PILLAR 3 DISCLOSURES FOR THE YEAR ENDED 30 JUNE 2020

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.

As a MiFID authorised Investment Firm, CISIL is required to comply with the Capital Requirements Regulation (CRR) which sets out the regulatory capital framework for Credit Institutions and Investment Firms across Europe. The CRR framework requires firms to consider regulatory capital based on three Pillars;

Pillar 1: Specifies the minimum regulatory capital requirements for Credit, Market and Operational Risks.

Pillar 2: Specifies the supervisory review process and an assessment conducted by CISIL on whether additional capital should be held for risks not covered by Pillar 1.

Pillar 3: Specifies the public disclosure of information concerning CISIL's risk exposures and risk management processes.

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 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 is a high priority for CISIL. Governance arrangements are established and maintained by the Risk Committee and Audit Committee and reported to the Board. The Board determines the risk appetite and business strategy.

RISK MANAGEMENT AND GOVERNANCE

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.

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 function.

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, client assets and regulatory risk. The Committee will also advise the Board on the adequacy of the Risk Management Frameworks and implementation thereof.

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 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.

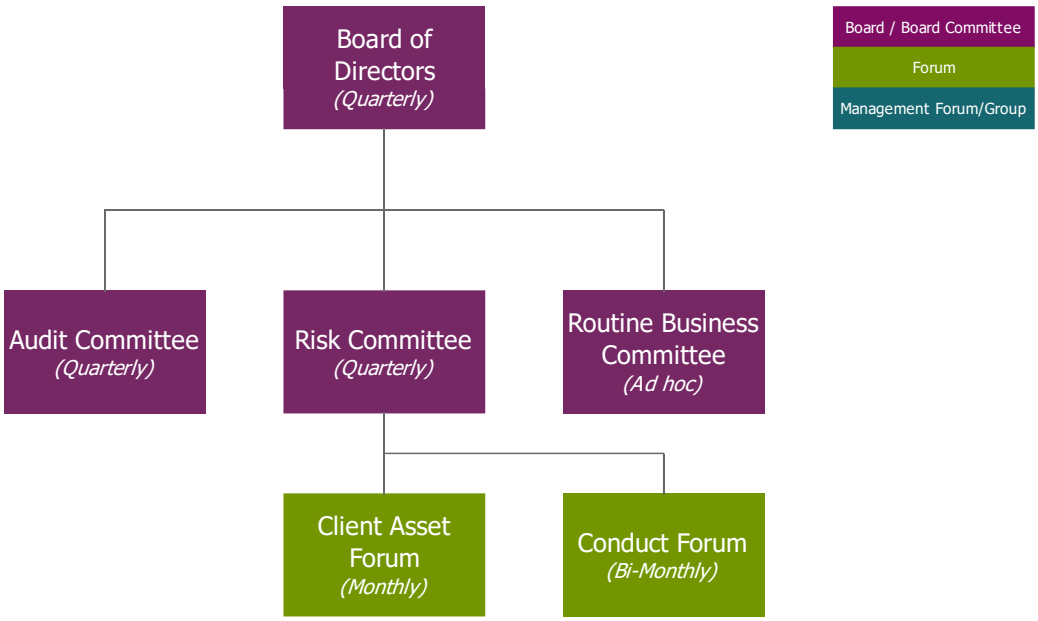
Leadership Team: manages CISIL's business to achieve its strategic objectives as agreed with the CISIL Board.

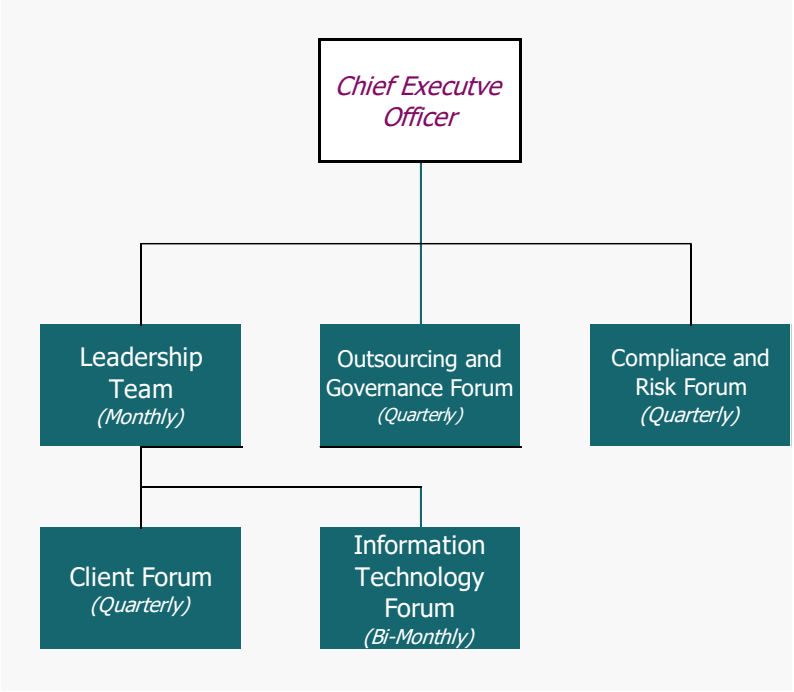
Client Forum: oversees the retention and growth of the CISIL business and to encourage collaboration with the wider Computershare Group where appropriate.

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.


Board of Directors
(Quarterly)
Board / Board Committee
Forum
Management Forum/Group
Audit Committee
(Quarterly)
Risk Committee
(Quarterly)
Routine Business Committee
(Ad hoc)
Client Asset Forum
(Monthly)
Conduct Forum
(Bi-Monthly)


Chief Executve Officer
Leadership Team
(Monthly)
Outsourcing and Governance Forum
(Quarterly)
Compliance and Risk Forum
(Quarterly)
Client Forum
(Quarterly)
Information Technology Forum
(Bi-Monthly)

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 2020 CISIL's regulatory capital resources are as follows:

	Capital Item	€,000
Tier 1	Share Capital	1,718
	Revenue Reserves	8,301
	Capital Reserves	314
	Less Goodwill	0
Tier 2	Total Tier 2 Capital	0
	Total Capital	10,333

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

CISIL's Pillar 1 capital requirement is calculated in accordance with CBOI guidelines, 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 2020 the Pillar 1 requirement was €2.8m.

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 and Regulatory 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 Pillar 3 statement.

Financial Risk

Material financial risks relating to CISIL incorporate two main areas:

- Credit Risk- The risk that creditors fail or have the potential to fail to pay all or part of a debt
- Financial Market Exposure Risk- The risk associated with changes in the level or volatility of interest rates, foreign exchange rates

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

- Utilising Delivery Versus Payment and cleared funds as appropriate;
- Periodically conducting due diligence on all counterparties to ensure they remain stable;
- Monitoring any exposure to interest rate or exchange rate movement risk through regular reviews of CISIL's budget and forecast process.

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.