DISCLOSURES FOR THE YEAR ENDED 30 JUNE 2025

INTRODUCTION AND SCOPE

Computershare Investor Services (Ireland) Limited ("CISIL" or "The Firm") is authorised and regulated by the Central Bank of Ireland as an Investment Firm under the Markets in Financial Instruments Directive ("MiFID").

CISIL is not a member of a consolidation group and consequently does not report on a consolidated basis for accounting and prudential purposes.

The information in this document has not been externally audited unless it is also included in the Annual Report and Accounts which have been prepared and audited under accounting requirements. This document does not constitute any form of financial statement and therefore must not be relied upon in making any judgment on the Computershare Group.

Since 26th June 2021, CISIL is required to comply with the Investment Firm Regulations ("IFR") which introduced a more proportionate and fit-for-purpose regime for investment firms. The regime allows for differentiated regulation of Investment Firms depending on their classification, with higher impact firms being subjected to more intensive regulation. The objective of the regime is to provide for capital, liquidity and other prudential requirements for investment firms that reflect the business models of those firms and proportionately capture the risks posed and faced by these firms. CISIL is a class 2 firm under the regulations. As a class 2 firm, CISIL is required to publicly disclose information concerning CISIL's risk management objectives, internal governance arrangements, remuneration policy, own funds and capital requirements.

RISK APPETITE

CISIL's risk appetite is owned by the CISIL Board ("The Board"). Risks are calculated using a combination of likelihood, consequence and the effectiveness of controls in place. Likelihood is based on probability and frequency of an event or transaction and consequence is based on financial, reputational, operational, regulatory and Customer/Client impact.

The risk appetite is embedded in CISIL's strategy and business plan and documented in the Enterprise Risk Management Framework and Internal Capital Adequacy & Risk Assessment Process ("ICARAP") document. The Board has identified the areas of risk to which CISIL might be exposed and the Risk Committee and Audit Committee assess and review the risks, their potential impact, controls, capital adequacy and other risk mitigation arrangements. The Board and senior management receive regular risk management information to ensure that the number and type of risks accepted do not prevent the fulfilment of business objectives and continued regulatory compliance.

RISK MANAGEMENT AND GOVERNANCE

Risk management is a high priority for CISIL. The Board of Directors is responsible for the overall direction, oversight of management and corporate governance of CISIL. CISIL's Board consists of two independent non-executive directors, one non-executive director and one executive director. The Directors collectively hold 29 directorships outside of other entities controlled by the Computershare Group. In selecting Board members, CISIL have regard to the Computershare Diversity, Equity and Inclusion Policy.

Risk Management follows a step-by-step approach: Identification, Assessment, Management and Mitigation. In line with Governance best practice, CISIL has formed a number of committees and the governance of the steps is reviewed by these committees.

Risk Committee: assists the Board in fulfilling the corporate governance and oversight responsibilities in relation to risk management framework and material risk exposures. In particular, the Committee will oversee, on behalf of the Board, the management and control of risk with particular attention to conduct, reputation, operational and regulatory risk. The Committee will also advise the Board on the adequacy of the Risk Management Frameworks and implementation thereof. The Committee meets at least four times each year and met four times in year ending June 2025.

Audit Committee: provides assistance to the CISIL Board in fulfilling corporate governance responsibilities of its Board and will have responsibility for the oversight of and advice in relation to CISIL's financial reporting, internal control structures, regulatory compliance monitoring, the internal audit function, regulatory client asset management framework and the adequacy of the external audit. The Committee meets at least four times each year and met four times in year ending June 2025.

Routine Business Committee: has responsibility for considering all matters of an administrative or routine nature that have been delegated to it in accordance with its terms of reference.

Regulatory Compliance Forum: oversee CISIL's compliance with regulatory requirements, including Client Asset Requirements (CAR) and the firm's Anti Money Laundering/Counter Terrorist Financing (AML/CFT) Framework.

Client Asset Operations Forum: is a coordination and supervisory group with responsibility for the provision of effective oversight of Client Asset arrangements in accordance with the Client Asset Regulations ("CAR") applicable to CISIL and associated governance and risk management. This includes oversight, review and challenge of the monthly report, prepared by the HCAO in line with CAR.

Risk Forum: oversees CISIL's compliance with regulatory risk requirements and the CISIL Risk Management Framework.

Conduct Forum: is a coordination and supervisory group with responsibility for the provision of effective oversight of Conduct arrangements in accordance with the Conduct Regulations applicable to CISIL and associated governance and risk management. This includes oversight, review and challenge of the monthly report, prepared by the Governance team.

Outsourcing & Governance Forum: ensures that CISIL's outsourcing arrangements comply with regulatory requirements and are sufficiently monitored and reviewed to ensure that such arrangements are fit for purpose.

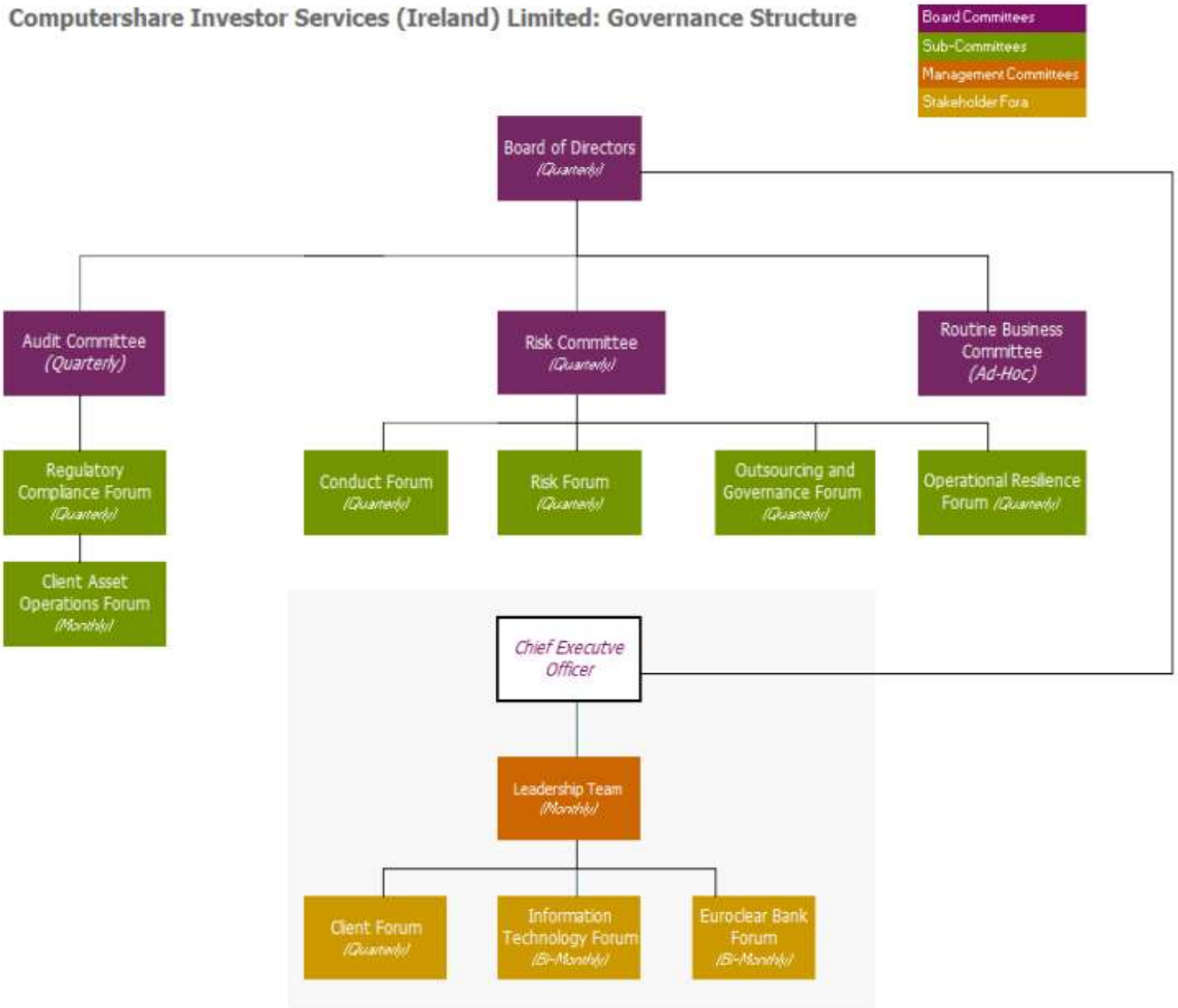
Operational Resilience Forum: provides oversight of the firm's operational resilience arrangements such as compliance with regulatory requirements, the firm's compliance with internal resilience related policies and the controls in place to manage risks and the assessment of all resilience related incidents in accordance with policy.

Leadership Team: manages CISIL's business to achieve its strategic objectives as agreed with the CISIL Board.

Client Forum: oversees the retention and growth of the CISIL business and to encourage collaboration with the wider Computershare Group where appropriate.

Information Technology Forum: ensures that the Computershare's information technology capabilities are sufficiently monitored and reviewed by CISIL to ensure the infrastructure of the Company is fit for purpose.

Euroclear Bank Forum: ensures that all EB system matters are subject to regular transparent oversight and associated control.



The Board are responsible for ensuring that an appropriate system of internal controls is maintained, and for reviewing its effectiveness by analysing updates provided to it by the Risk and Audit Committees. Each of the above committees has representatives from the core

business units and detailed terms of reference which sets out their respective roles and responsibilities.

CISIL has adopted the 'Three Lines of Defence' framework for risk governance.

First Line of Defence: The primary responsibility and accountability for risk management lies with line management within each business sector of the company. They are responsible for the identification, assessment, control, monitoring, mitigation and management of risk at business sector level including the implementation of appropriate controls and reporting to the Board in respect of all major risk events.

Second Line of Defence: The risk management functions are responsible for maintaining independent risk oversight of the first line of defence and ensuring that a risk control framework is in place. They formulate risk policy and strategy and provide independent oversight and analysis of risk reporting. The responsibility for risk oversight and governance of risk rests with CISIL's Risk Forum reporting to the firm's Risk Committee. In addition, support functions such as Compliance, Legal and Information Security undertake ongoing independent oversight of risks.

Third Line of Defence: This is provided by CISIL's Group Internal Audit function and provides an independent, reasonable, risk-based assurance to key internal and external stakeholders on the effectiveness of CISIL's internal control environment and culture.

REMUNERATION

The IFR requires Investment firms to disclose certain information regarding their remuneration policy and practices for those categories of staff whose professional activities have a material impact on the investment firm's risk profile, known as 'Identified Staff'.

The Computershare Group and the firm's management have established remuneration structures to determine the overall reward and remuneration policy and to ensure that this is consistent with the achievement of the Computershare Group and the firm's strategic objectives.

In general, remuneration practices will: aim to reflect the risk appetite of the firm, will ensure there is an appropriate balance between fixed and variable components and will seek to avoid conflicts of interest and excessive risk taking. No individuals are involved in assessing and approving their own remuneration. Remuneration is awarded based on a mix of quantitative and

qualitative factors. The Independent Non-Executive Directors are paid directors' fees only and do not receive variable remuneration.

Remuneration for Executive Directors may include one or more of the following: salary, bonus, pension, share based compensation and other benefits. Directors and other staff may provide services to a number of Computershare group entities and may be compensated through those entities for the services to the Group (including services to CISIL). CISIL's remuneration policy is gender neutral.

Gender Pay Gap* as at 30 June 2025:	
Mean Hourly Remuneration Identified Staff:	16.46%
Median Hourly Remuneration Identified Staff:	16.61%

*Gender Pay Gap represents the difference in pay of men and women, expressed as a percentage

Identified Staff Remuneration year ending 30 June 2025**	**€000**	**No. of beneficiaries**
Total Fixed	1,295	13
Total variable including benefits under long term incentive schemes and cash	225	10
Company pension contributions to defined contribution pension schemes	166	10
Severance payments awarded during the financial year (Upfront)	53	1

Deferred remuneration awarded for previous performance periods	**No. of Shares**
Deferred Shares	14,672
Due to vest	4,756

**Where Identified Staff receive direct remuneration from the Company, the figures are disclosed here. The remaining Identified Staff do not receive any direct remuneration in respect of their services to the Company

With respect to the ratio of fixed to variable remuneration set in accordance with IFR, in the reporting year, the maximum entitlement that a Computershare Senior Executive may receive as variable remuneration is 75% of their base salary. For all other staff and identified staff, variable remuneration does not exceed 50% of fixed.

CAPITAL ADEQUACY

As at 30 June 2025 CISIL's regulatory capital resources are as follows:

Capital Item		*€,000*
Tier 1	Share Capital	1,718
	Share Premium	3,000
	Revenue Reserves	15,082
	Capital Reserves	441
	Less Goodwill	0
Tier 2	Total Tier 2 Capital	0
	Total Capital	**20,241**

There are no deductions from tier 1 and 2 capital resources.

CISIL's Pillar 1 capital requirement is calculated in accordance with IFR and is currently based on the total K-Factor amount, this was reported as €2.1m in the June 2025 Internal Capital Adequacy & Risk Assessment Process (ICARAP).

The Fixed Overhead Requirement (FOR) is equal to one quarter of CISIL's relevant fixed expenditure and is also reviewed to determine CISIL's capital requirements. As at 30 June 2025 the FOR was €2.1m

Appendix 1 contains Own Funds disclosures which are required as a result of the introduction of the IFR.

The approach that CISIL employs in assessing the adequacy of its internal capital to support current and future activities is contained in the Internal Capital Adequacy & Risk Assessment Process (ICARAP). The analysis conducted on CISIL's Pillar 2 economic and normative risk assessment capital requirements identified the following material risks to which CISIL might be exposed; Operational Risk, Strategic Risk, Compliance and Regulatory Risk, People Risk and Change Risk.

MATERIAL RISKS

CISIL defines a Material Risk as any event that could: damage the core earnings of the company; reduce capital; threaten the company's reputation or viability; introduce cash flow volatility; and/or breach legal or regulatory obligations. Material risks have been identified in line with the firm's risk appetite statements and are outlined below. All other risks affecting CISIL have been assessed as immaterial and therefore are not disclosed in this statement.

Operational Risk

The risk of loss resulting from inadequate or failed internal processes, people and systems. Material operational risks relating to CISIL incorporate three main areas:

- Processing, Design and Execution Risk- Risks include poor design and development, and inaccurate execution, of operational processes and procedures leading to firm and/or client detriment
- Information Security Risk - Risk that data security, confidentiality, privacy or integrity is compromised. Supplier and Counterparty Risk- Risks where suppliers or counterparties (including intergroup companies, brokers, banking relationships, insurers, vendors and third parties) fail to deliver on contractual, promised and expected services.

This risk is managed by maintenance of appropriate systems and controls, including;

- First, Second- and Third-line monitoring of adequacy of processes and procedures in place and annually reviewing all documentation and recruiting and retaining high calibre employees supported by a robust training plan;
- Independent information security team with appropriate oversight for the group information security framework;
- Robust governance oversight of suppliers of material services and signed legal service level agreements to ensure services are delivered to the required standard as set by CISIL.

Strategic Risk

The risk of potential loss arising from a failure in CISIL's strategies due to external factors adversely influencing the outcome or execution of the strategies.

This risk is managed by maintenance of appropriate systems and controls, including;

- Monitoring the economic environment.
- Periodically reviewing the business plan and strategy to avoid loss of clients to competitors and ensuring the cost base is sufficiently flexible should business decline through transaction volumes or loss of client contracts.

Compliance and Regulatory Risk

The risk of failing to adhere to current and future laws and regulations within the regulatory regime of EU and Ireland.

This risk is managed by maintenance of appropriate systems and controls, including:

- Dedicated Compliance and Risk teams and implementation of the Annual Compliance Plan (including process and procedure review, transactional and thematic compliance monitoring and annual training plan);
- Regular review of upstream regulation with implementation projects tracked through a dedicated upstream legislation project;

- Oversight by Regulatory Compliance Forum and Risk Forum.

People Risk

The risk of insufficient capability including knowledge, skill, and experience capacity and / or right behaviours including culture, conduct and values, within the workforce.

This risk is managed by maintenance of appropriate systems and controls, including:

- Independent tacking of attrition levels through dedicated KRI's overseen by the firm's Leadership Team;
- Close monitoring on the hybrid working process and reporting performed by the Leadership Team via the Risk Profile Reviews;
- Documented risk and control procedures in line with the Enterprise Risk Management Framework.

Change Risk

The risk of Business disruption resulting from ineffective change management.

The Firm has a dedicated project team for change projects, including upstream legislation implementation oversight which is sponsored by the firm's CEO and CRO.

This risk is managed by maintenance of appropriate systems and controls, including:

- Increased resources to deliver change projects;
- Project governance processes in place;
- Oversight by the Leadership Team on the main ongoing projects.

Appendix 1

Template EU IF CC1.01 - Composition of regulatory own funds

	€000's	Source based on references of the balance sheet in the audited financial statements as at 30th June 2025
Common Equity Tier 1 (CET1) capital: instruments and reserves		
OWN FUNDS	20,241	
TIER 1 CAPITAL	20,241	
COMMON EQUITY TIER 1 CAPITAL	20,241	
Fully paid-up capital instruments	1,718	Called up share capital presented as equity
Share premium	3,000	Share premium account
Retained earnings	15,082	Profit and loss account
Other reserves	441	Capital redemption reserve/Other reserves

Template EU IFCC2: Own funds: reconciliation of regulatory own funds to balance sheet in the audited financial statements

Balance sheet as in audited financial statements as at 30th June 2025	€000's
Assets	
Total Assets	**27,417**
Liabilities	
Total Liabilities	**7,176**
Shareholders' Equity	
Called up share capital presented as equity	1,718
Share premium account	3,000
Capital redemption reserve	48
Other reserves	393
Profit and loss account	15,082
Total Shareholders' equity	**20,241**

The Firm has the same accounting and regulatory scope of consolidation.