SEI Investments (Europe) Limited

Pillar 3 Disclosure

Based on financial data as at 31st December 2021

Note: These disclosures have been prepared under the IFPRU regulations applicable at 31 December 2021.

Contents

1. Overview

1.1. Introduction

SEI Investments (Europe) Limited ("SIEL" or "the firm") is regulated in the United Kingdom ("UK") by the Financial Conduct Authority ("FCA"). Under the requirements of the Prudential Sourcebook for Investment Firms ("IFPRU"), as at 31 December 2021 SIEL was a significant €125k Limited Licence, and CRR Article 95 firm. SIEL was therefore required to calculate its Pillar 1 capital requirement as the higher of its Fixed Overhead Requirement ("FOR") and the sum of credit and market risk capital requirements as set out under the Capital Requirements Regulation ("CRR").

The FCA sets out certain capital adequacy standards and disclosure requirements to be implemented by regulated firms. These rules are built on three pillars.

Pillar 1 sets minimum capital requirements to meet credit and market risk.

Pillar 2 requires firms to assess capital adequacy in relation to the firm's actual risk profile and determine whether additional capital is required to cover these risks by the firm's Board of Directors through the Internal Capital Adequacy Assessment Process ("ICAAP") and the subsequent regulator's Supervisory Review and Evaluation Process ("SREP").

Pillar 3 seeks to improve market discipline by requiring firms to disclose certain information on their risks, including in respect of capital and risk management.

The Pillar 3 requirements have been implemented in the UK by way of IFPRU as set out in the FCA Handbook. This document contains the Pillar 3 disclosures required by IFPRU in respect of SIEL.

Effective from 1st January 2022, SIEL is subject to the Investment Firms Prudential Regulation (IFPR) which has different requirements. These disclosures have been prepared under the IFPRU regulations which were applicable as at 31 December 2021.

1.2. Purpose of Pillar 3

The purpose of Pillar 3 is to encourage market discipline by developing a set of disclosure requirements which will allow market participants to assess key pieces of information on a firm's capital, risk exposures and risk assessment process. The disclosures are to be made public for the benefit of the market.

These disclosures therefore allow market participants to assess the scope of application by regulated firms of the Basel framework and the rules in their jurisdiction, their capital condition, risk exposures and risk assessment processes, and hence their capital adequacy. Pillar 3 requires all material risks to be disclosed, enabling a comprehensive view of the firm's risk profile.

This document comprises SIEL's pillar 3 disclosures on capital and risk management as at 31st December 2021. It has two principal objectives:

I. To meet the regulatory disclosure requirements under the rules of the FCA;
II. To provide further information, useful to market participants, of these disclosures on SIEL's capital and risk profile.

1.3. Frequency of disclosure

The disclosures in this document are required to be updated annually, and if appropriate, more frequently.

2. Structure of SEI

SIEL is a wholly owned subsidiary of SEI Global Investments Corporation (“SGIC”), a company incorporated in the United States of America, which is wholly owned by SEI Investments Company (“SEIC”). SEIC is the ultimate parent company of SIEL. SEIC has its common stock traded on The Nasdaq Global Select Market® (NASDAQ) under the symbol “SEIC” and its common stock is registered with the U.S. Securities and Exchange Commission (“SEC”). SGIC is not a regulated entity.

SIEL is an asset management, custodian and investment processing services firm with its office located in London. SIEL also has an affiliate office located in South Africa, where SIEL itself is regulated by the Financial Sector Conduct Authority ("FSCA") as a Foreign Financial Services Provider. SIEL offers two core business services to its clients. These are Asset Management (“AM”) services and investment processing services, the latter being delivered utilising software technology known as the SEI Wealth Platform (“SWP”).

SIEL's AM services primarily include investment management programmes delivered to institutions and individual investors through intermediaries. AM is SIEL's original business offering in the UK and Europe. Investment management programmes in non-US markets are offered predominantly in the form of Undertakings for Collective Investment in Transferable Securities ("UCITS"). These are public limited companies with the objective of collective investment in transferable securities and other liquid financial assets of capital raised from the public and operating on the principle of risk spreading in accordance with the European Communities Undertakings for Collective Investment in Transferable Securities regulations. SIEL is the named distributor of the UCITS but is not the investment manager nor administrator. The UCITS are registered in the Republic of Ireland.

SWP is an investment accounting and securities processing system with capabilities that include global securities processing, trade-date and multi-currency accounting and reporting. It is designed around the client and portfolio management process. SWP is primarily offered to wealth managers and private banks delivering outsourcing of administrative and processing capabilities, enabling the wealth managers to focus more on the end client and their strategy and growth plans for their business. For some of the client firms, SIEL’s professional services assist them in managing their business transformation.

3. Capital resources and adequacy

3.1. Approach

SIEL determines its capital adequacy using the following process:

- Pillar 1 calculation: assumes the higher of;
  a) SIEL’s fixed overhead requirements (FOR), or
  b) the assessment of its Credit and Market risks, or
  c) the firm’s €125K base requirement.
- Pillar 2 calculation, based on a risk assessment and stress testing quantification of high impact, (severe but plausible) scenarios, including reverse stress tests on material macro-economic events, against SIEL’s Risk Appetite thresholds (see below), including its Operational risks.
- A cash flow analysis for winding down SIEL, in the event that a strategic decision is made to do so.

Pillar 2 capital requirements are outside the scope of this disclosure document.

3.2. Summary of the firm's capital position

Pillar 1 Capital Requirement	£m
Credit risk	5.1
Market risk	1.5
Total of credit and market risk	**6.6**
Fixed Overhead Requirement (FOR)	12.9
Pillar 1 capital requirement	**12.9**
Regulatory own funds	**121.4**
Excess of own funds over Pillar 1 requirement	108.5

3.3. Credit Risk – Exposure & Requirements

2021	Exposure (£m)	Average Risk Weight	Risk Weighted Exposure (£m)	Own funds requirement @ 8% (£m)
Institutions	110.2	20%	22.0	1.8
Corporates	29.9	100%	29.9	2.4
Other items	10.3	112%	11.5	0.9
Total	**150.4**	**42%**	**63.5**	**5.1**

3.4. Capital adequacy – Risk profile

Risk Appetite refers to the types and amount of risk that a company is willing to accept in the pursuit of its strategic objectives, given the available resources. Risk Appetite Statements provide the mechanism by which management communicates the general level of risk that the company is willing to take to achieve its strategic objectives and business plan. Notwithstanding SIEL's appetite for certain risks, the company recognises that for certain types of incidents, losses are inevitable. Therefore, SIEL may tolerate a loss within limits (Risk Tolerances).

Senior Management, with the assistance of the Chief Risk Officer, is responsible for articulating the company's Risk Appetite Framework. The Board of Directors is responsible for understanding Senior Management's Risk Appetite Framework, and, as necessary, challenging its suitability and providing independent, unbiased oversight. The Risk Appetite Framework should articulate the desired, forward-looking risk profile and improve the overall risk governance discussions and processes.

The SIEL Board reviews and approves the risk appetite statement at least on an annual basis to ensure that it is consistent with SEI's Group strategy, business environment, stakeholder requirements and UK regulatory requirements. Explicitly setting the risk appetite aims to ensure that SIEL's risk is proactively managed to the level desired and approved by the Board. Risk tolerance levels are set with escalation requirements which enable appropriate actions to be defined and implemented as required. In cases where the tolerance levels are breached, a Line Manager should immediately assess the incident as a Material Incident and follow the process established in the "Incident Escalation and Management Policy".

Any material amendments to the risk and capital strategy must be approved by the CRO, MRC, BRC, and/or the Board, depending on the significance.

At the legal entity level, SIEL utilises 3 primary risk categories in its taxonomy:

- Non-Financial (Operational) Risk: risks stemming from errors and omissions by personnel, inadequate processes and controls, technology failures or changes, and/or external events. This definition includes legal, regulatory and compliance

risks (risk related to the enforceability of contracts, interpretations of laws, compliance with the law, other impacts of regulation, and litigation)

- Financial Risk: risks associated with instability and losses in the financial market caused by movements in stock prices, currencies, interest rates, cash flow volatility, and balance sheet strength
- Strategic Risk: risks associated with the Company's ability to meet its business and performance goals and objectives

Within each of these 3 primary categories of risk, SIEL has identified sub-categories of risk that are material to our business.

Level 1	Level 2	Level 2 Definition
Non-Financial (Operational) Risk	**Processing and Execution**	The risk of unexpected financial or reputational loss as the result of poor execution of regular business tasks
	3rd party risk	The risk that engaging a third party to provide services may adversely impact an institution's performance and risk management.
	Employment Practices and Workplace Safety	The risk of acts inconsistent with employment, health and safety laws or agreements
	Business disruption (excluding Cyber)	The risk of events causing disruption of business, system failures or damage to physical assets
	Business Practices and Conduct	The risk that behaviours or business practices are illegal, negligent, unethical, or contrary to a firm's stated beliefs, values, and policies & procedures
	Fraud (including fraud perpetrated by cyber-crime)	The risk of events intended to defraud, misappropriate property, or circumvent regulations, company policy or the law
	Information & Cyber Security (including data privacy and theft)	The risks to SIEL and its stakeholders that could occur due to the threats and vulnerabilities associated with the operation and use of information systems and the environments in which those systems operate.
Financial Risk	**Credit Risk**	The risk of loss arising from the default of counterparties failing to meet their financial obligations
	Market Risk	The risk of losses arising from adverse movements in market prices
	Liquidity Risk	The risk that a firm, although solvent, either does not have available sufficient financial resources to enable it to meet its obligations as they fall due, or can secure such resources only at excessive cost.
Strategic Risk	**Business Risk**	The risk to a firm arising from changes in its business, including the risk that the firm may not be able to carry out its business plan and its desired strategy.
	Revenue concentration	The risk of revenue reductions from an excessive reliance on a particular Business Model
	Group Risk	The risk that the financial position of a firm may be adversely affected by its relationships (financial or non-financial) with other entities in the same group or by risks which may affect the financial position of the whole group, for example reputational contagion

SIEL's risk appetite within each of the risk areas relevant to it, is set out below:

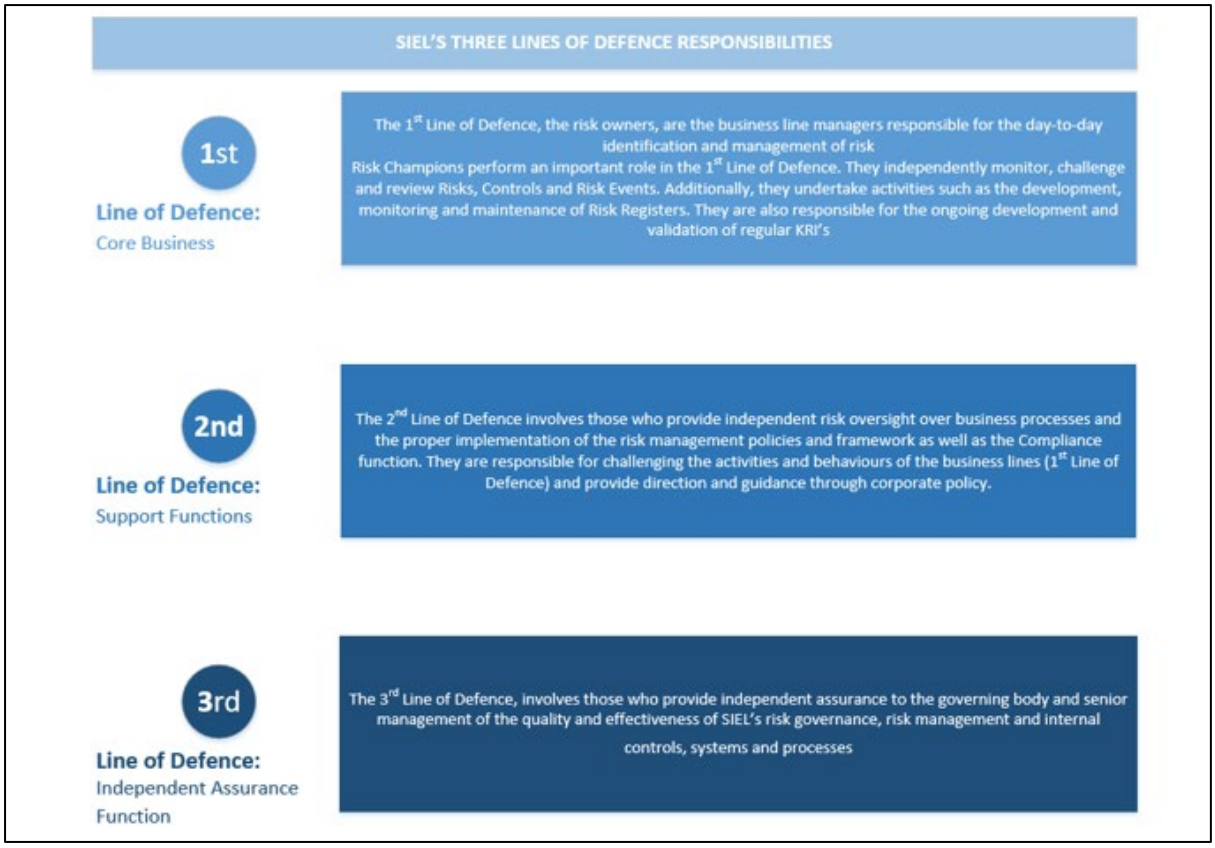
L1 Risk	Risk Appetite	Risk Appetite Statement
Non-Financial (Operational) Risk	**Risk Cautious**	SIEL is Risk Cautious for operational risk and has sought to increase UK resources to bolster the strong controls designed to ensure that operational risks are minimised. The nature of SIEL's SWP operating model means a level of operational risk is inevitable due to the provision of some front, middle and back office services to clients. SIEL seeks to identify, mitigate and manage these operational risks with appropriate control measures and safeguards, wherever possible. SIEL acknowledges that due to the nature and scale of its operations, and the reliance and interaction with multiple third parties, there are likely to be incidents and losses arising from business activities. SIEL recognizes that its operational processing is inherently linked to information technology platform availability and security, which is primarily, managed through its affiliate group companies. SIEL actively oversees the systems and controls relating to information security, access control and platform performance within its affiliates. SIEL receives management information and conducts monthly governance meetings with affiliated group companies providing leveraged services to monitor the effectiveness of agreed controls. SIEL is Risk Averse to instances of financial crime, defining this as Money Laundering, Terrorist Financing, Bribery and Corruption, notifiable breaches of Data Protection, Fraud (including Cyber Crime), Market Abuse, Tax Evasion and breaches of Economic and Financial Sanctions. Any instance where financial crime has occurred would result in a full investigation, active remediation and escalation within SIEL's senior management and to regulatory and/or law enforcement agencies, as applicable. SIEL is Risk Averse for financial or data loss or business disruption as a result of a cyber-attack. Whilst managing information security risk at a global level through systemic controls and protocols, because of the nature of SIEL's business the majority of the protection, including regular penetration testing is driven from SEI Group, local teams and control functions also take responsibility for appropriate/applicable monitoring and escalation processes and receive training on the various technological approaches, as befits their role. SIEL is Risk Cautious in operationalizing the controls designed to prevent financial crime, recognising the regulated status of our clients and counterparties and the broadly conservative approach to our business as an inherent risk mitigation. SIEL is Risk Averse for regulatory breaches or errors. SIEL has invested substantially in enhancing its CASS retail, regulatory monitoring, risk governance and control frameworks in order to minimise its regulatory risk exposures which may result in payment

L1 Risk	Risk Appetite	Risk Appetite Statement
		of client compensation and/or regulatory fines. Regulatory risks are assessed by the First Line of Defence with Second Line of Defence oversight.
Financial Risk	**Risk Averse**	SIEL is risk Averse for credit default. It is SIEL's policy to only deposit cash balances with industry leading banks. SIEL currently deposits its own cash with Wells Fargo and HSBC. It is SIEL's policy to invoice all of its clients at least quarterly, with collection monitored and receivables actively managed. SIEL is risk Cautious for market risk. SIEL does not conduct any proprietary trading activities. FX exposures are limited predominately to USD cash balances. SIEL is risk Averse for liquidity risk. As custodian, SIEL has CASS obligations which could result in SIEL temporarily providing funding to the client money pool. SIEL has implemented control to limit exposures within tolerances.
Strategic Risk	**Risk Neutral**	SIEL accepts a reasonable amount of strategic risk as a consequence of its current and future growth plans. SIEL has carried out asset management business from its inception and these services are provided to institutional clients and individuals through intermediaries. This business is profitable and SIEL expects growth in both assets under management and profitability. Strategic risks are relatively lower within the AM and AMD business segments, whilst higher in the SWP platform segment due to its earlier stage of maturity. SIEL has invested heavily in building the infrastructure to support investment processing activities.

4. Corporate governance framework

The risk management structure for SIEL has been developed in consideration of the current nature, scale and complexity of SIEL's operations and is aligned with the governance structure to provide an appropriate, effective and scalable control structure.

SIEL has adopted the three lines of defence model as its framework for risk governance. The framework comprises the governing body as well as the risk owners (1st LOD), those who fulfil risk oversight functions (2nd LOD) and those who fulfil independent assurance functions (3rd LOD). All three elements report to and are answerable to the governing body.



Board Oversight

The SIEL Board meets at least quarterly and is responsible, through its oversight obligation, for ensuring that the business affairs of the firm are adequately controlled and monitored. To appropriately discharge its function, the Board receives regular MI and reports from business units, subject matter experts and corporate functions. The Board delegates the executive management of the firm's business to the Chief Executive Officer ("CEO") to enable him to manage the day to day operations of the firm, subject to the Board reserved matters. The CEO is assisted in the discharge of his responsibilities, including the review and challenge of performance against risk appetite, by the London Executive Committee ("LEC"), a senior management forum comprising senior SIEL executives, which meets on a regular basis.

Specific matters reserved for the Board, include:

- Maintenance of a framework of prudent and effective financial, operational and compliance controls and risk management systems;
- Approval of the Group's Internal Capital Adequacy Assessment process; and
- Determination of the firm's corporate governance arrangements, including the review of risk management and control structures.

The SIEL Board has established a number of oversight committees, to help discharge its obligations, including the Board Audit & Compliance Committee and the Board Risk Committee. The Board receives regular management information reports from its sub-committees to ensure that it is in a position to determine the material risks that SIEL faces. The Board reviews these risks as frequently as it considers necessary based on the management information reports that it receives.

5. Risk management

Risk management and capital planning are established disciplines at SIEL and are part of the Board's review and consideration of its oversight and management of the business and the ICAAP as a whole.

The ICAAP is updated and formally reviewed by the Board at least on an annual basis. The previous ICAAP document was reviewed by the Board in April 2021. The assessment draws on the results of existing risk management techniques and reporting. Scenario analysis and stress testing are performed to assess SIEL's exposure to extreme events and ensure that appropriate mitigation actions are in place. SIEL is exposed to a range of risks; these are managed using a structured and consistent approach across the businesses. The techniques include formal controls, outsourcing, contingency planning, insurance and capital allocation.

5.1. Approach to risk management

SIEL's risk governance framework includes the Board Risk Committee, Management Risk Committee, Remuneration Committee and other relevant oversight committees and working groups deemed by the Board as being appropriate taking account of the size, nature and complexity of SIEL's current business and operational model.

SIEL's risk and control framework is designed around the following objectives:

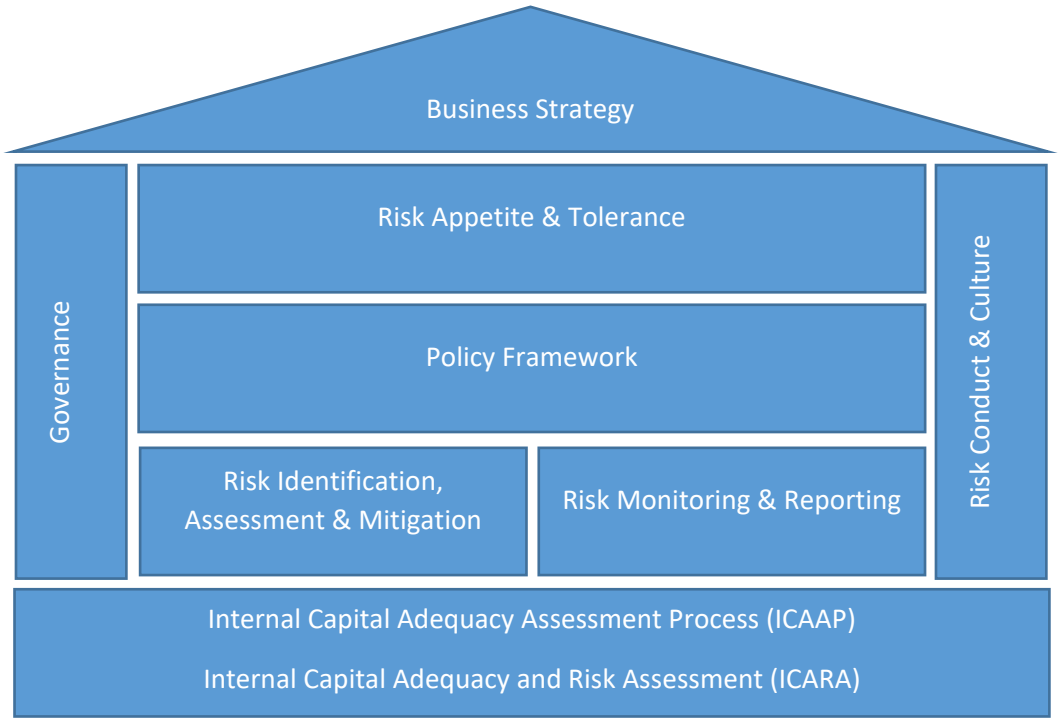
- Providing awareness, oversight, management and advice to SIEL in relation to current and potential future risk exposures in the business and future risk strategy;
- Promoting a culture of risk awareness and proactive mitigation across each business line; and
- Ensuring appropriate risk information is captured and reported to the Board Risk Committee so as to allow effective management of SIEL's risk profile.

5.2. Risk management framework

SIEL's Risk Management Framework (RMF) sets out the policy requirements and risk management components to identify, measure, mitigate, monitor, report and govern Financial, non-Financial (Operational) and Strategic risks in line with SIEL's regulatory obligations and Risk Appetite.

The RMF enables SIEL to achieve its strategic objectives and evidence that the firm is in control of its risks. By better managing its risks, SIEL protects the interests of clients, investors and the parent company, SEI Investments Company ("SEIC").

The RMF embeds the management of risk at all levels in the organisation and is subject to periodic review (at a minimum annually or in case of any relevant change to the risk framework) to ensure it recognises both new and emerging risks in the business and is appropriate and proportionate for a business of SIEL's size, scale, and complexity.



5.3. Risk identification and assessment methodologies

Risk & Control Self-Assessment (RCSA) is the process used to assess all risks identified by SIEL (new and existing risks), the control environment and the exposure to those risks. SIEL's RCSA is dynamic, combining both trigger-based and regular reviews (reviews should take place at a minimum annually). To ensure SIEL is able to define the live risk exposure, trigger-based reviews take place to consider the impact (including the cumulative impact of all individual events since the last annual review) of changes to the risk profile. The Risk Assessment process is undertaken by the 1st Line of Defence (1LOD) with oversight and challenge provided by the 2nd Line of Defence (2LOD).

All identified risks must undergo an Inherent and a Residual Risk Assessment. Inherent risk is the assessment of the risk expressed in terms of likelihood and impact either:

- before any dedicated controls or mitigating actions are put in place; or
- where there are controls or mitigating actions, these are assessed on the basis that they all fail.

Risk assessments are expressed in terms of likelihood and impact.

Controls which mitigate the risks are independently scored at regular intervals, in conjunction with empirical incident data. These independent control assessments are used to derive control factor scores which can be viewed by business unit or risk category.

Each risk category is assigned an *owner*, underneath a business unit or control function head, who is responsible for estimation and validation of the risk assessment parameters, documentation of existing controls, and monitoring of internal performance of these controls. The CRO, along with the relevant business unit or control function head, is responsible for overseeing and reporting on the development (for a newly identified risk) or

enhancement (for an existing risk) of systems and controls to effectively mitigate risk. The CRO is responsible for assisting the business unit and control function heads in escalating, managing, monitoring and mitigating risks within the business unit or control function which they oversee. The business unit and control function heads are responsible for controlling and managing risks within acceptable tolerance levels set by the Board. The risk management framework provides detailed local risk ownership and management.

6. Remuneration disclosures

6.1. Remuneration code applicability

The following groups of employees have been identified as meeting the FCA's criteria for Code Staff:

- The Directors of SIEL;
- Senior managers; and
- Employees whose professional activities could have a material impact on the firm's risk profile.

The categories above include all senior management, those responsible for the management of the main business units and the control function heads (including the heads of legal, finance and HR).

6.2. Link between pay and performance

Remuneration at SIEL is made up of fixed pay and variable performance-related pay.

Fixed pay is principally comprised of salaries but also includes appropriate employee benefits. All Code Staff receive a salary that reflects their talent, skills, competencies and contribution to the firm relative to the market for their roles.

Variable performance-related pay is principally comprised of bonus awards or, where appropriate, sales commissions.

- Annual performance bonus – All SIEL staff who are permanent employees are eligible to be considered for a bonus award annually. Bonuses for all employees take account of the overall group, department and individual performance against agreed objectives.
- Stock options – SEI's stock options vest at a rate of 50 per cent when specified financial targets are achieved, and the remaining 50 per cent when higher-specified financial targets are achieved. Options do not vest due to the passage of time but as a result of achievement of the financial vesting targets. Options granted in December 2017 and thereafter include a service condition which requires a minimum two or four year waiting period from the grant date along with the attainment of the applicable financial vesting target.
- Sales commissions – Members of staff whose role means that they are eligible for sales commissions do not receive annual bonuses. SIEL pays commissions based on sales procured. SIEL makes every effort to pay commissions on a quarterly basis only and on final sales.

Performance typically includes financial and non-financial measures including relevant risk and regulatory compliance factors to ensure that remuneration is appropriately risk-adjusted.

The Remuneration Committee ("REMCO") was established to ensure that the remuneration arrangements for executive management, senior management and other relevant SIEL staff align with the strategic aims of SIEL's business and also to enable, in an appropriate manner, the recruitment, motivation and retention of senior executives and management. The Board believes such arrangements are consistent with the principles of the relevant FCA Remuneration Code (i.e. SYSC 19A IFPRU Remuneration Code) and promote, effective risk management. Any exceptional arrangements for senior employees are approved by REMCO. REMCO has utilised the remuneration principles proportionality rule, taking into consideration the Board's risk appetite.

REMCO is governed by a formal set of terms of reference, which are reviewed at least annually. It is comprised of at least one independent non-executive director (there are currently three independent non-executive directors). There were four scheduled meetings during the year and two ad-hoc meetings.

The mandate of REMCO is to review and set or agree the remuneration policy and strategy for employees. It does so with a view to aligning remuneration with the successful achievement of SIEL's long term objectives, while taking into account market rates. Central to REMCO's mandate, is the ongoing review of the appropriateness and effectiveness of the Remuneration Policy with particular regard to best practice, in relation to regulatory and risk management considerations. No individual plays a part in any discussion about his or her own remuneration.

24 current Code staff were identified for 2021, including 15 individuals who are considered senior management. In respect of 2021, the following amounts were paid in fixed and variable remuneration to Code staff. Fixed remuneration includes base salary and benefits received between 1 January 2021 and 31 December 2021. Variable remuneration includes 2021 annual bonus awards made in February 2022 and the award value of long term incentive awards in respect of 2021.

£'000		**SIEL**	
		Senior Management (15)	**Other Code Staff (9)**
Fixed Remuneration		2,487	1,600
Variable	*Cash*	*2,130*	*771*
	Share-linked instruments	*1,152*	*565*
Total Variable Remuneration		3,283	1,336
Total Remuneration		**5,770**	**2,936**
Previously deferred variable remuneration paid out in 2021		458	16
Deferred variable remuneration outstanding from previous years			
Total vested		1,576	321
Total unvested		843	318

Two individuals were remunerated between €1m and €1.5m. One severance payment was made during the year. For confidentiality reasons the amount has not been disclosed. There were no sign-on payments during the year for this group.