliency of future CHES operations. <i>(Inflight Initiative)</i>
Operations	O-7	In Progress	Sep 23	CHES Access upgrade	

Pillar	ID	Status	Indicative Date	Initiative Name	Description
Operations	O-8	Planned	Jun 24	[REDACTED]	[REDACTED]
Operations	O-9 & O-10	Planned	Jan 24 (Phase 1 – O-9) June 24 (Phase 2 – O-10)	Address CORE dependencies: Reference Data (Batch) & Trade Data (Real time)	Address CHES dependency on CORE by migrating off CORE to new CORE replacement platform that has been currently tested to 15 million trades per day.
Operations	O-11	Planned	Mar 24	Monitoring application upgrades	Upgrade CHES and CORE monitoring application to be on the latest hardware and latest version. <i>(Planned Initiative)</i>
Operations	O-12	Planned	Dec 26	Backend upgrades	[REDACTED]
Operations	O-13	Planned	Jul 24	Backend upgrades	[REDACTED]
Operations	O-14	Planned	Jun 24	Assess alternative hardware architecture for backend servers to support CHES	Assess alternative hardware architecture to support CHES. The initiative will be a driver for the future CHES server hardware upgrades.
Operations	O-15	In Progress	Jun 23 (Phase 1)	Customer VPN Access	Customer Site VPN software is required to be upgraded to maintain ongoing support arrangements by the customer. <i>(Inflight initiative)</i>
Operations	O-16	In Progress	Nov 23	HSM Device upgrades	Upgrade the CHES hardware security modules, critical to the secure operation of CHES, to the latest hardware. <i>(Inflight Initiative)</i>
Continuity	C-1	Planned	Jul 24	Review CHES resilience scenario testing	Further analysis will be performed to support an end to end view of the CHES operating environment. This will support completion of a stocktake of current resilience testing activities against plausible disruptions scenarios. Any identified gaps will be risk assessed and an appropriate approach formed to



Pillar	ID	Status	Indicative Date	Initiative Name	Description
					enable testing of scenarios. A test program will be created that details the outcomes of the stocktake, plausible scenarios, detailed approach to ongoing testing and reporting requirements.
Continuity	C-2	Planned	Dec 23	[REDACTED]	[REDACTED]
Continuity	C-3	Planned	Dec 23	[REDACTED]	[REDACTED]
Continuity	C-4	Planned	Mar 24	CHESS - Review backup and restore processes	Review CHESS backup and restore processes as these pertain to the Business Continuity and Security Standards for RITS Members - December 2022.
Continuity	C-5	Planned	Mar 24	CORE - Review the backup and restore processes	Review the CHESS Signal Feeds (presently delivered by CORE) backup and restore processes as these pertain to the Business Continuity and Security Standards for RITS Members - December 2022.
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

Pillar	ID	Status	Indicative Date	Initiative Name	Description
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]



## Appendices

### Appendix A – Introduction to ASX and CHES

#### Introduction to Australian Securities Exchange (ASX)

ASX is an integrated exchange that offers listings, trading, clearing, settlement, technical and information services, technology, data, and other post-trade services.

ASX also acts as an AMO, clearing house and payments system facilitator. It oversees compliance with its operating rules, promotes standards of corporate governance among Australia’s listed companies and provides education to retail investors.

ASX operates markets for a wide range of asset classes including equities, fixed income, and commodities. As an integrated exchange, ASX’s activities span primary, secondary and derivative market services, including the raising, allocation and hedging of capital flows; trading and price discovery; counterparty risk management; and securities settlement for both the equities and fixed income markets.

ASX Limited (the parent entity of the ASX group) is a listed company, the first exchange in the world to demutualise and directly list on its own market on 14 October 1998. ASX was created by the merger of the Australian Stock Exchange and the Sydney Futures Exchange in July 2006 and is one of the world’s top 20 listed exchange groups measured by market capitalisation.



Figure Appendix A.A ASX Group Structure Relevant to CHES



**Figure Appendix A.B ASX Business and Support Divisions**

ASX's business is structured around four business divisions, each led by a Group Executive and supported by the Customer and Technology teams and enabling functions (such as Finance and Risk Management).

The S&P business division operates the licensed cash equities CS facilities, and the settlement and depository business for the wholesale debt market (Austraclear) and ASX Collateral. The operation of the cash equities CS facilities is supported by the Risk Management team, particularly Clearing Risk utilising a number of RMS that interact with CHES.

CS services are critical to the operation of Australia's financial markets. The CS services provided by ASX help reduce counterparty and systemic risk and provide transaction efficiency and certainty for end investors.

Backed by significant capital and collateral, and overseen by Australian regulators, ASX's CS infrastructure supports the world-class reputation of Australia's financial markets.

### Regulatory Environment for CS Facility Licenses

ASX Clear and ASX Settlement operate licensed CS facilities under the Corporations Act, regulated by ASIC and the RBA.

CHES is the core system used to fulfil the CS functions of ASX Clear and ASX Settlement.

As CS facility licensees, ASX Clear and ASX Settlement must, to the extent that is reasonably practicable to do so, comply with the FSS and do all other things necessary to reduce systemic risk. In addition, they must:

- 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.
- Have adequate arrangements for supervising the facility, including arrangements for:
  - Handling conflicts between the commercial interests of the licensee and the need for the licensee to ensure that the facility's services are provided in a fair and effective way; and
- Enforcing compliance with the facility's operating rules.

- Have sufficient resources (including financial, technological and human resources) to operate the facility properly and for the required supervisory arrangements to be provided.

The Australian Securities and Investments Commission (ASIC) provides whole-of-market regulation across all trading venues and CS facilities.

Additional responsibility for policy setting for the Australian financial system lies with the Department of the Treasury and the APRA respectively. Together with ASIC and the RBA, these four bodies comprise the Council of Financial Regulators in Australia (CFR).

As the current sole licensed operators of CS facilities for the Australian cash equities market, ASX Clear and ASX Settlement are committed to providing CS services in accordance with the principles of stakeholder input to governance, transparent and non-discriminatory pricing, transparent and non-discriminatory access, and the protection of commercially sensitive information received from non-affiliated AMOs. The [ASX Cash Equities Clearing and Settlement Code of Practice](#) set out ASX's commitment to comply with the CFR's [Regulatory Expectations for the Conduct of Cash Equity Clearing and Settlement Services in Australia](#).

## Introduction to CHES

### What is CHES?

CHES is operated by ASX Clear and ASX Settlement as the relevant CS facility licensees.

Since its implementation 29 years ago, CHES has provided clearing, settlement, asset registration and other post-trade and issuer services essential to operating an effective cash equities market in Australia. To do this, a number of different types of market users (CHES users) interact with CHES each Business Day in accordance with prescribed technical, security, operating rules, and procedural requirements.

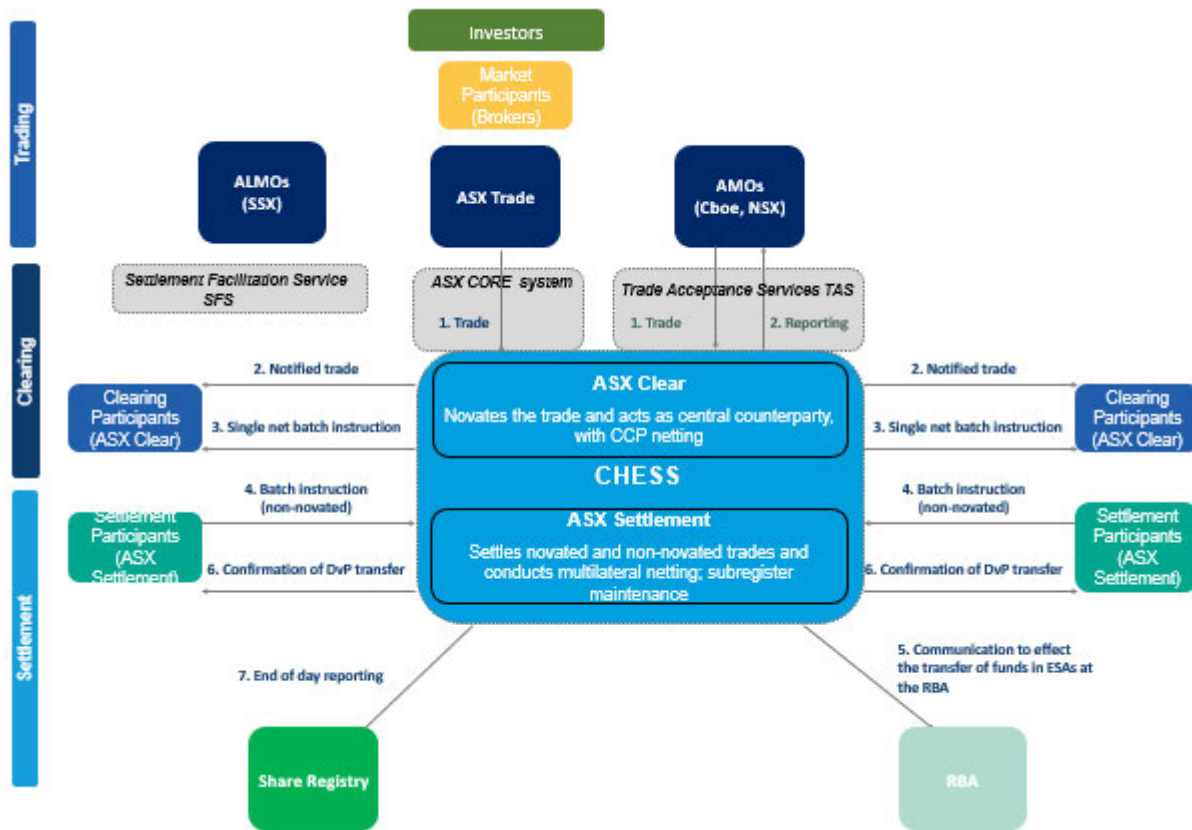
The market stakeholders or users that interact with CHES include:

- **AMOs** that facilitate market trade matching and the subsequent reporting of matched trades to CHES for clearing and settlement.
- **Participants** – the Clearing Participants and Settlement Participants such as brokers, custodians and institutions that make up the majority of CHES users and act on behalf of investors (i.e., sponsored holders) in CHES.
- **Issuer Share Registries** – the service providers appointed by Issuers to maintain the Issuer's register including operating the Issuer-Sponsored Subregister and interacting with the CHES Subregister on its behalf.
- **Payment Providers** – the banks authorised by Settlement Participants to make and receive payments on their behalf as part of the settlement process.
- **RITS** - is Australia's high-value settlement system and is used to affect the cash leg of CHES batch settlement.
- **Investors** – while investors are not direct users of CHES, their holdings are maintained on the CHES Subregister by their sponsoring participant (if CHES holdings) or for Issuer sponsored holdings are temporarily transferred to the CHES Subregister as part of the settlement process in CHES for market transactions by its broker. For CHES holdings, holders are provided with CHES holding and other statements or notifications when there are movements or other changes to that CHES holding or holder details.

Users that connect directly to CHES via secure connectivity channels, have pre-defined roles and permitted activities and communicate with CHES through CHES messaging.

### Role of CHES in CS Services

The diagram below shows the relationship between CHES in its operation of CS services and the CHES users. The key processes are numbered in the diagram and described below.



**Figure Appendix A.C Relationship between CHES and Australia's Cash Equities, Trading, Clearing and Settlement Services**

**The CHES Subregister and Maintenance of Holdings**

CHES provides a centralised electronic subregister (the CHES Subregister) for investor holdings of Approved Financial Products (each Issuer’s quoted and traded security classes, for example, ordinary shares). The subregister is set up in CHES before the commencement of trading for each Issuer, in liaison with the Issuer and its Share Registry, including details of the initial holders, if any.

Any investor that trades on market may have an account with a sponsoring broker who in turn creates an account in CHES for that investor in order to facilitate settlement and maintenance of its holdings and holder details. Each holder’s account is represented by a HIN and maintained as ‘name on register’ with direct ownership of the financial products. Investors benefit from the direct ownership structure through legal ownership and greater portability of its holdings, compared to the nominee model used in many other countries.

A separate Issuer-Sponsored Subregister is maintained by each Issuer’s Share Registry covering holdings that are not held in the CHES Subregister as well as an Issuer’s register which represents and aggregate of holdings on the Issuer-Sponsored Subregister and the CHES Subregister. As shown at point 7 on the diagram, Share Registries are provided with reports each day by CHES regarding any changes to CHES holdings as a result of settlement. Share Registries can also advise changes to investor holdings in CHES as a result of Issuer activity, such as the placement of additional securities to investors.

**Trades reported to CHES, Novation**

Three AMOs are currently approved to report trades to CHES for the purposes of clearing and settlement. The AMOs include ASX Limited (**ASX Trade**) reporting trades via the ASX CORE system, and Cboe and National Stock Exchange Pty

Limited (**NSX**) reporting trades using the TAS. The AMOs report on and off market trades executed on or reported to each of its own markets to CHESSE each Business Day – an activity is known as trade registration.

Once the trades are received and validated in CHESSE, the clearing of equity transactions is performed by the clearing house, ASX Clear, acting as a central counterparty for the trades. As the central counterparty, ASX Clear becomes the seller to every buyer and the buyer to every seller, becoming the counterparty assuming the credit risk and liable for completing all cleared transactions on the relevant market on a net basis. This occurs through a contractual process known as novation, in accordance with the operating rules of ASX Clear. ASX Clear, therefore, provides protection to non-defaulting Clearing Participants (and indirectly its clients) from a defaulting Clearing Participant who does not meet its obligations. ASX Clear is approved as a 'netting market' for the purposes of the Payment Systems and Netting Act. This enables the netting of settlement obligations in each individual security per participant, providing greater market efficiency at the time of settlement and reducing participant transaction and funding costs.

### Notified Trades and Netting

During the trade date (T) CHESSE will provide each Clearing Participant with notification of its novated trades (refer to point 2). Overnight on the trade date, each Clearing Participant will also receive the netted delivery and payment obligations across its novated trades which are to be settled in its capacity as a Settlement Participant, or if they have appointed another Settlement Participant to act as its settlement agent, by that Settlement Participant (refer point 3).

### Settlement

Two Business Days after the trade date (T+2) CHESSE affects the settlement of each trade. It does this by transferring the title or legal ownership of the securities in CHESSE while simultaneously facilitating the transfer of money in RITS for those securities between participants via its respective payment banks. This type of settlement is called Delivery versus Payment (**DvP**). It is irrevocable. CHESSE achieves DvP settlement through a Model 3<sup>5</sup> multilateral net batch settlement mechanism. This batch settlement completes at around 12.30 pm each Business Day. Multilateral net batch settlement involves the determination of each participant's net funds and security delivery obligations and the net funds obligations of all participants' payment providers. This maximises the efficiency of settlement by:

- Netting settlement obligations (buys and sells) in each individual security into one net buy or sell per participant.
- Netting all payment obligations (pays and receipts) into one net pay or receipt per payment provider (across the payment facilities it operates for participants).

Funds settlement (the transfer of money) occurs across the Exchange Settlement Accounts (**ESAs**) of those payment providers in the RBA RITS (refer to point 5). Once completed, this triggers the movement of securities from delivering to receiving Settlement Participants within CHESSE.

Batch settlement can also include scheduled bilateral DvP transactions that are conducted off exchange or for an AMO that does not use ASX Clear services (for example Sydney Stock Exchange Limited (**SSX**) that utilises the Settlement Facilitation Service). These transactions are not novated (refer to point 4).

CHESSE can also transfer the title (ownership) of securities on its Subregister on a demand basis (for example, free of payment), as instructed by participants.

Each Issuer's Share Registry will receive reports following batch settlement of any changes to holdings in CHESSE, so they can be updated in the Issuer's register (refer to point 7).

On any Business Day CHESSE performs three key activities in connection with the settlement of trades – registration and novation of trades executed that day, facilitating movements of securities in and onto CHESSE by participants and Share Registries (in the period from trade execution up until batch settlement) to support the settlement of trades, and

---

<sup>5</sup> Per settlement models defined by Committee on Payment and Settlement Systems of the Bank for International Settlements (BIS)

conducting batch settlement for trades executed two days ago, bilateral transactions giving effect to such trades and transactions that have previously failed settlement.

CHESS is processing a rolling peak volume of 2.9 million trades per day over a three-month period as of March 2023. The daily average settled value from January to March 2023 was \$11.9 billion (including non-novated transactions).

### Clearing Risk Management

A key requirement of the RBA's FSS for Central Counterparties is that a central counterparty must have sufficient risk controls to provide a high degree of confidence that it can settle its obligations if there is a default by its two largest Clearing Participants and its affiliates in extreme but plausible market conditions.

As a result, ASX Clear has multiple layers of risk controls including:

- Minimum capital requirements for Clearing Participants, monitored through financial returns.
- End of day margining of Clearing Participants' cash market and equity derivatives market positions.
- At times of high market volatility, intraday margining of Clearing Participants' equity derivatives market positions.
- Daily stress testing of Clearing Participant positions under extreme but plausible market conditions to ensure the ongoing adequacy of clearing house financial resources.
- Additional margining of Clearing Participants where the size of their margins, or the projected shortfalls from closing their positions if they were to default in extreme but plausible market conditions, exceed acceptable levels.
- Conditions to restrict permissions, impose limits or direct participants to close out contracts.

CHESS provides data for cash markets to ASX's various RMS to support the above activities.

### History of CHESS

CHESS was implemented in two phases in 1994 and 1996 to provide the cash equity market with an electronic name-on-register Subregister system that replaced the existing share certificate holding method and paper-based asset transfer system. The change to the dematerialisation of share certificates and the introduction of a proprietary electronic messaging standard<sup>6</sup> offered enormous improvements in processing speed, efficiency, integrity and accuracy in clearing, settlement, and asset registration as well as enabling the ability to automatically support a large number of corporate actions.

The electronic nature of CHESS also enabled the introduction of DVP settlement in the Australian cash equities market, which paved the way for a substantial reduction in settlement time and improved the general efficiency and effectiveness of post-trade processing in Australia. CHESS was implemented with a T+5 (Trade date + 5 Business Days) settlement period. In 1999 the settlement cycle transitioned to T+3, and in 2016 it was further reduced to the current T+2 settlement cycle.

Other significant enhancements made to CHESS during the past 20 years include:

- Support for additional asset classes, including:
  - Exchange Traded Funds (**ETFs**), introduced in 2001.
  - Exchange traded Australian Government Bonds (**AGBs**), introduced in 2013. From that time retail investors could buy and sell AGBs on the ASX, with full CS services available.
- Implementation of the TAS in 2011 to facilitate the reporting of trades by AMOs other than ASX to support the provision of CS services to those AMOs and their participants. Chi-X Australia (now Cboe Australia) was the first user of the TAS.

---

<sup>6</sup> At the time of CHESS implementation, existing global standards in post trade processing lacked the message sophistication to accommodate the advanced functionality of CHESS.



- Establishment of the Managed Fund Settlement Service (**mFund**) Settlement Service in 2014, introducing a new asset class for unlisted managed funds, with holdings held on CHES and the purchase or sale of units settled in CHES.
- The introduction of optional electronic CHES holding statements for investors available from December 2021.

Additionally, over nearly three decades of operations, ASX has been progressively investing in the security, resilience, and reliability of CHES. CHES continues to be reliable, stable, resilient, and the average monthly service availability<sup>7</sup> has not fallen below the availability target of 99.80%. CHES service availability is tracked on two levels – overall CHES availability, and more specifically the CHES TAS availability, as shown in the chart below covering the period 2012 to 2022.

CHES Annual Average Service Availability

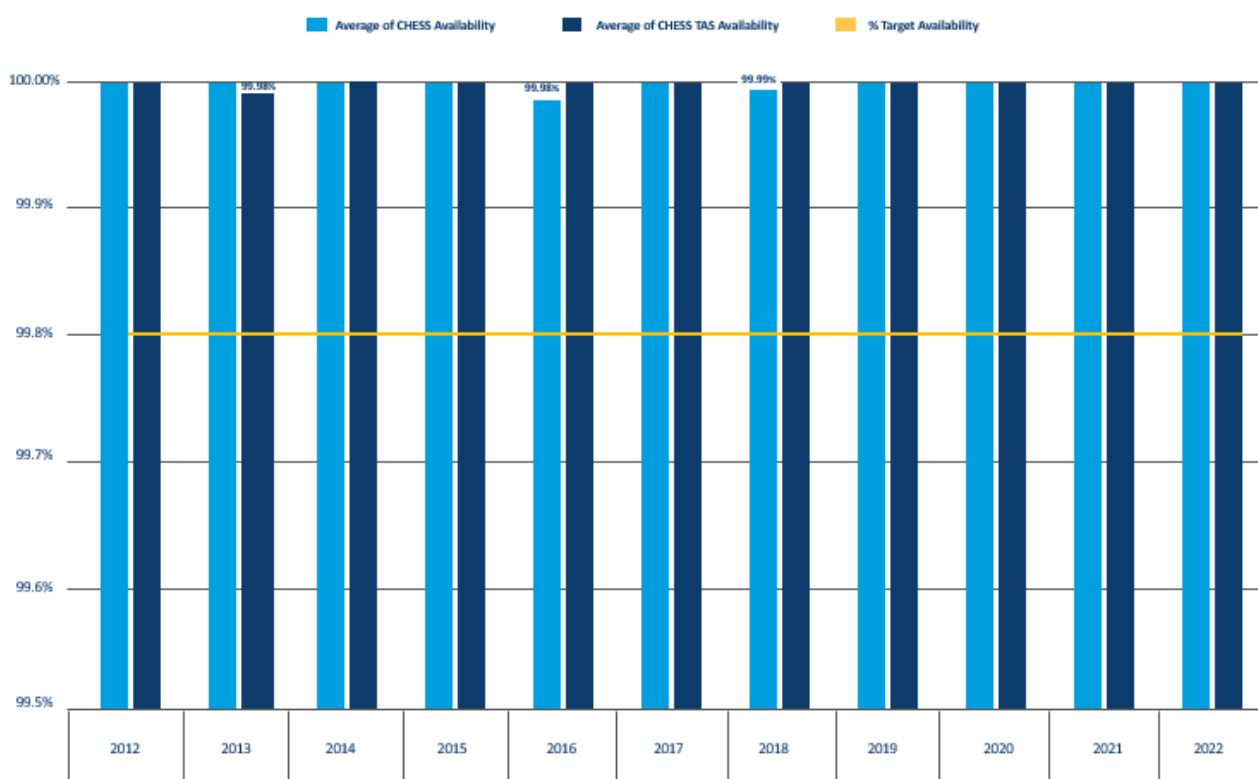


Figure Appendix A.D CHES Actual Service Availability vs Availability Target

### Current Performance of CHES

ASX recognises the importance of maintaining market confidence in the continued performance, resilience, security, and supportability of CHES, including its ability to meet the requirements set under the RBA’s FSS and the requirements of Australia’s financial markets.

CHES continues to operate within KPIs, achieving or exceeding service level objectives for all of the calendar year 2022:

- 100% actual availability for CHES and CHES TAS compared to the availability target of 99.80%.

<sup>7</sup> Availability is a metric defined as a percentage of accessibility of a business service to its users within agreed time windows. For the purposes of regulatory reporting, any unavailability is when the business service is unable to be used or accessed by users. For CHES the time window is 6.00am to 7.00pm Monday to Friday; for the TAS the time window is 7.10am to 7.00pm Monday to Friday. For an average year, acceptable total time that CHES would be unavailable is 6.5 hours for the year or 32.5 minutes per month; and for the TAS 5.917 hours for the year or 29.583 minutes per month.

- No major incidents (as defined by ASX).
- No failed changes or changes resulting in incidents to CHES and all related environments.
- Successful disaster recovery test completed on 28 May 2022 (an annual test).
- No overdue ASX internal audit actions.

### CHES Operating Model

The S&P business is the sponsoring business division for CHES and is responsible for the external delivery of CHES. The CHES application has a Technical Owner, the General Manager of S&P Technology, a Business Owner, the General Manager of Equity Post Trade, and Operations Owner, the General Manager of S&P Operations.

The Technology and Data business division is responsible for delivering the underlying infrastructure which is utilised by CHES and the systems integrated into CHES, as well as Security and Vendor Management.

The ASX Technology Centre of Excellence and *ASX Delivery Framework* defines the best practice guidelines for the S&P delivery teams.

Some of the enabling functions described in Figure A.B of this Appendix are responsible for enterprise-wide governance, and for maintaining the frameworks and policies within which CHES operates. These include the *ERM Framework* and *Investment Governance Framework*.

The S&P Operations and S&P Technology teams have extensive experience and frameworks, practices, and policies to support its business and technology operations, supported by the enterprise-wide services provided by the enabling teams.

More details on the operating model are provided in *Section 8.2 Operating Model – Resources and Vendor Support*

### The CHES Architecture and Boundaries

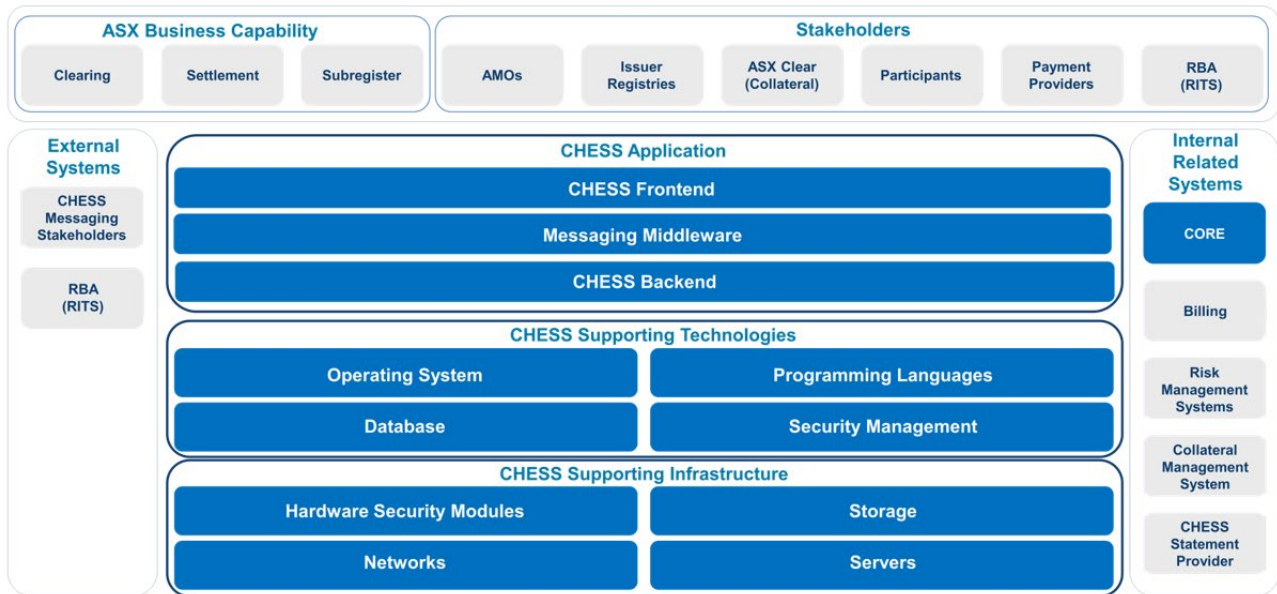
CHES operates within an ecosystem *Figure Appendix A.E CHES Ecosystem* represents a visual summary of the ecosystem, including the Clearing, Settlement and Subregister business capabilities, the stakeholder groups and CHES users, the CHES application and the associated technology stack, and the key internal and external systems that CHES interacts with. The boxes coloured blue are considered in the scope of this report.

For the purposes of this report, CHES is defined as comprising:

- CHES Application.
- CHES Supporting Technologies.
- CHES Supporting Infrastructure.

External Systems and Internal Related Systems (other than CORE) as identified in *Figure Appendix A.E CHES Ecosystem* not included in the scope of this report.





**Figure Appendix A.E CHESSEcosystem**

## Business Capabilities

CHESSE provides three key ASX business capabilities to support the Australian cash equities market, including:

- Clearing – The receipt and validation, registration, novation, and netting of on-market trades.
- Settlement – The T+2 market wide net batch delivery versus payment of both on-market obligations (novated) and off-market obligations (non-novated).
- Subregister – The register of CHESSE sponsored holdings that in conjunction with the Issuer-Sponsored Subregisters held off CHESSE by the Issuer Share Registries, form the complete register for each Issuer.

## Stakeholders

As outlined above, CHESSE interacts with a number of different stakeholders in the provision of CS services.

## Interfaces

CHESSE is a functionally rich platform to which ASX's customers have aligned their own processes and bespoke technologies. CHESSE operates as a computer-to-computer system that relies on an electronic message exchange between CHESSE and CHESSE users' own systems over a communications network.

CHESSE is a message-based transaction processing system where users primarily interact with CHESSE by sending and receiving electronic messages over a network. The messaging interfaces utilised by CHESSE to interact with CHESSE users include:

- CHESSE messaging – This is the message standard and transport used by CHESSE users including Participants, Share Registries, Payment Providers and AMOs (other than ASX Trade) to communicate with CHESSE. CHESSE messaging is defined in the CHESSE External Interface Specification (EIS).
- 15022 messaging via SWIFT – This is the message standard and transport used by CHESSE to communicate with RBA's RITS to perform cash settlement.
- ASX internal signals – This is the message standard and transport used by CHESSE to internally receive security (i.e., financial product) reference data from the ASX reference data system and trades from ASX Trade.

## Application

The CHES application is made up of three logical components the "front-end", the messaging middleware, and the "backend".

- The "front-end" is responsible for managing secure CHES messaging sessions. CHES users establish CHES messaging sessions and while they are logged on, they are able to send and receive encrypted messages conveying information about settlement obligations, accounts, holdings, and other transactions. CHES messaging is always available except for some periods during CHES overnight processing where CHES is taken offline for backups.
- The messaging middleware is a purpose-built store and forward message broker that provides a loosely coupled persistent interface between the front-end and the functional backend processing.
- The "backend" is comprised of over 100 distinct functional components that specialise in particular aspects of CHES processing and maintenance of the associated data in the CHES database. Some of these components interact with its own dedicated queues on the messaging middleware and process messages received from CHES users. For example, there are functional components that process messages to create accounts, bilateral settlement instruction messages, trade registration messages, netting, and batch settlement.

## External Systems

There are ■■■ CHES users, each of which has its own system that is compliant with CHES messaging. There are ■■■ unique CHES user side systems, ■■■ of which are supplied by the ASX, with the remainder being bespoke builds by users or provided to them by software vendors.

CHES interfaces to the RBA RITS systems over the SWIFT network to affect the cash payments for net batch settlement.

## Internal Systems

CHES interacts with a number of internal ASX systems to perform all tasks associated with cash equities CS services.

### CORE

An important ASX system that feeds CHES critical information is CORE. It is the source of all security related reference data such as Issuers, financial products, corporate actions, and the settlement (Business Day) calendar. It is also the source of trades that have occurred on ASX Trade.

### Billing

CHES collects data based on transactional and other activities and calculates fees applicable to each CHES customer each month. CHES creates a monthly file that is sent to the ASX billing system for the purpose of invoicing customers.

### Risk Management

The risk management models for ASX Clear such as Capital Stress Test and Cash Market Margin are managed in a different system called the RMS. CHES provides CSV format extracts of obligations and other reference data at the end of online processing for use by RMS.

### Collateral Management

Cash market margin and equity options margin can both be collateralised by placing a pledge on units held in CHES. This requires CHES communications using CHES messaging with the ASX collateral systems called Collateral Management System (**CMS**), the ASX Clear Derivatives Clearing System (**DCS**) and the Stock Lodgement System (**SLS** – part of the DCS).

### CHESS Statements

Any changes to a HIN account or holding level is notified to the holder (investor) via monthly CHESS statements. CHESS creates file extracts and sends them via secure File Transfer Protocol (**FTP**) to an external statements provider. The same provider produces either paper or electronic statements depending on the holder's preference, as recorded in CHESS.



**Appendix B – CHES Risks**

The following table is an extract from the ASX ERM system of the 31 CHES related risks with associated controls, risk ratings and CHES Roadmap initiatives. The initiatives are identified to maintain the low risk appetite for matters relating to CHES now and into the future. In addition to the roadmap initiatives listed against each risk, there are additional operational actions that are being tracked by the S&P RWG, that are recorded in the ERM system.

**Table Appendix B.A Extract of ASX ERM system of the CHES Related Risks**

ASIC Category	ASX Risk Theme	No.	CHES Risk	Inherent Risk	Summary of Controls	Residual Risk	Initiative ID	CHES Roadmap Initiative
<b>Resilience</b> The ability to avoid / recover from incidents or events	Outage or unavailability of critical systems or services due to a natural disaster or another unexpected event	1	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	C-1	Review CHES resilience scenario testing
							C-2	[REDACTED]
							C-3	[REDACTED]
							C-4	CHES - Review backup and restore processes
							C-5	CORE - Review the backup and restore processes
<b>Reliability</b>	Outage or unavailability of	2	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	O-6	Front end – OS and Hardware upgrade



ASIC Category	ASX Risk Theme	No.	CHES Risk	Inherent Risk	Summary of Controls	Residual Risk	Initiative ID	CHES Roadmap Initiative
The ability of the system to function and perform consistently	critical systems or services due to a software or hardware defect	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	O-7	CHES Access upgrade
		[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	O-8	[Redacted]
		[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	O-11	Monitoring application upgrades
		[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	O-12	Backend upgrades [Redacted]
		[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	O-13	Backend upgrades [Redacted]
		[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	O-16	HSM Device upgrades
		[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]		
		[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]		
		[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]		
		[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]		





ASIC Category	ASX Risk Theme	No.	CHES Risk	Inherent Risk	Summary of Controls	Residual Risk	Initiative ID	CHES Roadmap Initiative
			[REDACTED]					
	Market Outage and/or Business disruption due to system malfunction/failure	4	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	O-2 O-3 O-9 O-10 O-11 O-14	Improve maturity level of the Availability and Capacity Management Framework and processes based on COBIT Stress test CHES to determine further points of failure Address CORE dependencies: Reference Data (Batch) & Trade Data (Real time) Monitoring application upgrades Assess alternative hardware architecture for



ASIC Category	ASX Risk Theme	No.	CHES Risk	Inherent Risk	Summary of Controls	Residual Risk	Initiative ID	CHES Roadmap Initiative
								backend servers to support CHES
							O-15	Customer VPN Access
							O-16	HSWM Device Upgrades
							C-1	Review CHES resilience scenario testing
	Non-compliance with contractual obligations with third parties - Technology	5	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]		Not Applicable
		6	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	O-5	Establish a Managed Service Contract agreement [REDACTED]
			[REDACTED]					





ASIC Category	ASX Risk Theme	No.	CHES Risk	Inherent Risk	Summary of Controls	Residual Risk	Initiative ID	CHES Roadmap Initiative
	Non-compliance with regulatory obligations or relief	7	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	C-1	Review CHES resilience scenario testing





ASIC Category	ASX Risk Theme	No.	CHES Risk	Inherent Risk	Summary of Controls	Residual Risk	Initiative ID	CHES Roadmap Initiative
	Ineffective or inefficient process design or manual execution	9	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]		Not Applicable
<b>Integrity</b>	Outage or unavailability of critical systems or services due to an internal procedural error	10	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	C-1	Review CHES resilience scenario testing



ASIC Category	ASX Risk Theme	No.	CHES Risk	Inherent Risk	Summary of Controls	Residual Risk	Initiative ID	CHES Roadmap Initiative
The validity and accuracy of data	Ineffective system functionality and utility (including performance and capacity)	11	[Redacted]	[Redacted]	[Redacted]	[Redacted]	O-1	Develop a new model for forecasting future trading growth
			[Redacted]	[Redacted]	[Redacted]	[Redacted]	O-4	Capacity & Performance Improvements
			[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
	Inefficient, untimely and ineffective delivery of technology changes	12	[Redacted]	[Redacted]	[Redacted]	[Redacted]		Not Applicable



ASIC Category	ASX Risk Theme	No.	CHES Risk	Inherent Risk	Summary of Controls	Residual Risk	Initiative ID	CHES Roadmap Initiative
			[REDACTED]					
	Data entry, maintenance or input error	13	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]		Not Applicable
			[REDACTED]		[REDACTED]			



ASIC Category	ASX Risk Theme	No.	CHES Risk	Inherent Risk	Summary of Controls	Residual Risk	Initiative ID	CHES Roadmap Initiative
		14	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]		Not Applicable
	Data entry, maintenance or input error	15	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]		Not Applicable



ASIC Category	ASX Risk Theme	No.	CHES Risk	Inherent Risk	Summary of Controls	Residual Risk	Initiative ID	CHES Roadmap Initiative
			[REDACTED]					
Security	Unauthorised access and/or use of customer (and data) from harm	16	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
			[REDACTED]					
	External fraud	17	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]



ASIC Category	ASX Risk Theme	No.	CHES Risk	Inherent Risk	Summary of Controls	Residual Risk	Initiative ID	CHES Roadmap Initiative
			[REDACTED]		[REDACTED]		[REDACTED]	[REDACTED]
	Internal fraud by management or staff (including contractors)	18	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
		19	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]





ASIC Category	ASX Risk Theme	No.	CHESS Risk	Inherent Risk	Summary of Controls	Residual Risk	Initiative ID	CHESS Roadmap Initiative
			[REDACTED]		[REDACTED]		[REDACTED]	[REDACTED]
	Inadequate cyber resilience framework	20	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]		Not Applicable
	System or data compromised by unauthorised or malicious activity	21	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]		Not Applicable



ASIC Category	ASX Risk Theme	No.	CHES Risk	Inherent Risk	Summary of Controls	Residual Risk	Initiative ID	CHES Roadmap Initiative
Other	Compliance with ASX's rules and frameworks is inadequately monitored	22	<p>The risk of failing to have in place inadequate arrangements for identifying and escalating instances of non-compliance with the following Operating Rules to Compliance teams for further investigation.</p> <ul style="list-style-type: none"> <li>ASX Listings Rules,</li> <li>ASX Clear Operating Rules</li> </ul>	[REDACTED]	<ul style="list-style-type: none"> <li>Employees are trained</li> <li>Checklists and/or templates used</li> <li>Documented procedures</li> </ul>	[REDACTED]		Not Applicable
	Failure to report in a complete, accurate and/or timely manner to regulators	23	<p>The risk of failing to provide data to CRO teams for reporting to regulators (including providing settlement batch daily statistics from CHES to ASIC and the RBA):</p> <ul style="list-style-type: none"> <li>In accordance with prescribed timelines; and</li> <li>Which has not undergone a content sensibility review/check by Settlement Operations staff.</li> </ul>	[REDACTED]	<ul style="list-style-type: none"> <li>Checklists and/or templates used</li> </ul>	[REDACTED]		Not Applicable



ASIC Category	ASX Risk Theme	No.	CHES Risk	Inherent Risk	Summary of Controls	Residual Risk	Initiative ID	CHES Roadmap Initiative
			FSS Reporting and daily operational reporting (to be re-reviewed once FMI in place)					
	Inability to identify new competitors and/or manage existing competition resulting in loss of business, customer complaint, reputational damage and deteriorating investor sentiment.	24	Competition in Cash Market Clearing or Settlement services - Clearing and Settlement - The Council of Financial Regulators (CFR) has released Government endorsed policy statements setting out the regulatory framework for competition in cash equities clearing and settlement. Government has indicated that a CS facility licence will not be granted to a new entrant until the regulatory framework for competition is legally enforceable. Exposure draft legislation for competition in clearing and settlement was released for comment in March 2023.		<ul style="list-style-type: none"> <li>• Effective external stakeholder/customer engagement</li> <li>• Effective regulatory engagement</li> <li>• Review and monitoring</li> <li>• Adequate investigation / due diligence conducted</li> </ul>			Not Applicable



ASIC Category	ASX Risk Theme	No.	CHES Risk	Inherent Risk	Summary of Controls	Residual Risk	Initiative ID	CHES Roadmap Initiative
			In addition, the detailed operational and regulatory requirements needed to support a new CS facility (for either clearing or settlement) still need to be developed. [REDACTED]					
		25	Competitive threats due to change in market structure, introduction of new technology or behaviour of customers and competitors.	[REDACTED]	<ul style="list-style-type: none"> <li>Review and monitoring</li> <li>Adequate investigation / due diligence conducted</li> </ul>	[REDACTED]		Not Applicable



ASIC Category	ASX Risk Theme	No.	CHES Risk	Inherent Risk	Summary of Controls	Residual	Initiative ID	CHES Roadmap Initiative
	Inappropriate management of the ASX brand and / or reputation	26	Customer facing engagements, Reporters, analysts (Media Coverage), documents published by the team tarnish the reputation of ASX	[REDACTED]	<ul style="list-style-type: none"> <li>Review and monitoring</li> <li>Effective external stakeholder/customer engagement</li> <li>Management reporting</li> <li>Management approval / authorisation</li> </ul>	[REDACTED]		Not Applicable
	Inappropriate pricing of products or services	27	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]		Not Applicable
	Inappropriate strategy or prioritisation of strategic initiatives	28	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]		Not Applicable
	Lack of responsiveness to changes or exposure to economic conditions that	29	Market activity levels or activities could potentially change leading to sustained revenue reduction from low activity levels or pricing pressure. [REDACTED]	[REDACTED]	<ul style="list-style-type: none"> <li>Monitoring and alerting tools</li> <li>Effective regulatory engagement</li> </ul>	[REDACTED]		Not Applicable



ASIC Category	ASX Risk Theme	No.	CHES Risk	Inherent Risk	Summary of Controls	Residual Risk	Initiative ID	CHES Roadmap Initiative
	affect ASX's market position.		[REDACTED]		<ul style="list-style-type: none"> <li>Monitoring and alerting tools</li> <li>Business Continuity and/or Disaster Recover Planning</li> <li>Effective external stakeholder/customer engagement</li> <li>Adequate investigation / due diligence conducted</li> </ul>			
Non-compliance with licence obligations		30	<p>The risk of adverse regulatory, reputational and customer impact as a result of failing to comply with:</p> <ul style="list-style-type: none"> <li>ASX's Clearing &amp; Settlement Licences; and</li> <li>ASX's Australian Financial Services Licence.</li> <li>This impacts the following entities:</li> </ul>	[REDACTED]	<ul style="list-style-type: none"> <li>Restricted system access</li> <li>Checklists and/or templates used</li> <li>Segregation of duties including independent reviews</li> <li>Restricted system access</li> <li>Documented procedures</li> </ul>	[REDACTED]		Not Applicable



ASIC Category	ASX Risk Theme	No.	CHES Risk	Inherent Risk	Summary of Controls	Residual Risk	Initiative ID	CHES Roadmap Initiative
			<ul style="list-style-type: none"> <li>○ ASX Clear Pty Ltd</li> <li>○ ASX Settlement Pty Limited</li> <li>○ Austraclear Ltd</li> <li>○ Collateral Management Services</li> <li>○ Austraclear Services Ltd</li> </ul>		<ul style="list-style-type: none"> <li>• Skill/support availability is tracked and regularly assessed</li> <li>• Exception/error reports reviewed</li> <li>• Management reporting</li> <li>• Management approval / authorisation</li> <li>• Monitoring and alerting tools</li> <li>• Data backups and replication</li> <li>• Effective change management</li> <li>• Asset management</li> <li>• Review and monitoring</li> <li>• Governance frameworks and processes</li> </ul>			
	Poor management of customers or	31	Complaints lodged with ASX regarding equities clearing and settlement service, potentially		<ul style="list-style-type: none"> <li>• Management reporting</li> </ul>			Not Applicable



ASIC Category	ASX Risk Theme	No.	CHESS Risk	Inherent Risk	Summary of Controls	Residual Risk	Initiative ID	CHESS Roadmap Initiative
	disputes with external parties (including clearing participants, listed entities, vendors) leading to complaints [REDACTED]		raised with regulators, not being managed in accordance with ASX's complaints handling framework.		<ul style="list-style-type: none"> <li>Adequate investigation / due diligence conducted</li> <li>Effective external stakeholder/ customer engagement</li> </ul>			



## Appendix C – Glossary of Key Terms, Acronyms and Abbreviations

**Table Appendix C. Glossary of Key Terms, Acronyms and Abbreviations used in the Special Report**

Acronym	Term	Definition
AGBs	Australian Government Bonds	Australian Government Bonds available for trading on market
	Approved Financial Products	Those products approved to be cleared and settled through CHES.
AMO	Approved Market Operator	A Market Operator approved by ASX Clear and ASX Settlement as an Approved Market Operator.
APRA	The Australian Prudential Regulatory Authority	Australia’s independent statutory authority that is responsible for promoting financial stability
ARC	Audit and Risk Committee	
ASIC	The Australian Securities and Investments Commission	Australia’s financial markets conduct regulator that is responsible for promoting fair and efficient financial systems
ASX	ASX Limited	ASX Limited is an Approved Market Operator
ASX Clear	ASX Clear Pty Limited	The ASX wholly owned subsidiary provides clearing facilities for Australia’s equities markets, including cash equities and exchange-traded equity options
ASX Group	Australian Securities Exchange	
ASX Settlement	ASX Settlement Pty Limited	The ASX wholly owned subsidiary that provides settlement services for Australia’s equities markets and maintains the CHES Subregister
ASX Trade	The ASX cash equities trading market	
BAU	Business as Usual	Usually refers to day to day business activities
BCM	Business Continuity Management	
BCMF	Business Continuity Management Framework	An ASX enterprise-wide framework that guides the ASX business division specific approach to business continuity planning, testing and backups and recovery
BC	Business Continuity	
BC/DR	Business Continuity / Disaster Recovery	
BCP	Business Continuity Plan	Outlines the arrangements to be followed in the event of a significant operational or technology disruption impacting ASX’s key services.
	Business Day	A day other than Saturday, Sunday, New Year’s Day, Good Friday, Easter Monday, Christmas Day, Boxing Day, and any other day which ASX notifies Market Participants is not a Business Day.
CAB	Change Advisory Board	
Capex	Capital expenditure	
Cboe	Cboe Australia Pty Limited	Cboe is an Approved Market Operator (previously known as Chi-X Australia)
CCO	Chief Compliance Officer	

CCOO	Chief Customer and Operating Officer	
CEO	Chief Executive Officer	
CFO	Chief Financial Officer	
CFR	The Council of Financial Regulators	The coordinating body for Australia's main financial regulatory agencies.
CHESS	Clearing House Electronic Subregister System	The core system used by ASX to fulfil its CS obligations.
	CHESS Roadmap	A Roadmap that includes appropriate initiatives and investments to enable CHESS to remain operationally resilient until CHESS is replaced
	CHESS user	Any organisation that connects directly to the CHESS – including AMOs, Clearing and Settlement Participants, Product Issuer Settlement Participants, Share Registries and Payment Providers
CIO	Chief Information Officer	
	Clearing Participant	An entity admitted as a participant under the ASX Clear Operating Rules. The participant is authorised to clear trades through the clearing house operated by ASX Clear.
CISO	Chief Information Security Officer	
CMM	Cash Market Margining Model	All cash market transactions novated to ASX Clear are margined using the CMM. The model consists of Risk Margin and Mark to Markets components.
CMS	Collateral Management System	CMS manages collateral of Clearing Participants for risk exposures.
COBIT	Control objectives for information and related technologies	An IT Governance framework for businesses looking to implement, monitor and improve IT management best practices.
CoP	Code of Practice	
CORE	CORE	CORE is an ASX system that feeds critical information to CHESS including security related reference data such as Issuers, financial products, corporate actions, and the settlement (Business Day) calendar. CORE is also the source of trades that have occurred on ASX Trade.
	Corporations Act	Corporations Act 2001 (Cth)
CRO	Chief Risk Officer	
CS	Clearing and Settlement	
	CS Boards	The ASX Clearing and Settlement Boards
	CS Lead Executive	The Group Executive responsible for the S&P business division
CTO	Chief Technology Officer	
DCS	ASX Clear Derivatives Clearing System	The system used by ASX Clear for clearing exchange-traded options traded on the ASX market
	Delivered Risk	A risk introduced by the delivery of a project to a business function or service.
	Delivery Risk	A risk that threatens the execution/delivery objectives of a project or change initiative, to be addressed within the project.

DR	Disaster Recovery	A set of strategies that execute the necessary steps to restore business critical applications
DRP	Disaster Recovery Plan	
DvP	Delivery versus Payment	
EIS	External Interface Specification	EIS stands for External Interface Specification and means a document, made by ASX Settlement that provides detailed information about protocols, message formats and security features or communications between Facility Users and ASX Settlement.
EPMO	Enterprise Project Management Office	
ERM	Enterprise Risk Management	The Enterprise Risk Management function and framework of ASX.
	Enterprise Risk Management system	ASX's Governance, risk and compliance tool that supports oversight and accountability across all ASX businesses.
ESA	Exchange Settlement Accounts	
ETF	Exchange Traded Fund	Open-ended managed investment funds that can continually issue new units and redeem existing units.
	Extended Period	The period in which CHES remains operationally reliable over a planning horizon that extends to 2032 or until such time that a new solution is implemented.
FE	Fair and Effective	
FOT	Fair and Orderly Trading	
FSS	Financial Stability Standards	As published by the RBA
FTP	File Transfer Protocol	
HIN	Holder Identification Number	A number used to: (a) identify a Holder of financial products on the CHES Subregister; and (b) link the Holding details maintained on the CHES Subregister with the Holder's Registration Details.
	Issuer	An entity who issues or makes available or proposes to issue or make available, Approved Financial Products (e.g., a listed company).
ITSM	IT Service Management	The end-to-end delivery of IT services to customers.
JSG	Joint Steering Group	
KPI	Key Performance Indicator	
KRI	Key Risk Indicator	
MAO	Maximum Allowable Outage	
	Market Participant	An entity authorised as a participant (broker) of an AMO for the purposes of trading.
mFund	Managed Fund Settlement Service	The settlement service called mFund provided by ASX Settlement in respect of unlisted managed fund products.
MSA	Master Services Agreement	
NFT	Non-functional testing	

NSX	National Stock Exchange of Australia Limited	NSX is an Approved Market Operator
OGC	Office of the Group General Counsel	
Opex	Operating expenditure Payment Provider	An entity that operates an exchange settlement account with the RBA in its own name who is eligible to authorise and make payments on behalf of all types of eligible Settlement Participants or RTGS Participants, make payments to Settlement Participants or RTGS Participants, and facilitate CHES batch settlement and/or RTGS by approving or making payments
PDAf	ASX Project Delivery Assurance Framework	
PISP	Product Issuer Settlement Participant	An entity admitted for limited purposes including facilitating the settlement in Batch Settlement of transactions relating to requests for issue and redemption of unlisted managed fund products.
PGG	Portfolio Governance Group	
PgWG	Program Working Group	
PWG	Portfolio Working Group	
RACI	Responsible, Accountable, Consulted, and Informed Matrix	
RAG	Red/Amber/Green	
RAID	Risk, Assumptions, Issues and Dependencies register	A tool used to track risks, actions, issues, and decisions at ASX
RAS	Risk Appetite Statement	
RBA	Reserve Bank of Australia	
RITS	Reserve Bank Information and Transfer System	Australia's high-value settlement system, which is used by banks and other approved institutions to settle its payment obligations on a Real Time Gross Settlement (RTGS) basis.
RMS	Risk Management System	Operated by ASX Clear, RMS provides an end of day risk reporting capability to the ASX Clearing Risk Management team, with data sourced from DCS and CHES.
RSA	Risk Self-Assessment	Annual risk self-assessment by business units
RTO	Recovery Time Objective	Set time periods for recovery for ASX systems during a disaster or incident
RWG	Risk Working Group	
S&P	Securities and Payments business division of ASX	A business division within the ASX responsible for cash equity post trade services including clearing, settlement and services provided to issuers. Securities and Payments is responsible for CHES and also Austraclear.
SCR	Software Change Request Settlement Participant	An entity authorised to create and maintain accounts on the CHES Subregister; and to settle transactions

		in Approved Financial Products through CHES, including in batch settlement
SGG	Strategic Guidance Group	
	Share Registry	An organisation which on behalf of an Issuer (listed or quoted) manages the register of members for that issuer.
SLA	Service level agreement	
SLS	Stock Lodgement System	Collateral part of DCS
SOC	Security Operations Centre	
SORA	System Operational Risk Assessment	
SSX	Sydney Stock Exchange Limited	SSX is an Approved Market Operator
SWIFT	Society for Worldwide Inter-bank Financial Telecommunication	SWIFT is a global member-owned cooperative providing secure financial messaging services.
T	Trade (or Trading) Day	A day determined by the Approved Market Operator to be a Trading Day and notified to Market Participants.
TAS	Trade Acceptance Service	A service provided by ASX Clear and ASX Settlement to an Approved Market Operator under which certain categories of market transactions are accepted by ASX Clear and ASX Settlement for clearing and settlement.
	The Code	<i>ASX's Cash Equities Clearing and Settlement Code of Practice</i>
TMC	Technology Management Committee	
TOGAF	The Open Group Architecture Framework	An industry framework used for enterprise architecture that provides an approach or designing, planning, implementing and governing an enterprise information technology architecture.
ToR	Terms of Reference	
TSR	Test Summary Report	
TURNs	Technology Upgrade Release Notices	
UAT	User Acceptance Testing	
VPN	Virtual Private Network	