Scientific Infra Pte. Ltd.

Outsourcing Management Framework and Policy

Scientific Infra Pte. Ltd.

Contents

1. Purpose and scope

The Outsourcing Management Framework and Policy is the document to,

A. Set out a Framework for managing outsourcing within the Company, where it outlines a holistic framework for risk management in the outsourcing arrangement. The Framework will enable the Company, its Board of Directors and Head of Business Functions to oversee, manage and control outsourcing risks.

B. The Policy will define broad principles to manage outsourcing risks and in compliance with The EU Benchmark Regulation (Regulation (EU) 2016/1011[1]) (the "BMR") on Article 10 on Outsourcing.

Outsourcing arrangement is defined as an arrangement in which an Outsourced Service Provider ("OSP") provides the Company with a service that may currently or potentially be performed by the Company itself and which includes the following characteristics:

a. The Company is dependent on the service on an on-going basis; and
b. The service in integral to the Company's provision of its services.

2. Governance Structure

The Company's Outsourcing Governance Structure (shown below in Figure 2.1) sets out the Framework in managing outsourcing and its associated risks.
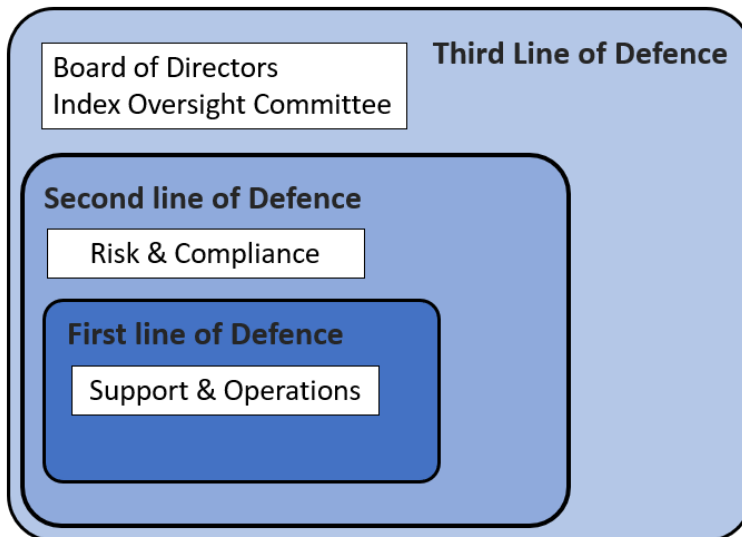

Figure 2.1

The various stakeholders involved as diagrammed above are further described in subsequent sections.

---

[1] Regulation (EU) 2016/1011 of the European Parliament and of the Council of 8 June 2016

3. Roles and Responsibilities

3.1 Board of Directors and Index Oversight Committee

The Board of Directors ("BOD") and the Index Oversight Committee ("IOSC") oversee outsourcing arrangements ensuring service review assessments are done at least annually, outsourcing arrangements are managed per The EU Benchmark Regulation and make decisions on renewing or engaging a new outsource provider.

3.2 Risk and Compliance Team

The Risk and Compliance Team, as the second line of defence, shall be responsible in:

a. Developing and maintaining the Outsourcing Management Framework and Policy, Procedures and Guidelines to manage the outsourced activities with the OSP;
b. Initiate the annual review and confirmation exercise of outsourcing arrangements;
c. Ensure The Company's Operations and Support Teams ("Infra Ops") perform annual reviews of outsourcing arrangements;
d. Review the overall reasonableness of assessments submitted by Infra Ops for all outsourcing arrangements through "Key Operational Risks and Control assessment" conducted monthly by Infra Ops on OSP;
e. Maintain a register of all outsourcing arrangements and Outsourcing Policy deviations;
f. Update IOSC regularly (at least quarterly during IOSC meeting) on all new outsourcing arrangements, as well as any significant outsourcing risks/issues that may potentially impact The Company and its reputation due to any adverse event that could potentially lead to prolonged service failure or disruption in the outsourcing arrangement, or any breach of security and confidentiality of customer information.

3.3 Company's Operations and Support

While activities may be outsourced, the responsibility to manage the outsourcing arrangements rests with the Infra Ops and their respective Function Heads should directly manage their outsourcing risks and are primarily responsible to:

a. Perform yearly a comprehensive service review on the nature, scope and complexity of all outsourcing arrangement to identify, assess and mitigate key risks based on the Outsourcing Management Framework, Policy, Procedures and Guidelines;
b. Assess the OSP's ability to employ a high standard of care in the delivery and performance of the outsourcing arrangements and meet regulatory standards, as if the outsourcing arrangement continues to be performed by the Company;
c. Implement, monitor and maintain effective security and control measures of all risks identified throughout the entire lifecycle of all outsourcing arrangements;
d. Inform Risk and Compliance of any adverse development, significant issues and/or risks arising from its outsourcing arrangements in a timely manner;
e. Ensure that contingency plans (e.g., Business Continuity Plans), based on realistic and probable disruptive scenarios, are in place and tested;
f. Ensure that appropriate and timely remedial actions are taken to address exceptions reported from audits;
g. Comply with all applicable laws, regulations, policies and guidelines;
h. Ensure that the legal and contractual documents for all outsourcing arrangements are in order.
i. Ensure that the OSP cooperates with the relevant competent authority/regulators regarding the outsourced activities, and the Company and the relevant competent authority/regulator have effective access to data related to the outsourced activities, as well as to the business premises of

the service provider, and the relevant competent authority/regulator is able to exercise those rights of access; and

j. Protect customer information against any anticipated threats/hazards to the security/integrity of customer information and against unauthorized access to or use of customer information.

Infra Ops will evaluate OSP's services rendered and their performance through monthly assessment exercise on the "Key Operational Risks & Control" and monthly management reporting.

Infra Ops will ensure completeness of such assessment and timely notification of any deviations, significant issues and adverse developments to Risks and Compliance Team.

4. Outsourcing Management Guidelines

While activities may be outsourced, the Infar Ops must ensure that the outsourced services continue to be managed as if the services were still managed by the Infra Ops.

Infra Ops may be required to modify, make alternative arrangements or re-integrate an outsourced service if:

a. It is unable to manage the risks arising from the outsourcing arrangement in a satisfactory and timely manner;
b. adverse developments that impact the Infra Ops arising from the outsourcing arrangement;
c. the Infra Ops effective access to data related to the outsourced activities, as well as to the business premises of the service provider, and the relevant competent authority/regulator is able to exercise those rights of access are hindered; or
d. The security and confidentiality of customer information is lowered due to changes in the control environment at the OSP.

The Infra Ops must have sufficient manpower resources to manage the outsourcing arrangement.

5. Risk Assessment

The Infra Ops must conduct comprehensive service review on an OSP based on the nature, scope and complexity of an outsourcing arrangement before entering into the outsourcing arrangement.

For ongoing reviews and assessment, the Infra Ops will,

a. Conduct service review which must be re-performed at least once every 12 months.
b. Conduct service review involving the evaluation of all relevant information about the OSP.
c. Ensure that the employees of the outsourced service provider performing any part of the outsourcing arrangement have been assessed to meet the Company's hiring policies for the role they are performing.
d. Perform on-site visits must be conducted at the OSP's processing center to verify the operating capacity, security and control environment as part of pre-outsourcing assessment.
e. On-site visits should be conducted by persons who possess the requisite knowledge and skills to perform the assessment.

6. Approval and Notification

All new outsourcing arrangements must be approved by the Company's BOD and those in relation to provision of Indexes must be made aware to IOSC before the outsourcing contract is signed.

7. Contract Negotiation

The Company must ensure outsourcing contracts

a. protects the Company's interests and include full specifications of functions, relationships, obligations, responsibilities, terms and conditions.
b. must enable the Company to retain an appropriate level of control and meet legal and regulatory obligations.
c. Service Level Agreements ("SLAs") with clearly defined key performance monitoring measures must be established for all outsourcing arrangements.
d. enable the Company to terminate the outsourcing arrangement in the event of default, adverse development, curtailment of the Company or Authority's ability to audit/ inspect the outsourced service provider or circumstances that, in the Company's assessment, could impair the OSP's ability to continue to provide the service in accordance with SLAs.

8. Confidentiality and Security

In protecting and ensuring the confidentiality and security of the Company's information and data, the Company shall,

a. Only disclose customer information to the OSP only on a need-to-know basis.
b. Ensure that the OSP is able to protect the confidentiality of customer information, documents, records and assets.
c. Must consider legal or contractual obligations to notify customers of outsourcing arrangements and the circumstances under which customer information may be disclosed.

9. Implementation

The Company shall maintain the Standard Operating Procedures (SOPs) relating to the outsourced functions and ensure that these SOPs are updated and fulfilled by the outsourced service provider whenever there are changes. Associated risks with outsourcing must be identified and have appropriate security and control measures implemented internally and by the outsourced service provider. Such measures should be commensurate with the nature, scope, complexity and materiality of the outsourcing arrangements.

10. On-going Monitoring and Review

Infra Ops must establish processes and procedures for on-going monitoring of the performance of the outsourced service provider and ensure that SLAs, operational, internal control and risk management standards are met.

When there are intended changes to existing outsourcing arrangements, Infra Ops must review the changes in the outsourcing arrangements and obtain clearance from the relevant subject matter expert (SME), where appropriate.

For outsourcing arrangements due to expire, Infra Ops must:

- Conduct reviews of the outsourcing arrangements before contract expiry; and
- Obtain approval for contract renewal. Approval is required even when the outsourcing arrangements are auto-renewed; or
- Obtain approval for contract termination.

11. Business Continuity Management

Infra Ops must develop business continuity plans (BCPs) relating to outsourcing arrangements to ensure continuation of the Company's business operations in the event of:

- Disruption of outsourcing arrangements; or
- Unexpected termination of outsourcing arrangements; or
- Liquidation of outsources service provider.

Infra Ops must review and update their BCPs every calendar year to ensure continued effectiveness and relevance and must conduct BCP exercises regularly to ensure they are adequately prepared in an event of disruption.

Where relevant, Infra Ops must involve OSP in their BCP tests and participate in the OSPs' BCP tests.

12. Termination

Infra Ops must escalate any adverse or significant development in any outsourcing arrangement promptly to enable management to make informed decisions.

Procedures must be implemented to ensure a smooth transition of the service, either back to the Company or to another third-party service provider, including ensuring that sufficient time and resources are planned.

Infra Ops must ensure that all documents, records and information given to the OSP are promptly returned or deleted, destroyed or rendered unusable upon termination of the service.

13. Outsourcing Reporting

Infra Ops must escalate any adverse or significant development in any outsourcing arrangement promptly to enable management to make informed decisions.

14. Record Retention

Records in relation to the provision of Benchmarks are retained in accordance for at least 5 years or per applicable legal and regulatory requirements.