



# DISCLOSURES FOR THE YEAR ENDED 30 JUNE 2021

## **INTRODUCTION AND SCOPE**

Computershare Investor Services (Ireland) Limited (CISIL) 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.

Up to 26th June 2021, CISIL was required to comply with the Capital Requirements Regulation (CRR) which set out the regulatory capital framework for Credit Institutions and Investment Firms across Europe. 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 new 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 Assessment Process (ICAAP) 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 three independent non-executive directors, one executive director and one non-executive director. The directors have 31 directorships in total. In selecting Board members, CISIL have regard to the Computershare Diversity 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:** provides assistance to 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 and regulatory client asset management framework. 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 2021.

**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, the internal audit function and the adequacy of the external audit.

**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.

**Client Asset Regulation Forum (CAR 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.

**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.

**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.

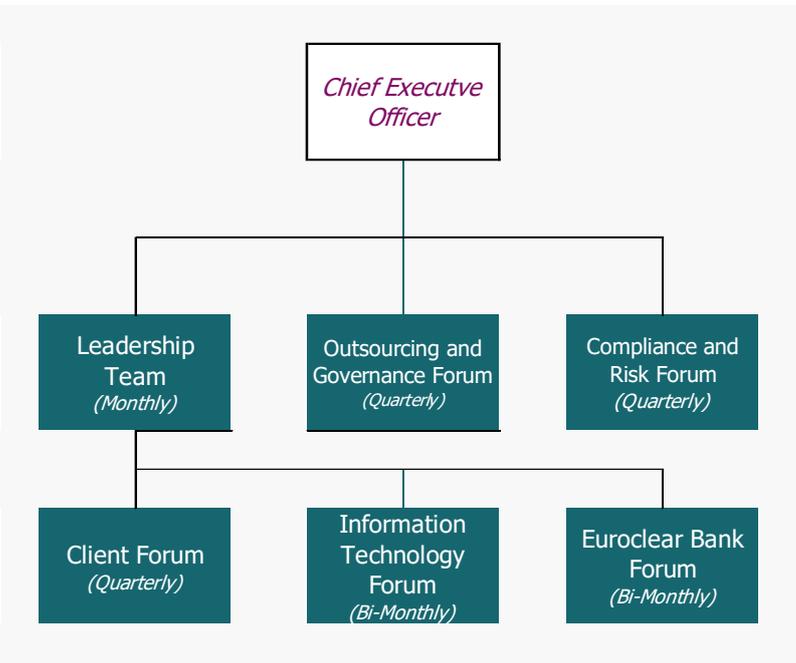
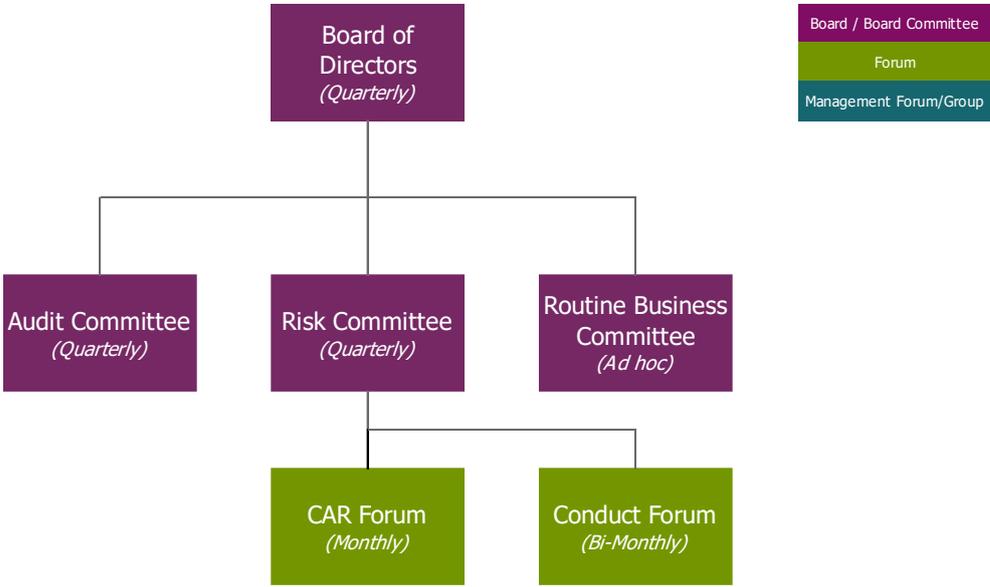
**Information Technology Forum:** ensures that the Computershare's information technology capabilities are sufficiently monitored and reviewed by CISIL to ensure the infrastructure of the Company is fit for purpose.

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

**Compliance and Risk Forum (CRF):** oversees CISIL's compliance with regulatory requirements and the CISIL Risk Management Framework.

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

# Computershare Investor Services (Ireland) Limited : Governance Model



|                         |
|-------------------------|
| Board / Board Committee |
| Forum                   |
| Management Forum/Group  |

The Board are responsible for ensuring that an appropriate system of internal controls is maintained, and for reviewing its effectiveness by analysing reports 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 Compliance and Risk Forum. 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 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).

## CAPITAL ADEQUACY

As at 30 June 2021 CISIL's regulatory capital resources are as follows:

| Capital Item  |                         | € ,000 |
|---------------|-------------------------|--------|
| Tier<br>1     | Share Capital           | 1,718  |
|               | Share Premium           | 3,000  |
|               | Revenue Reserves        | 7,935  |
|               | Capital Reserves        | 314    |
|               | Less Goodwill           | 0      |
| Tier<br>2     | Total Tier 2<br>Capital | 0      |
| Total Capital |                         | 12,967 |

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 Fixed Overhead Requirement (FOR). The FOR is equal to one quarter of CISIL's relevant fixed expenditure and determines CISIL's capital requirements. As at 30 June 2021 the Pillar 1 requirement was €2.8m.

The total K-Factor amount as at 30 June 2021 was calculated as €11k.

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 Assessment Process (ICAAP). The analysis conducted on CISIL's Pillar 2 capital requirements identified the following material risks to which CISIL might be exposed; Financial Risk, Operational Risk, Strategic Risk, Regulatory Risk and People 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 statement and are outlined below. All other risks affecting CISIL have been assessed as immaterial and therefore are not disclosed in this statement.

### **Financial Risk**

As prescribed in the IFR, two financial risks relating to CISIL incorporate two main areas:

- › Concentration risk – The risk to the firm's trading book position due to the default of counterparties.
- › Liquidity risk – The risk of failing to plan, or not being able to meet financial obligations as they fall due, or financial obligations required by regulators or legislators.

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

- › Monitoring the firm's liquid assets through monthly financial information to ensure sufficient liquidity in place.
- › Monitoring the firm's total own funds against regulated capital requirement and internal capital target.
- › The firm does not operate a firm trading book.

### **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 data 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.

## 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 team 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;
- › Oversight by Compliance 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.

As a result of the Covid-19 pandemic, People risk has been indicated as a material risk. The workforce has remained resilient and business continuity contingencies have been activated.

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

- › Activated BCP, enabling personnel to work from home;
- › Oversight of the Pandemic environment and the Irish Government guidelines performed by the Leadership Team via the Risk Profile Reviews;
- › Documented risk and control procedures in line with the Enterprise Risk Management Framework.

## 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 2021 |
|--|--------|--|
| <b>Common Equity Tier 1 (CET1) capital: instruments and reserves</b> |        |  |
| OWN FUNDS  | 12,967 |  |
| TIER 1 CAPITAL   | 12,967 |  |
| COMMON EQUITY TIER 1 CAPITAL   | 12,967 |  |
| Fully paid up capital instruments                                    | 1,718  | Called up share capital presented as equity  |
| Share premium  | 3,000  | Share premium account  |
| Retained earnings  | 7,935  | Profit and loss account  |
| Other reserves   | 314    | 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 2021 | €000's        |
|---|---------------|
| <b>Assets</b>   |               |
| Total Assets  | <b>17,444</b> |
| <b>Liabilities</b>  |               |
| Total Liabilities   | <b>4,477</b>  |
| <b>Shareholders' Equity</b>   |               |
| Called up share capital presented as equity                           | 1,718         |
| Share premium account   | 3,000         |
| Capital redemption reserve  | 48            |
| Other reserves  | 266           |
| Profit and loss account   | 7,935         |
| <b>Total Shareholders' equity</b>                                     | <b>12,967</b> |

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