Summary of Expenditure and Procurement Policy

1 Introduction

This policy sets clear guidelines for budget holders and staff in respect of expenditure and procurement. Adherence to this policy is essential to ensure that 3i consistently operates in a cost-effective manner, maintains the appropriate level of control over expenditure and proactively identifies and manages third-party risks. This policy applies to one off and cumulative spend with a supplier.

2 Procurement

2.1 Procurement principles

Procurement activities involve acquiring goods and services to meet 3i's needs, ensuring compliance with legal and regulatory requirements and following good commercial practices. All staff who undertake procurement activities are responsible for following this policy and the guidelines set out by Group Procurement.

All procurement activity should be conducted in alignment with the procurement principles outlined in figure 1.

Figure 1 - Procurement principles

2.2 Third-party risk management

Maintaining operational resilience to protect 3i's business requires robust risk management. This includes when third-party suppliers are involved in providing services. Effective risk management includes identifying and assessing service and supplier risks, conducting due diligence on proposed suppliers, implementing strong contractual obligations to mitigate risks, and throughout the life of the contract, conducting supplier performance monitoring that is proportionate for the level of risk, as shown in figure 2 below:

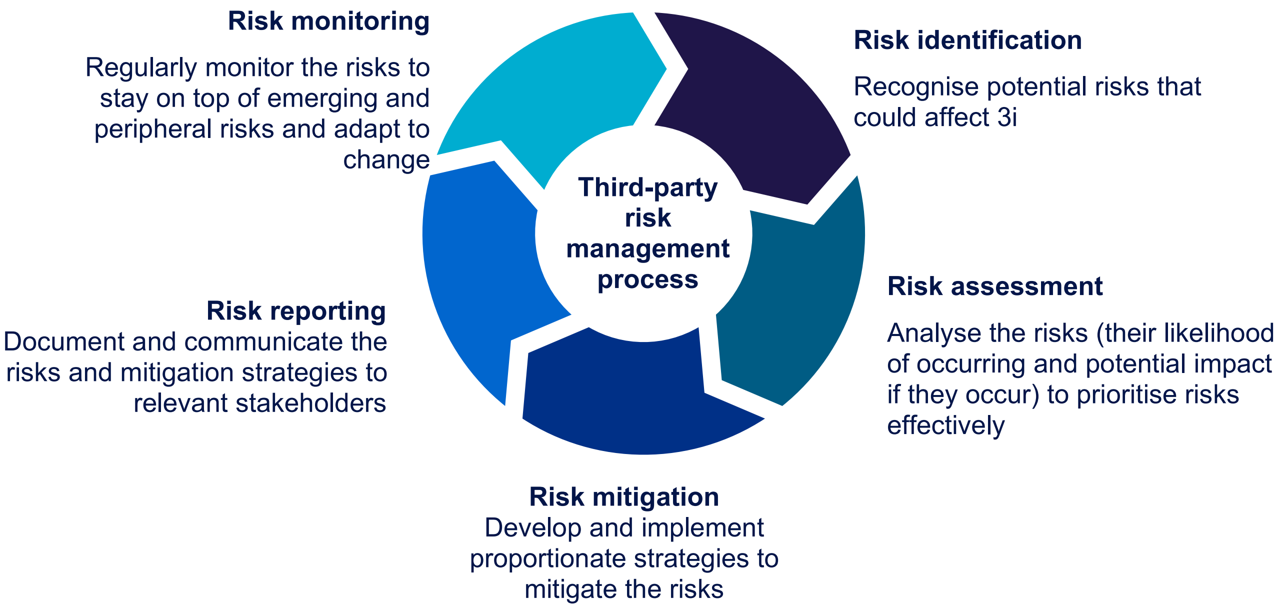

Figure 2 – Third-party risk management process

2.2.1 Risk identification and assessment

The business function is required initially to assess the level of commercial complexity involved in the goods or services being bought. Repeat, low value items or services, being acquired for single use, such as consumables, and travel expenses, do not typically require a formal risk assessment or Group Procurement support. If there is any uncertainty, the business function should consult Group Procurement.

For all other requirements, the business function should undertake a Service Risk Assessment (SRA) prior to engaging with the market, irrespective of the commitment value. The risk outcome of the SRA, considered along with the value, informs the level of Group Procurement oversight of the process. Adequate record of actions undertaken must be retained by the business function. Any risks identified in the SRA, as well as further risks identified in completion of the follow-up action, relevant mitigations, and supplier due diligence are to be captured in the Pre-contract Risk Profile. A copy of the completed SRA and Pre-contract Risk Profile document must be provided to Group Procurement prior to commitment with the supplier to enable comprehensive tracking of third-party risk.

2.2.2 Due diligence on proposed suppliers

Due diligence is the investigation and evaluation of proposed suppliers to verify they are capable of providing the goods or services, are trustworthy, are well-run and able to meet 3i's policies, and are financially robust. An appropriate level of due diligence must be conducted and documented on each of the prospective suppliers, before they are appointed and/or expenditure is committed, to ensure that 3i understands with whom it is trading and to minimise risks to operational resilience.

The appropriate level of due diligence required is proportionate to the output of the SRA assessed risk and determined by the risk owners (Group Procurement, CISO or Group Compliance). However, as a general rule:

- Integrity due diligence must be conducted on proposed suppliers who are considered high risk for bribery, corruption or fraud. See Integrity Due Diligence Procedure (Integrity due diligence procedure)

- Due diligence on information/data/cyber security (including a GDPR Impact Assessment and/or a Systems and Software Security Assessment) must be conducted on proposed suppliers if confidential 3i data will be processed or held by the supplier

- General Data Protection Regulation (GDPR) due diligence must be conducted on proposed suppliers if information about individuals ("data subjects") is transferred. See security and transferring of personal data (Security and transferring of personal data)

- Due diligence on human rights policies, equal opportunity policies and employment policies must be conducted if the proposed supplier is deemed to be at risk in these, with particular focus on the providers' commitments on the use of child or forced labour in their operations or those of their supply chain

- Proposed suppliers must provide evidence to 3i of a modern slavery and human trafficking statement if section 54 of the UK's Modern Slavery Act 2015 applies

- In addition to the above, a proportionate evaluation of environmental impact, health & safety and business resilience must be undertaken. Business resilience considerations might include, for example, financial performance of the supplier, insurance cover, evidence of accreditation(s), evidence of contingency planning, disaster recovery plans and tests, and third-party dependencies

Evidence that the appropriate due diligence activities have been completed (eg email correspondence with the risk owners) should be documented in the Pre-contract Risk Profile and provided to Group Procurement.

Where suppliers do not meet due diligence standards to sufficiently mitigate risk, effective controls are required to be in place through contract terms and governance, or 3i should decide not to proceed with the procurement. The risks associated with using a supplier who does not meet 3i's due diligence standards must be outlined in the Supplier Risk Profile and approved by Group Procurement and the risk owner, prior to finalising the contract.

2.2.3 Establishing efficient prioritisation of suppliers

Under the third-party risk management framework, 3i identifies suppliers that require closer monitoring and management due to their potential impact on the business. By segmenting suppliers into Tier 1, 2 and 3 before the contract is placed, 3i can determine appropriate contract and supplier management actions that need to be put in place within the contract.

It is essential that business functions send Group Procurement the completed SRA and Pre-contract Risk Profile to enable the segmentation to be conducted. Group Procurement will determine the appropriate tier, proportionate to the supplier risk and relationship value, and inform the business function before the contract has been executed, to enable the appropriate governance structure to be agreed with the supplier.

2.3 Managing suppliers

The third-party risk management (TPRM) approach provides a consistent and comprehensive framework for appropriate and efficient management of the relationship, a clear audit trail of assessment and a consolidated overview of the supplier risks throughout the life of the contract.

The appropriate level of management of existing suppliers must be applied to ensure there is sufficient oversight and risks are proactively managed. Business functions should use either the Tier 1 or Tier 2 TPRM Toolkits as advised by Group Procurement to manage their suppliers.

Business functions and Group Procurement will agree the suitable cadence of reviews in the TPRM Toolkit.

2.4 Fraud, bribery and conflicts of interest

3i has zero-tolerance towards fraud, bribery, and corruption. All staff are expected to be familiar, and comply, with 3i's Anti-bribery policy.

Any hospitality or gifts offered to or received from suppliers must be in accordance with the Hospitality and gifts rules.

Any actual or perceived conflict of interest with suppliers must be clearly documented and appropriately managed, see 3i's Conflicts of interest policy.

All staff should report any concerns regarding fraud, bribery, or conflicts of interest in accordance with the reporting a concern page of 3i's Compliance Manual.

Fraud, bribery or conflict of interest inherent risks with particular suppliers (eg sector or geographical risk) should be flagged as a risk in the SRA tool, appropriately mitigated and managed, and documented in the Pre-contract Risk Profile.

2.5 Roles and responsibilities

All staff are responsible for adhering to this policy when conducting procurement activities and maintaining accurate records of decisions and approvals to ensure a clear audit trail.

Business functions are responsible for conducting procurement activities according to this policy, assessing service risks using the SRA tool, performing due diligence in collaboration with other functions, agreeing suitable terms with suppliers, sharing the executed contracts and completed SRA with Group Procurement, liaising with Accounts Payable for new supplier setup, and agreeing the Relationship Manager in line with the governance framework.

Budget holders are responsible for confirming the procurement activities within their budget adhere to this policy, confirming sufficient budget for purchases and approving spend, and referring spend over £100,000 including VAT to the CEO for documented spend approval.

Group Procurement is responsible for procurement activities over £100,000 including VAT or where the SRA indicates high risk, acting to realise contract value and savings, providing advice to business functions and maintaining intranet guidance materials, conducting appropriate due diligence, managing, coordinating appropriate advice on contracts, managing the central register of contracts, SRAs and due diligence, and the creation of the supplier risk profiles, conducting supplier segmentation, and reviewing the supplier spend to ensure that 3i receives good value for money from its suppliers and risks are managed proportionately.

Operations/Service Managers are responsible for regular monitoring and reporting of supplier performance to operational standards, ensuring compliance with regulations and contractual obligations, identifying and mitigating supplier risks, and supporting suppliers to improve service delivery.

Group Compliance is responsible for ensuring this policy is compliant with internal and external requirements, assisting the business function with compliance related due diligence activities and providing contract advice where necessary.

CISO is responsible for assisting the business function with any information security related due diligence activities and accepting the level of mitigated risk.

2.6 Policy governance

The policy will be reviewed on an annual basis. The Head of Property, IT and Procurement will ensure that the organisation is made aware of any updates to this policy.

3 Budget

The annual budget process reflects the resourcing requirements to deliver the strategic plan and is reviewed and approved by the Executive Committee, prior to Board approval before the start of each financial year.

3i employees shall only incur Group expenditure on items where an approved budget exists. Budget holders may only approve expenditure from their budgets within the limits of the expenditure authority delegated to them.

All expenditure equal to or exceeding £100k must be specifically approved by the CEO even if the amount is included in the budget for the year. All non-deal related costs equal to or exceeding £100k must additionally be reviewed by the central Procurement team at the earliest opportunity. For this purpose, deal-related costs are defined as fees directly related to the acquisition or disposal of an investment, which are otherwise approved by the Investment Committee.

The £100k limit is a gross threshold, and approval must be sought where spend equal to or exceeding £100k is expected: on behalf of 3i alone, 3i and its associated funds, and inclusive of appropriate taxes. Approval should also be obtained where individual invoices for a connected piece of work are each below £100k, but the cumulative total is expected to exceed this threshold.

Each budget holder is responsible for monitoring and controlling expenditure against their respective budget. Operating expense performance, including actual spend compared to the approved budget, will be reported by cost centre in the monthly operating expenses report. A summary of operating expenses will also be reviewed by Executive Committee and the Board in the monthly Board report.

Where possible, this approval should be attached to the relevant invoice when sending to the Accounts Payable Team for processing.

4 Expenditure

4.1 Payment practices reporting

On 1 April 2018, 3i plc and 3i Group plc became subject to legislation that requires it to report on payment practices. We are required to report the following:

- narrative descriptions of our payment terms and processes for resolving disputes
- statistics on:
  - average number of days taken to make payments
  - percentage of payments made in 30 days or fewer, between 31 and 60 days and in 61 days or longer
  - percentage of payments not made within the agreed payment period

The information must be reported within 30 days of the end of the relevant 6-month period and is publicly available. Invoices must be sent to Accounts Payable at KRC as soon as they are received.

4.2 Expenditure with KPMG LLP (KPMG)

In line with KPMG's publicly announced policy, 3i will not generally use KPMG for any non-audit services that are not closely related to KPMG's role as 3i's external auditor. This includes investment related services such as due diligence.

All proposals for services with KPMG must be forwarded to the Group Financial Controller in the first instance and will require the approval by the Chairman of the Audit and Compliance Committee above a defined limit and provided the work is not closely related to KPMG's role of 3i's external auditor. Examples of services that require additional approval include:

- The fee exceeds £100,000
- The service is work other than services closely related to KPMG's role as external auditor

In addition, we extend non-audit services restrictions to cover portfolio companies which are deemed as being controlled undertakings of 3i. Group Finance will maintain an up-to-date list of the portfolio companies captured, but these are broadly those portfolio companies where we hold a majority economic interest and which are valued above the level of audit materiality.

These portfolio companies should also not use KPMG for any non-audit services unless KPMG acts as their external auditor and the services directly relate to KPMG's role as their external auditor. 3i will communicate this policy to all of the relevant portfolio companies annually.

Any non-audit services which KPMG provides to 3i and its controlled undertakings, including controlled portfolio companies, will be subject to a cap of 70% of the average audit fee over the previous three years. Group Finance will monitor the total fees for non-audit services in conjunction with KPMG to ensure this cap is not exceeded.

4.3 Expenditure with Deloitte LLP (Deloitte)

From 1 April 2017, Deloitte assumed responsibility for the audit of 3i Infrastructure plc ("3iN"). This impacts contingent fees payable to Deloitte by 3i.

Contingent fees – Deloitte provide due diligence services (ie tax) to 3i where the amount payable is dependent on the outcome of the transaction. Deloitte are able to provide this service to 3i as long as the work on the transaction would not subsequently be reviewed as part of their audit work on 3iN.

Deloitte must confirm that the work will not impact their own audit work on 3iN before any due diligence engagement is accepted. This must be sent to the Group Financial Controller prior to the work commencing.

In addition, no Deloitte staff may be seconded to 3i Group.