Commentary

November 2017

SEI New ways. New answers.®

Enterprise Risk Management

- SEI is much more than an asset manager—we also provide software platforms, operational processes and a myriad of other business support functions.
- As with any business venture, all of these functions involve the willing acceptance of a variety of risks.
- To help our clients and business partners feel more confident when working with SEI, we base our formal Enterprise Risk Management program on one of the most widely recognised and applied risk management frameworks in the world.

The preceding papers in our Risk Management series dealt primarily with SEI's efforts to manage investment risk in a variety of forms. However, for many of our clients, SEI is much more than an asset manager—we also provide software platforms, operational processes and other business support functions. As such, we must manage many types of risks across the enterprise, including strategic, brand reputation, financial, operational, technology, talent, and regulatory and compliance risks. Accordingly, it is appropriate to conclude this series with a brief overview of SEI's Enterprise Risk Management efforts.

Working with a Proven Framework

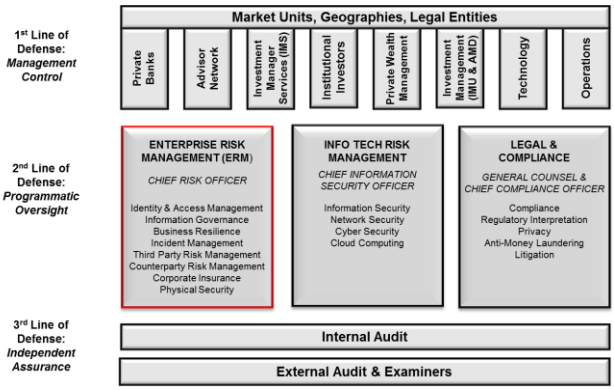
SEI's formal Enterprise Risk Management (ERM) program is aligned with the Committee of Sponsoring Organizations (COSO) Framework. COSO is a non-profit organisation, originally established by several of the largest accounting, audit and finance oversight committees in the US. The COSO Framework provides thought leadership on three inter-related subjects: enterprise risk management, internal controls and fraud deterrence. COSO is one of the most widely recognised and applied risk management frameworks in the world.

Consistent with the COSO ERM Framework, ultimately responsibility for providing oversight of enterprise risk management efforts sits with SEI's Board of Directors. Each year, the Board reviews, updates, and approves the firm's risk appetite and risk tolerance statements. Risk appetite statements establish SEI's willingness and capacity to take on risks as part of executing its business strategy; risk tolerance defines levels of acceptable risk for each business unit. Business unit managers are expected to identify and manage risks within established tolerance bands.

The firm conducts regular risk assessments throughout the company. As potential risks are identified, they are analysed and considered for probability (likelihood of occurrence) and severity (impact to the company). Risks are assessed on a gross (inherent) and net (residual) basis, taking into consideration key mitigating controls that we have put in place.

Three Lines of Defence

Everyone has a responsibility to help manage risk. SEI, like many organisations, uses a traditional "three lines of defence" approach to managing overall risk. This structure is depicted in the chart below.



The first line of defence is management control within the business or operating unit. As the principle owners of risk, these units are responsible for managing risk in their day-to-day activities. For example, our asset management group is responsible for managing investment risk in our

portfolios, while our U.S. limited purpose federal savings association is responsible for managing operational risk in our processing activities. These units implement our system of internal controls.

The second line of defence provides support through programmatic oversight. The primary groups supporting the second line of defence include the ERM team (led by our Chief Risk Officer); the Information Technology Risk Management team (led by our Chief Information Security Officer); and our Legal and Compliance teams (led by Chief Compliance Officers and General Counsel within each SEI legal entity or subsidiary). These teams help define our internal controls through the development of corporate policies, programs, interpretation of law, and guidance on risk management activities.

The third line of defence provides independent assurance that SEI's internal controls are effective and working as intended. This includes our Internal Audit team and our external auditors and examiners.

Orchestrating Efforts Across the Organisation

SEI's ERM team takes a leading role in coordinating risk management efforts across the three lines of defence. In particular, this team provides guidance, develops corporate policies, implements risk responses, monitors the adequacy and effectiveness of our control environments, and routinely reports on risk matters to our Operational Risk Committee and the Board of Directors. SEI's ERM Team focuses its efforts in six primary areas:

1. Information Governance—provides guidance and sets policy on how SEI values, classifies, handles, stores, archives, and deletes or destroys information; ensures that we meets our legal, regulatory, and business demands for information.

2. Business Resilience—develops and tests contingency plans to ensure that SEI can quickly adapt to disruptions while maintaining continuous business operations; business resilience activities are closely coordinated with disaster recovery, incident response, and physical security efforts to ensure that we safeguard our people, assets, and brand reputation.

3. Third Party Risk Management—identifies, analyses, and mitigates the risks presented by various business agreements and outsourcing relationships; this includes oversight of traditional vendors, strategic partnerships, and referrals, as well as other non-traditional arrangements such as guidance on crowdsourcing and use of open-source code.

4. Financial Risk Modelling—constructs financial or mathematical representations of potential business decisions; monitors external macro-economic and geo-political developments that could impact our business; quantifies potential outcomes and scenarios whenever SEI considers mergers and acquisitions, large investments, or other strategic initiatives.

5. Identity and Access Management—provides guidance on security measures and business disciplines around physical and logical access control; sets requirements on how we associate specific user rights (or restrictions) with known identities so that only the right individuals can access the right resources at the right times and for the right reasons.

6. Corporate Insurance—provides advice and assistance to business units on all insurance-related issues; ensures prompt reporting of insured risks and exposures, supports any claim matters, generates loss reports, and responds to daily insurance inquiries.

All opportunities come with some degree of risk, and no set of internal controls is completely fool proof. However, a strong Enterprise Risk Management program should help our clients and business partners feel more confident when working with SEI.

Important Information

No offer of any security is made hereby. This material represents an assessment of the market environment at a specific point in time and is not intended to be a forecast of future events, or a guarantee of future results. This information should not be relied upon by the reader as research or investment advice.

While considerable care has been taken to ensure the information contained within this document is accurate and up-to-date, no warranty is given as to the accuracy or completeness of any information and no liability is accepted for any errors or omissions in such information or any action taken on the basis of this information.

This information is issued by SEI Investments (Europe) Limited ("SIEL"), 1st Floor, Alphabeta, 14-18 Finsbury Square, London EC2A 1BR which is authorised and regulated by the Financial Conduct Authority.

SIEL is the distributor of the SEI UCITS Funds and provides the distribution and placing agency services to the Funds by appointment from the manager of the Funds, namely SEI Investments Global, Limited, a company incorporated in Ireland ("SIGL"). SIEL is a wholly owned subsidiary of SEI Investments Company ("SEI").