REQUEST FOR PROPOSAL:
EMINVEST DATA PARTNER

TABLE OF CONTENTS

TERMS OF REFERENCE

1. INTRODUCTION

EMInvest is an investor-led initiative to build an anonymised database of realised private investment performance in emerging markets and developing economies (EMDEs). It is a database platform that pools confidential, transaction-level data contributed by commercial banks and asset managers, and turns it into comparable, anonymised risk and performance benchmarks that the wider market can use. The initiative is convened by Systemiq, funded by the Government of Norway, and in partnership with the UK Foreign, Commonwealth & Development Office EMDE Investor Taskforce.

This RfP seeks a long-term partner across two phases: first, to design and build the EMInvest platform; and second, to operate it on an ongoing basis, including running the annual data submission process.

2. ABOUT SYSTEMIQ

EMInvest is convened by Systemiq, a global advisory and investment firm specialising in systems change with a focus on sustainable finance. Systemiq brings experience in climate and development finance in emerging markets and a track record of building collaborative, market-shaping initiatives, including the Blended Finance Taskforce and contributions to the broader international climate finance agenda. Its combined capabilities across finance, data analytics and coalition-building position it to convene the public and private institutions involved and to coordinate delivery of the initiative.

Systemiq currently holds the secretariat role for EMInvest through the build and MVP phases. EMInvest is designed to transition over time to a long-term institutional host who will take over Systemiq's role, with a sustainable governance and funding model intended to ensure long-term operation and growth, in a not-for-profit arrangement that ensures the database is operated according to its mission, with outputs made as widely accessible as possible consistent with data security. The Data Partner appointed under this RfP may transition the engagement from Systemiq to the future long-term institutional host. The host could be the same organisation as the Data Partner long-term, subject to the fulfilment of host criteria.

3. CONTEXT

EMDEs are projected to contribute 65% of global economic growth over the next decade[1], growing at twice the rate of the US and EU over the next five years[2], yet private capital remains constrained by persistent information asymmetry[3]. Private financing costs remain 2-7 times higher in EMDEs than in advanced economies, deterring capital flows. A key driver is the absence of transparent, comparable data on realised investment performance, preventing investors, regulators and rating agencies from pricing risk effectively and for institutional investors to build a credible business case for capital allocation to EMDE markets. The result is that EMDE corporates and projects are often benchmarked to sovereign risk regardless of their underlying fundamentals, leading to systematic overestimation of

---

[1] S&P Global (2024) Emerging Markets: A Decisive Decade
[2] IMF (2026) World Economic Outlook
[3] World Economic Forum (2025) From Risk to Reward: Unlocking Private Capital for Climate and Growth

risk, inflated risk premia, and missed investment opportunities. As a result, global investors are leaving returns on the table and under-allocating to EMDE opportunities.

The Global Emerging Markets Risk Database (GEMs) has demonstrated the transformative power of data transparency, already disproving prevailing risk assumptions and contributing to S&P revising its treatment of MDB portfolios, freeing up an estimated $600–800 billion in additional lending headroom over the next decade (CGD, 2025). Yet GEMs is limited to MDB/DFI data and not accessible to private investors. At the same time, around 70% of private investors surveyed by GEMs report dissatisfaction with the current availability of EMDE private credit data. (GEMs, 2024).

This initiative addresses this gap by building an anonymised, investor-led database of realised private-sector investment performance in EMDEs. Drawing on transaction-level data contributed by domestic and international investors, the platform will generate comparable benchmarks on default and recovery rates, returns, pricing, and deal structures. By converting private data into aggregated market insights, it will support asset owners and managers, banks, credit rating agencies, and regulators in making informed decisions.

4. BRIEF DESCRIPTION OF THE REQUIRED SERVICES

EMInvest is an initiative bringing together private sector financial institutions to share and aggregate the performance of their investments in emerging markets and developing economies (EMDEs). The initiative is in its design phase: building a coalition of contributing institutions and consulting them, alongside other experts, to define the product and requirements. EMInvest is now seeking a Data Partner to build a database platform for the initiative, based on the design work already undertaken.

The Data Partner is a third-party service provider that will develop a platform that collects and aggregates contributors' individual data to produce the anonymised risk and performance statistics, which EMInvest will publish on the EMInvest platform, and high-level benchmark reports, which will be shared publicly.

This call for tenders is to award a contract to a Data Partner that will support EMInvest across the full set of data activities, including product development, data collection, transformation, quality control, reporting and analytics, using a secure environment and modern IT tools. The Data Partner will be responsible for developing the database platform and, once it is live, for managing the recurring annual data submission and analytical reporting process.

The Services shall be provided in compliance with the requirements set out in Annex A – Technical Specifications. We will, however, accept an alternative delivery model where a bidder proposes to meet EMInvest's requirements outlined in Annex A by building on, adapting or extending an existing product or platform of its own, rather than by building a new standalone platform. This recognises that an established organisation may be able to deliver the outcome more quickly or sustainably through infrastructure it already operates.

4.1. Proposed Timing

- Activity 1: September 2026 – October 2026
- Activity 2: October 2026 – December 2026
- Activity 3: January 2027 – June 2027
- Activity 4: June 2027 – November 2028

5. PROCUREMENT PROCEDURE AND TIMETABLE

5.1. Procedure

EMInvest is convened by Systemiq and funded by the Government of Norway. Systemiq will act as the contracting authority for this procurement and will be the counterparty to the resulting services contract through the build and MVP phases. Once a long-term institutional host has been established, the parties may agree to renew the contract on the same terms with that host, and the host will assume the role of contracting counterparty in place of Systemiq. The host could be the same organisation as the Data Partner in the long term, subject to the fulfilment of host criteria.

The RfP and the associated contract will be structured around the four activities, with a formal approval gate at the end of each, as described in the Scope section. Progression beyond each activity is at the contracting authority's discretion: the authority reserves the right not to proceed to a subsequent activity, or to pause the engagement, at any activity. Bidders are asked to price all four activities in their proposal, on the intended basis of a fixed price per activity. Pricing requirements are set out in the Budget section.

Procedure	Open
Expected Start	September 2026
Type of Contract	Services Contract
Number of envisaged operators	One
Duration	2 years and 4 months The engagement spans all four activities. Activities 1 to 3 (final product development plan through final product) run from contract start to the public launch of the platform (June 2027). Activity 4 runs for an initial term 1.5 years from go-live.
Lots	This call for tenders is not divided into Lots
Variants	Not permitted but an alternative delivery model as described in Annex A, Section 2: Alternative Delivery Model is allowed. Proposals are assessed on their ability to deliver the required outcomes and services.
Consortia	Permitted but must be clearly described in proposal. A consortium must nominate a single lead partner that will hold the contract and remain fully accountable for delivery. Any change to the composition of the team after award requires the contracting authority's prior written approval.
Subcontracting	Permitted but must be clearly described in proposal. Any change to the composition of the team after award requires the contracting authority's prior written approval.

5.2. Procurement Timetable

All times are UK time. Questions and the single point of contact for this procurement are set out in the Proposal format and submission requirements section.

Milestone	Date
RfP issued	17 July 2026
Expression of interest deadline	24 July 2026
Deadline for clarification questions	24 July 2026
Consolidated responses to questions published	31 July 2026
Proposal submission deadline	7 August 2026
Evaluation of written proposals	21 August 2026
Clarification interviews with shortlisted bidders	24-25 August 2026
Award notification	26 August 2026
Contract signed	Early September
Contract start	Early September

6. FINANCIAL PROPOSAL

Bidders may use their own template(s), provided that the Financial Proposal is complete and consistent. At a minimum, it must include the **three schedules** specified below. All schedules must reconcile fully to the same Total Proposal Price.

1) An **activity- & deliverable-based budget**, following the Technical Specifications as described in Annex A:
    a. A fixed price for each of Activities 1 to 3
    b. A fixed annual price for Activity 4 (for the purposes of ensuring comparability between proposals, the expansion of product features workstream within Activity 4 should be priced on the basis of 60 days of engineering work per year)

2) A **cost-category-based budget**, breaking down and quantifying, as appropriate, the prices stated in (1) above, including but not limited to:
    a. Personnel (name/role/title, daily rate, estimated number of days, etc.)
    b. Travel & expenses (unit costs x number of units for travel, technology costs, etc.)
    c. Third party costs (unit costs x number of units for consultants, subcontractors, etc.)

3) A **payment schedule** linked to the completion and acceptance of activities & deliverables as specified in Annex A: Technical Specifications. The proposed allocation of payments must reasonably reflect the level of effort associated with each activity/deliverable. Schedules that are materially inconsistent with the Technical Proposal (e.g. artificially front-loaded) may be rejected (or be subject to clarification in accordance with the rules stated here before being scored in the evaluation).

<u>Other Pricing Requirements</u>:

- **No maximum budget or indicative budget range will be disclosed as part of this procurement**. Bidders shall submit a realistic, competitive, and comprehensive Financial Proposal that is consistent with the proposed scope of work & delivery approach, and the required quality standards.

- All prices, rates and totals shall be quoted in **GBP**.
- The Total Proposal Price shall be **fully inclusive of all costs required to perform the Services, including VAT and other applicable taxes**, **which should be stated/shown separately** in the Financial Proposal tables. Systemiq Ltd is based in the UK and is not VAT exempt. For financial evaluation purposes, Systemiq will use the total cost to Systemiq, including any VAT or other taxes that Systemiq cannot recover.
- Each Bidder shall bear its own costs of preparing and submitting its proposal. **Systemiq will not reimburse proposal preparation or submission costs.**

7. GUIDELINES FOR PROPOSAL SUBMISSION

7.1. Eligibility criteria

By submitting a proposal, tenderers confirm they are in agreement with the contracting terms (*Section 9*) and none of the below apply to them:

i) They are bankrupt or is being wound up, whose affairs are being administered by court, has entered an arrangement with creditors, has suspended business activities or is subject of an injunction against running business by court.

ii) They are the subject of proceedings for a declaration of bankruptcy, for an order for compulsory winding up or administration by court, or for an arrangement with creditors or of any other similar proceedings.

iii) They have been found guilty of grave professional misconduct by any means which the grant recipient can justify.

iv) They are not registered in a national official register or registered for declaration and payment of tax in accordance with national legislation.

v) They have not fulfilled obligations relating to payments of taxes or social security contributions.

vi) They or persons having powers of representation, decision-making or control over them have been convicted for fraud, corruption, involvement in a criminal organisation or money laundering.

vii) They or persons having powers of representation, decision-making or control over them have been convicted of an offence concerning their professional conduct

7.2. Ethics & Sustainability

Applicants and tenderers shall observe the highest standards of ethics during the procurement and execution of contracts. This shall always include:

i) Respecting minimum ILO standards such as the respect of working conditions and avoidance of child labour.

ii) Respecting basic social rights and environmental aspects.

iii) Having zero-tolerance for corruption and financial irregularities.

iv) Having zero-tolerance for inaction to sexual exploitation, sexual abuse, and sexual harassment (SEAH).

7.3. Requirements

The assignment requires a firm or consortium with expertise in:

- Designing, building and operating secure data platforms of comparable scale and sensitivity, evidenced by at least two comparable assignments in the last three years;
- Handling and safeguarding highly sensitive financial data;
- Standing in the market, demonstrated through recent clients, customers or data contributors;
- Domain familiarity with credit risk and/or private investment.

7.4. Proposal Content

Applicants should submit:

- Statement of interest, including relevant experience;
- Proposed methodology and work plan (max 5 pages);
- Budget / Financial Proposal in GBP
- CVs of team members;
- Examples of similar assignments;
- Two references;
- Proof of registration, tax compliance, and absence of debts to satisfy donor compliance requirements

7.5. Expression of Interest (EOI), Deadline for Questions and Proposal

Submission of an Expression of Interest (EOI) and any related communications are non-binding, do not constitute an offer capable of acceptance, and do not create any contract or other legal obligation on the part of the procuring entity/contracting authority. Systemiq may amend, suspend, or cancel the EOI process at any time and reserves the right to reject any or all EOIs, without obligation to proceed, shortlist, invite tenders, negotiate, or award any contract. Respondents participate at their own cost and risk, must make their own enquiries, and may not rely on any information provided; Systemiq disclaims all liability for reliance or use of such information to the extent permitted by law. Any contract will arise only upon execution of a definitive written agreement.

All expressions of interest should be received *by 24 July 2026 at 18:00 BST,* and subsequent questions about this RFP must be received via email to the contact below by *24 July 2026 at 18:00 BST*. The primary contact details are:

Name: Daisy Ferleger

Email address: emde.data@systemiq.earth

With the subject title: EMInvest RFP – Data Partner

Answers to the questions will be shared with all parties who have asked questions or otherwise expressed interest in the RFP.

All proposals must then be sent by *7 August 2026 at 18:00 BST* in electronic format to the same contact listed above.

8. Evaluation and award criteria

8.1. Evaluation Criteria

Eligibility is first checked on a pass/fail basis (see Eligibility and submission requirements). Only proposals that pass proceed to scored evaluation. Eligible proposals are then scored on the elements below, a maximum of 100 points will be awarded. A minimum score is required on certain sections: a proposal that does not meet the stated minimum for a section will be excluded from further consideration, regardless of its total score. Proposals will be evaluated against the following criteria:

#	Award criteria	Max score	Min score required
1	**Technical proposal**	**30**	**15**
1.1	Quality and credibility of the proposed approach, methodology and work plan across the four activities, including the method for the final product development plan activity, the approach to data security, infrastructure and software development, and the realism of the work plan against the gates and launch milestones, with particular emphasis on the ability to build secure, financial-grade infrastructure capable of handling highly sensitive data	15	n/a
1.2	Quality of the proposed approach to the ongoing management and operation of the platform, including data submission processes, quality control and validation	15	n/a
2	**Qualification and experience**	**30**	**15**
2.1	Relevance and appropriateness of the proposed team based on qualifications, skills and professional experience, and split of responsibilities, in particular a strong software development team with demonstrable experience delivering and operating financial-grade, secure data platforms	15	n/a
2.2	Track record of the firm on comparable assignments; relevant domain expertise in credit risk and/or EMDE investment with experience implementing complex domain methodologies; ability to contribute or mobilise relevant data that would strength the platform’s coverage, subject to necessary rights and contributor consent	15	n/a
3	**IT Security and Business Continuity Management**	**20**	**10**
3.1	Robustness of the proposed approach to IT security, disaster recovery and business continuity, including the quality of supporting documentation and evidence of relevant standards and certifications	10	n/a
3.2	Efficiency of the proposed approach and standards to ensure data confidentiality and anonymity and restricted access to the data and platform	10	n/a

4	**Financial proposal**	**20**	**n/a**
4.1	Total cost, priced per activity, assessed on value for money. The lowest compliant price receives the maximum score; other tenders are scored pro rata (lowest price ÷ tender price × 20)	20	n/a
	Total	**100**	**40**

9. CONTRACTING TERMS

The full terms are set out in the draft contract (Annex C) and the funder requirements (Annex B). By submitting a proposal, tenderers agree to the following terms:

- **Intellectual Property Rights** means patents, utility models, rights to inventions, copyright and neighbouring, related and associated rights, moral rights, trade marks and service marks, trade names, business names and domain names, rights in get-up and trade dress, rights in goodwill and the right to sue for passing off, unfair competition or similar causes of action, rights in designs, rights in computer software, database rights, rights to use, and protect the confidentiality of, confidential information (including know-how and trade secrets), and all other intellectual property rights, in each case whether registered or unregistered and including all applications and rights to apply for and be granted, renewals or extensions of, and rights to claim priority from, such rights and all similar or equivalent rights or forms of protection which subsist or will subsist now or in the future in any part of the world.
- **Ownership.** The right of ownership of Intellectual Property Rights procured or developed by the Partner may be vested in Systemiq, unless otherwise stated in the Subcontract.
- **Public accessibility and public domain**. Intellectual Property Rights financed in whole or in part from this Subcontract shall, in the spirit of securing such rights as a common global good, be managed to maximise public accessibility and allow the broadest possible use. Deliverables and/or EMInvest produced as a result of this Subcontract shall, as far as possible and appropriate, be placed in the public domain for non-commercial use.
- **Contributor data.** All data, content and other materials provided or made available by contributors in connection with the Services (**Contributor Data**) shall remain the property of the relevant contributors at all times. The Partner shall process Contributor Data solely on Systemiq's documented instructions and only to the extent necessary to perform the Services, and shall not use, disclose, sell, licence, exploit or otherwise process Contributor Data for any other purpose. Except for the limited right to process Contributor Data strictly in accordance with this clause and the Contract, the Partner acquires no right, title or interest (including any intellectual property rights) in or to any Contributor Data. Any primary Data, raw Data and any associated metadata that is classified as confidential by a Contributor Data and provided to the Partners in connection with this Agreement shall (a) be treated as confidential by the Partner, and (b) remain aggregated and anonymised at all times when used, disclosed or published in connection with this Agreement
- **Changing the work.** Systemiq may reasonably vary the scope, focus and priorities of the Services within the overall scope of the requirements of the engagement. Any change that materially affects the cost, resourcing or timetable/phases will be implemented only through the parties' written change control procedure (and no such change is effective unless agreed in writing
- **Termination.** Systemiq may terminate the engagement for convenience with effect from the end of any project stage by giving the Partner written notice. In addition, Systemiq may terminate the engagement immediately (or on such shorter notice as it specifies) at any time if project funding is reduced, suspended, or withdrawn, including by the relevant funder. On termination, the Partner shall be entitled only to payment for Services and Deliverables

properly performed and accepted by Systemiq up to the effective date of termination, and no payment shall be due for unperformed work; to the fullest extent permitted by law, Systemiq shall have no liability for any loss of profit, anticipated savings, or any indirect or consequential loss. Following termination, the Partner shall promptly deliver to Systemiq all work-in-progress, materials, and Deliverables (whether complete or not) and shall provide reasonable transition assistance on request.

ANNEX A: TECHNICAL SPECIFICATIONS

1. BACKGROUND

The EMInvest Performance Database is in the design phase. The outcome of this procurement is a secure, web-based platform (the "EMInvest Platform") that collects confidential, contract-level investment performance data from commercial contributors, validates and aggregates it, and produces anonymised risk and performance benchmarks for EMDEs.

The procurement covers two things: 1) building and architecting the EMInvest Platform, and 2) operate it on an on-going basis. Operation means running EMInvest as a service by operating a recurring submission cycle, maintaining a cumulative multi-year database, and serving outputs to defined user groups on controlled terms. The platform must be setup in the most secure IT environment possible given the highly sensitive and confidential nature of the data within.

The Services outlined in this Technical Specification are to be delivered in close coordination with Systemiq, and under its general supervision, in its capacity as secretariat of the initiative.

2. ALTERNATIVE DELIVERY MODEL

We will accept an alternative delivery model to the activities outlined below where a bidder proposes to meet EMInvest's requirements by building on, adapting or extending an existing product or platform of its own, rather than building a new standalone platform. This recognises that an established organisation may be able to deliver the outcome more quickly or sustainably through infrastructure it already operates. Any such delivery model must deliver the same outcome and scope of services set out in the Description of Services.

Any such model must also: preserve EMInvest's distinct mandate, governance principles and contributor relationships, and maintain a recognisable EMInvest identity; keep contributor data logically separated and protected to the standards in the IT Security section.

3. DESCRIPTION OF SERVICES

3.1. Overview

The work will be delivered across four activities (see 2.2). Activities 1 to 3 (final product development plan, MVP development, feedback integration and final product build) are sequential and gated: each must be completed and approved before the next begins. Activity 4 (operation and maintenance) begins once the platform goes live, then runs continuously for the remainder of the contract.

Each is set out below with its description, deliverables and gate decision. The responsibilities in 2.2 apply across all activities and are not repeated under each.

3.2. Responsibilities

The following responsibilities apply throughout the engagement, across every activity. Where one has a specific expression in an activity (for example, anonymisation is designed in Activity 1, built in Activity 3 and run in Activity 4), the activity refers to it rather than restating it.

Platform maintenance, availability and security. The partner shall:

- Keep the platform and all of its environments (build, test and production) secure, maintained and available at all times, to the standards in IT security section;
- Monitor the platform continuously and respond to faults, incidents and outages within the agreed response times (see Performance standards);
- Apply dependency updates and upgrades promptly, and manage vulnerabilities on an ongoing basis;
- Maintain regular backups and tested recovery procedures;
- Conduct periodic security reviews and keep the platform prepared against evolving threats; and
- Sustain the platform's performance and reliability as data volumes and the user base grow.

Confidentiality and data protection. The partner shall:

- Confidentiality: keep all Contributor Data and EMInvest information confidential and use it only to perform this Agreement, restricting access to personnel/approved subcontractors on a need-to-know basis under written confidentiality obligations.
- UK GDPR / DPA 2018 (processor): where processing Personal Data for EMInvest, act as processor and process only on EMInvest’s documented instructions and in accordance with the UK GDPR and Data Protection Act 2018.
- Cyber Security: implement and maintain appropriate technical and organisational measures to protect the data and EMInvest information against unauthorised/unlawful processing, loss, destruction or damage, aligned to EMInvest’s cyber security requirements and proportionate to risk.
- Data location: store and process the data only in the locations agreed in writing with EMInvest and not transfer it elsewhere without EMInvest’s prior written approval and appropriate UK GDPR safeguards.
- Subcontractors: not appoint any subcontractor with access to the data/information without EMInvest’s prior written approval, and ensure equivalent contractual confidentiality, data protection and security obligations; the Partner remains liable for subcontractors.
- Incidents/breaches: notify EMInvest without undue delay (and in any event within [24] hours) of any actual or suspected security incident or personal data breach affecting the data/information, and promptly assist EMInvest with investigation, containment, remediation and any required notifications.

Methodology integrity and independent validation. The partner shall:

- Work with the EMInvest team and its advisers to finalise the methodology, which is in draft and being designed with expert input, and translate into the technical implementation;
- Implement the analytical methodology, as agreed with EMInvest and its advisers;
- Keep the methodology and its implementation documented, transparent and inspectable;
- Support independent validation of the methodology and its implementation, rather than self-certifying its own work;
- Make no change to the methodology without EMInvest's prior written approval; and
- Advise on potential enhancements based on experience and best practice, for EMInvest to approve.

Stakeholder engagement, governance and reporting. The partner shall:

- Identify a single point of contact for all operational and administrative communication with EMInvest;

- Work in close coordination with, and under the general direction of, the EMInvest team and its advisers;
- Engage with the adviser group and contributors as required for the work;
- Prepare for and participate in EMInvest meetings and working groups, and follow up agreed actions;
- Report progress, risks and issues against the plan and the activities at an agreed cadence; and

Documentation and handover-readiness. The partner shall:

- Produce and keep current the technical documentation, user and submission guides, methodology documentation and an administration manual;
- Document the architecture, code, data model and operational procedures to a standard that allows another competent operator to take the platform over;
- Prevent avoidable lock-in to proprietary components, and disclose all third-party and open-source dependencies;
- Maintain the documentation continuously, not only at the end of an activity or the contract; and
- Support the transfer of the platform, code, data and documentation at the end of the contract, providing knowledge transfer and reasonable cooperation.

3.3. Activities

Activity 1: Final product development plan. Close any open questions or gaps in the proposal product plan through research, design work, and stakeholder engagement where needed. The final plan is to be presented to EMInvest for sign off before development begins.

The partner shall:

- Support the review of the existing draft analytical methodology, data template, user groups, user research, and access principles provided by EMInvest, and finalise with research, technical discovery and any further user or contributor consultation;
- Produce a finalised product requirements and functional specification covering the data model, submission workflow, validation and QA, anonymisation and disclosure control, analytics and metrics, access tiers and outputs, user interface, and integrations, translating and operationalising methodology into product workflows;
- Define the technical architecture and the data-security design, including the hosting approach, environments, access control and data flows;
- Define and prioritise the MVP scope, being the features to be built and tested in Activity 2, with the rationale for that prioritisation;
- Propose the acceptance criteria for the MVP and final-product gates;
- Produce a delivery plan with milestones, resourcing and the proposed team; and
- Consolidate the above into a single proposal

Deliverables:

- Findings from the partner's own gap-filling research and design work
- Confirmed product requirements and functional specification
- Technical architecture and data-security design
- Prioritised MVP scope (the features to be built and tested in Activity 2)
- Delivery plan, milestones, proposed team

Outcome: EMInvest team reviews and approves the product development plan.

1. **Activity 2: MVP development**

Build a working minimum viable product containing the core set of platform features. This will provide the basis for user testing and refinement, ensuring that the core design assumptions are validated with real contributor data and feedback before the full build. The MVP 'core set of platform features' will contain, but not limited to, an end-to-end process from data submission to user-facing output data and visualisations, according to the set methodology developed in partnership with the EMInvest team.

The partner shall:

- Stand up a secure environment for the MVP capable of handling real contributor data, in line with Annex B;
- Build the MVP product covering the prioritised features;
- Implement the data template and submission workflow for the MVP scope;
- Implement the methodology to the extent the MVP scope requires, with the EMInvest team and its advisers validating the implementation;
- Develop, in partnership with the EMInvest team, the methodology and user submission guide;
- Onboard the MVP contributor(s) [to be confirmed] and support them through a live submission, approximately 5-10 organisations;
- Test and validate the MVP end to end, including data ingestion, the validation rules, anonymisation and disclosure control on real data, and output generation;
- Document the test and validation results, setting out what worked, what did not, and the recommended refinements;
- Update the specification for the final product to reflect the MVP lessons.

Deliverables:

- Working MVP product covering the prioritised features
- Methodology and user submission guide, developed in partnership with the EMInvest team
- Test and validation results, setting out what worked and what did not
- Updated specification for the final product, reflecting the MVP lessons

Outcome: EMInvest decides whether the design assumptions have been validated, whether the refinements are acceptable, and whether to proceed to the full build. If they have not been validated, the MVP may be reopened or the engagement stopped.

2. **Activity 3: Feedback integration and final product build**

Deliver the full platform build to the agreed specification, incorporating the feedback and refinements from the MVP testing.

The partner shall:

- Build the full platform to the agreed specification, including secure hosting, the submission workflow, the validation and QA engine, anonymisation and disclosure control, analytics and metric generation, access tiers and user management, outputs and reporting, the user interface, and the agreed integrations;
- Implement and embed the full analytical methodology;
- Complete the technical documentation, user and submission guides, methodology documentation and administration manual, in partnership with EMInvest;
- Conduct acceptance testing against the agreed criteria, including security and penetration testing in line with IT security (Section 4);

- Configure the platform for live use, and support the onboarding of contributors at scale; and
- Support the beta release and the public launch milestones.

Deliverables:

- The full platform built to the agreed specification, including secure hosting, the submission workflow, the QA and validation engine, anonymisation and disclosure control, analytics and outputs, access tiers and the user interface (per Annex A)
- Technical documentation, user guides and embedded methodology, developed in partnership with EMInvest
- Acceptance testing against the agreed criteria
- A launch-ready platform supporting the beta and public launch milestones

Outcome: The platform is assessed against the agreed acceptance criteria. EMInvest signs off for go-live, or specifies remediation to be completed before go-live.

3. Activity 4: Operation

Running of the EMInvest platform as a live service, maintaining and upgrading the product, running the annual, recurring submission cycle, performing quality assurance and validation, generating the statistics and benchmarks. The first year (June 2027 – May 2028) of the database operation will involve continuous onboarding of all of the data contributors and users, with the following years (June 2028+) involving onboarding only new participants. The partner operates the service. EMInvest provides governance and oversight, owns the contributor relationships, and directs the priorities for outputs.

The partner shall:

- Maintain the product
  - Host the platform in a secure, ring-fenced environment, ensuring its continued access, functionality and availability;
- Support expansion of the product features
  - Design, build, test and integrate enhancements (e.g. enhanced analytics, reporting formats or user-facing tools) into the live platform for a cost of **60 days per year of development work**
  - Maintain a product roadmap with EMInvest reflecting agreed priorities;
  - For each agreed enhancement or extension, scope and cost it against the day-rate card and obtain approval before building it;
  - Update the documentation for each change.
- Operate the data submission process
  - Manage user access, including setting up and maintaining credentials for contributors and other user types, reviewing their technical requirements, and enforcing the tiered access rules;
  - Plan and run the recurring submission cycle, expected to operate annually, to meet publication deadlines, including opening each cycle, managing the timeline, and supporting contributors through submission, with a group of approximately 10-15 organisations;
  - Provide ongoing technical and subject-matter support to contributors during and between cycles;
  - Check the quality of and validate the input data with a validation process developed in partnership with the EMInvest team and its advisers;
  - Run regular and ad-hoc routines to produce the aggregated statistics and benchmark outputs, and validate the output statistics with EMInvest;

- Prepare and circulate, at the end of each cycle, a data quality assurance report setting out the key results;
- Draft, produce and publish the EMInvest publications (tables, graphs and text) as agreed with EMInvest; and
- Support EMInvest governance, including preparing for and participating in meetings and working groups and following up agreed actions.

Deliverables:

- A live service meeting the agreed availability standards
- Each recurring submission cycle, expected to operate annually, run end to end, with contributor support and access management
- A data quality assurance report each cycle
- Aggregated statistics and benchmark outputs

Outcome: The platform is maintained and data submission and analysis managed by the partner until the end of the contract period.

4. FUNCTIONAL AND TECHNICAL REQUIREMENTS

This section describes the platform this procurement aims to build: who it serves, what it must do for them, the modules required to deliver that, and the requirements that cut across all of them. The detailed disclosure rules, methodology and data template are provided as inputs and refined in the final product development plan (Activity 1).

4.1. Who the platform serves

EMInvest closes a specific gap. There is no shared, credible source of contract-level risk and performance data for private investment in EMDEs. The platform pools confidential data from lenders, anonymises it, and returns benchmarks that no single contributor could produce alone. It is complementary to GEMs, covering the private investment activity that GEMs does not.

A single product must serve five user groups, each with a different job:

- Contributors (lenders): submit contract-level data and, in return, see aggregated benchmarks and their own portfolio set against the anonymised market;
- Other paying members (institutional investors, asset owners, CRAs, regulators): use benchmarks and breakdowns to calibrate and evidence ratings, justify and size allocations to EMDEs, etc
- The public: access the agreed aggregate statistics in the form of summary reports.

A controlled route may also support external access for research and analysis, for example by academics. This is subject to agreement from the data contributing members.

The design implication is that the same anonymised dataset will serve different decisions, from pricing a single deal to justifying a portfolio allocation, with each group seeing only what its tier and the disclosure controls allow.

4.2. What the platform does

The platform runs one data journey, repeated each submission cycle:

1. Contributors submit contract-level data through a secure web application;
2. The platform validates each submission and returns clear errors for correction;

3. Validated data enters a cumulative, multi-year database, with contributor identifiers encrypted on ingestion;
4. The platform applies the embedded EMInvest methodology to compute risk and performance metrics;
5. Disclosure controls are applied so that no contributor or transaction can be re-identified;
6. Each user group receives outputs on controlled terms, according to its tier.

The modules in 3.3 are the components that deliver this journey. The requirements in 3.4 apply across all of them.

4.3. Modules

4.3.1. Data model and storage

Holds the contributed data and the cumulative record that makes benchmarking over time possible.

The platform must:

- Store contract-level data in an appropriate schema, structured on the Excel-based EMInvest data template;
- Encrypt or pseudonymise contributor identifiers on ingestion, so that stored data cannot be traced to a contributor;
- Maintain a cumulative, multi-year database that tracks the status of contracts and defaults over time;
- Be extensible to new data types, asset classes and contributor segments as coverage grows, without re-architecting.

4.3.2. Submission workflow

The process by which contributors enter and submit their contract-level data to the platform, designed to minimise the reporting burden on data-contributing members. The platform must:

- Allow contributors to submit data securely through the web application, with submissions mapped into the database and made available for validation;
- Support submission by completed Excel template at launch
- Be designed to accommodate additional submission routes over time, for example direct entry, bulk or API-based submission, which the partner should explore and propose as part of the final product development plan;
- Support a recurring submission cycle, with the ability to open and close cycles, accept resubmissions, and version submissions so the audit trail is preserved;
- Confirm receipt and submission status back to the contributor.

4.3.3. Validation and quality assurance

Identifies errors so the database is robust and contributors can self-correct without manual back-and-forth.

The platform must:

- Run automated validation checks on each submission against the template's rules, covering format, completeness, valid values and internal consistency, before data is accepted into the database;
- Return clear, specific error and warning feedback to the contributor, identifying what failed and where, so they can correct and resubmit without manual back-and-forth;
- Distinguish blocking errors from warnings, and allow controlled resubmission;
- Keep a record of validation outcomes for each submission;

- Support the secretariat's own quality review on top of the automated checks.

4.3.4. Anonymisation and disclosure control

The mechanisms by which contributor and transaction-level data are anonymised and aggregated before being shared. The platform must:

- Apply aggregation thresholds and statistical disclosure-control rules to every output, so that no individual contributor or transaction can be re-identified, with the thresholds designed and tested in consultation with the EMInvest team and its advisers;
- Suppress, mask or further aggregate cells that fall below the disclosure thresholds
- Enforce these controls consistently at the point of query and output, across all access tiers, including any granular or ad-hoc access;
- Implement the detailed disclosure rules and thresholds, provided as an input and refined as part of the final product development plan (Activity 1), in a way that the secretariat can adjust under governance.

4.3.5. Analytics and metrics

Turns the pooled data into the benchmarks users require.

The platform must:

- Compute the EMInvest metric set by applying the embedded methodology, including default rates, recovery rates, pricing and return measures;
- Produce these metrics across the agreed breakdowns, for example by country, region, income group, sector, project type and seniority;
- Generate the regular outputs for each cycle;
- Produce results that are reproducible and traceable to the methodology and the underlying cohort;
- Embed the methodology so that it is inspectable, can be independently validated, and changed only under governance.

4.3.6. Access tiers and outputs

Serves each user group (3.1) what it is entitled to, and no more.

The platform must:

- Enforce role-based access, so each user group sees only the outputs its tier entitles it to, consistent with the access model and disclosure controls;
- Let users view, filter and export the outputs they are entitled to, through dashboards and benchmark views;
- Provide contributors with a self-service facility to download their own data with the methodology applied, so they receive their position set in the anonymised market context;
- Support controlled access for further research and analysis, for example by academics;
- Publish the agreed aggregate statistics to the public through the platform.

4.3.7. Admin and secretariat portal

Gives the secretariat control of each cycle and oversight of quality and release.

The platform must provide a back-office interface for the EMInvest team to:

- Monitor the progress of each submission cycle and the status of each contributor's submission;

- Review submissions and validation results, and raise or resolve data-quality queries with contributors;
- Manage users, roles and access entitlements;
- Configure validation rules, disclosure-control parameters and reference data without a new release wherever practical;
- Review and approve outputs before they are released or published.

4.3.8. Integrations

Enables users to access the data in other workflows. The platform should provide at minimum:

- Provide export in standard, widely usable formats;

In addition, and based on the outcomes of user research:

- Offer programmatic access (an API) for higher-tier users, as reflected in the access model;
- Be capable of future integration with end-user platforms used by the target audiences, for example market-data and portfolio systems, which the partner should assess during in the final product development plan.

4.4. Cross-cutting requirements

These are tested as properties of the whole system, not features of any one module. They are additional to the operational responsibilities in 2.2 and the IT security requirements in Annex B.

- **Security by design**: every environment built, secured and operated to the standards in Annex B, given the confidential nature of the data;
- **End-to-end anonymisation**: disclosure controls enforced at the point of query and output, across all tiers, including granular and ad-hoc access, not applied only at publication;
- **Methodology integrity**: the methodology embedded so it is inspectable, reproducible, traceable to the underlying cohort, independently capable of being validated, and changed only under governance;
- **Extensibility**: new data types, asset classes, contributor segments and integrations added as coverage grows, without re-architecting;
- **Configurability under governance**: validation rules, disclosure parameters and reference data adjustable by the secretariat without a new release wherever practical.

5. IT SECURITY REQUIREMENTS

EMInvest holds confidential, financial-grade information contributed by commercial institutions. The Partner acknowledges the sensitivity of this information and agrees to implement and maintain a security posture commensurate with its criticality and risk profile.
The Partner shall meet a high security bar and comply with EMInvest's cybersecurity requirements, policies and standards as notified to the Partner from time to time, including any technical, organisational and governance controls mandated by EMInvest. This section sets out the minimum requirements and how bidders must evidence compliance for procurement purposes. Bidders shall provide clear, current evidence of their security controls and assurance, including summaries of relevant certifications, independent audit reports, penetration testing results, risk assessments, incident response playbooks, and supply chain security measures, together with named points of contact for security governance.

Detailed cybersecurity and data protection terms, including control baselines, audit and assurance rights, and incident management obligations, will be finalised and incorporated into the contract.

EMInvest may test, assess and verify the Partner's security controls during due diligence and throughout the term, including by requesting documentation, interviews and technical testing, and by requiring reasonable remediation.

The Partner is liable for any unauthorised access, loss, corruption, alteration, disclosure, or other breach of the security of EMInvest information or contributor data to the extent caused by the Partner, its personnel or its subcontractors. The Partner shall maintain appropriate contractual flow-downs and oversight of subcontractors to ensure equivalent security controls and obligations apply

5.1. Organisational requirements the partner must demonstrate

- **Certification and assurance.** Hold a current, recognised information-security certification, such as ISO 27001 or SOC 2 Type II, or demonstrate an equivalent independently assessed standard.
- **Data protection.** Comply with applicable data-protection law (UK GDPR and the Data Protection Act 2018) and be able to act as a processor on EMInvest's documented instructions.
- **Operational security processes.** Maintain documented vulnerability, patch, intrusion-prevention and incident-management processes, including notification to Systemiq within 24 hours of becoming aware of a breach affecting EMInvest data and conduct external penetration testing at least annually.
- **Business continuity.** Maintain tested business-continuity and disaster-recovery arrangements.
- **Subcontractors and subprocessors.** Disclose any subcontracors or subprocessors who will have access to EMInvest data and ensure equivalent security and data-protection obligations are contractually passed down to them.
- **Personnel security.** Conduct background checks on personnel with access to production data and maintain confidentiality/NDA coverage for all staff assigned to the engagement.
- **Cyber insurance.** Hold cyber liability insurance covering data breach and security incidents and provide evidence of cover on request.

5.2. Security capabilities the platform must provide

These are features the partner will design and build into the platform, and must show experience of delivering:

- **Encryption.** Encrypt all data at rest (to at least AES-256 or equivalent) and in transit.
- **Access control.** Role-based access on a least-privilege basis, with strong authentication, and controls to detect and mitigate misuse by privileged or rogue administrators.
- **Secure, separated hosting.** Host the platform in a secure environment in which EMInvest's data is logically or physically separated from any other client's data, held only in the agreed locations.
- **Logging and audit.** Access and activity logs, available to EMInvest.
- **Backup and recovery.** Regular backups with tested recovery, supporting the availability standard (see Performance standards).
- **Data portability and exit.** Self-service export of all data in standard formats on request and at the end of the contract, deletion on instruction, and support for a clean transfer of the platform and data to a future host.
- **Secure development**. Evidence a secure development lifecycle for the build, including code review and dependency/vulnerability scanning as part of the development pipeline, and

segregation of development, test and production environments with no live financial data used outside production.

5.3. How to evidence this in the proposal

Bidders should:

- state the security certifications they hold, with evidence; and
- provide a short security statement (no more than [2 pages]) describing their approach against the areas in 5.1, in particular how they would secure financial-grade data and separate it from other clients' data.
- Provide a list of any subcontractors or subprocessors proposed for this engagement, and a summary of their most recent external penetration test (data and high-level findings)

The successful bidder will be expected to evidence these controls in full, and to agree detailed security and data-protection terms, before contract signature.

6. PERFORMANCE STANDARDS

These are the service levels for the operating stage (Activity 4). They define what running the platform well means and are the basis for the periodic continuation reviews. The targets below are the headline standards; the precise figures, measurement method and any service credits are confirmed in the contract. Performance against them is reported to EMInvest at an agreed cadence.

Measure	Target
Platform availability	At least [99.5%] per month, excluding agreed planned maintenance
Planned maintenance	Scheduled outside peak periods, with at least [14 days'] notice
Support response — critical (platform unavailable or data at risk)	Within [4 hours]
Support response — high (a major function impaired)	Within [1 business day]
Support response — normal (minor issues and queries)	Within [3 business days]
Submission cycle	Run to the agreed annual schedule, with publication deadlines met
Data validation turnaround	Submissions validated and errors returned to contributors within [X business days]
Data quality assurance report	Delivered within [X weeks] of each cycle close
Breach or critical security incident notification	EMInvest notified within [24 hours] (see section 5)

The partner should propose how it will monitor and report against these standards. Sustained or material failure to meet them is addressed through remediation and the continuation-review and break provisions, with any service credits set out in the contract.

ANNEX B: FUNDER CONTRACT FLOW-DOWN REQUIREMENTS

Funder Flow-down Requirements

Norwegian Agency for Development Cooperation (Norad)

This Subcontract is funded either in whole or in part by an award to Systemiq from the Norwegian Agency for Development Cooperation ("Norad") and, as such, the Contractor must agree to comply with the following requirements.

Systemiq is subject to certain audit (Section 1 below), control measures, financial management, record-keeping and document retention obligations under its funding agreement with Norad ("Norad Obligations"), and the Contractor shall cooperate with Systemiq and provide all assistance reasonably requested and necessary to enable Systemiq to comply with the Norad Obligations, including by maintaining and retaining all complete and accurate records and supporting documentation relating to this Contract for five (5) years following the expiry and/or termination of the Agreement. Upon a written request from Systemiq to the Contractor at any time during the Agreement and for the five (5) year retention period, the Contractor shall promptly provide Systemiq with access to, and copies of, the records and any other information reasonably required to evidence compliance with this Agreement and the Norad Obligations.

The Contractor will not contact Norad directly; any and all communication with Norad, including requests for prior approval, shall be coordinated through Systemiq.

1. **Audit**.

1.1. The annual financial statements of the Project shall be audited in accordance with International Standards of Auditing (ISA). The auditor shall comply with ISA 800 (Special Considerations – Audits of Financial Statements Prepared in Accordance with Special Purpose Frameworks), ISA 805 (Special Considerations of audits of single financial statements and specific elements, accounts or items of a financial matter) and all ISAs relevant to the Project audit.

1.2. The audit shall be carried out by an independent chartered or certified state-authorized public accountant (auditor).

1.3. Systemiq reserves the right to approve the auditor and may require that the auditor shall be replaced if Systemiq finds that the auditor has not performed satisfactorily or if there is any doubt as to the auditor's independence or professional standards.

1.4. The auditor shall form an opinion on whether the Project's financial statements fairly reflect the financial position of the Project and whether they are prepared, in all material respects, in accordance with the applicable financial reporting framework and the requirements of this Subcontract.

1.5. The auditor shall report in accordance with the applicable audit standards, as agreed in clause D of the terms and conditions of the Subcontract.

1.6. The audit report shall include:

a. the Project name and agreement number;
b. the Project period subject of the audit,
c. reference to the financial reporting framework applied,
d. the auditing standards applied,
e. a statement that the auditor has obtained reasonable assurance about whether the financial statements as a whole are free from material misstatement;
f. the auditor's opinion.

1.7. If any findings have been reported in the Project's management letter, the Contractor shall prepare a response including an action plan to be submitted to Systemiq together with the management letter.

1.8. The costs of the audit of the Project's financial statements shall be included in the Project's budget.

1.9. The audit requirements stated in this Subcontract are applicable for the total Subcontract, including any part of the Subcontract that has been transferred to a cooperating partner or Contractor.

1.10. The auditor of the Project's consolidated financial statement is responsible for the direction, supervision and performance of the audit of any part of the Subcontract that has been transferred to a cooperating partner or Contractor. The auditor shall assure itself that those performing the audit for cooperating partners or Contractors have the appropriate qualifications, that the audit is in compliance with professional standards, and that the audit report is appropriate under the circumstances. ISA 600 establishes standards and provides guidelines when using the work of other auditors.

1.11. The auditor of the Project's consolidated financial statement shall express an opinion on whether the statement is prepared, in all material respects, in accordance with the requirements of this Subcontract. To this end, the auditor shall obtain sufficient appropriate audit evidence regarding the financial statements of the cooperating partner or Contractor and the consolidation process.

2. Equipment, Consumables and Intellectual Property.

2.1. Consistent with the Head Agreement with Norad, the right of ownership to equipment, consumables and intellectual property rights procured or developed by use of the Subcontract shall vest in the Systemiq or its cooperating partner or Contractor, unless otherwise stated in the Application. All matters associated with such equipment, consumables and intellectual property rights are the exclusive responsibility of the Contractor. However, significant use of such equipment, consumables and intellectual property rights for purposes outside the Project shall be subject to prior approval.

2.2. Intellectual property rights financed in whole or in part from the Subcontractor shall, in the spirit of securing such rights as a common global good, be managed in a way that maximizes their public accessibility and allows the broadest possible use. Material produced as a result of this Subcontractor shall, as far as possible and appropriate, be placed in the public domain for non-commercial use.

2.3. Norad shall have a non-exclusive and royalty-free license to use all intellectual property rights procured or developed by the use of the Subcontract. Norad may assign this right to any individual or organization at its own discretion.

2.4. Transfer of ownership of such equipment, consumables or intellectual property rights during the project period shall be made at market terms. Ownership may not be transferred to an employee of the Contractor, or to anyone related or connected to an employee, if such relation could lead to a conflict of interest as described this Subcontract.

2.5. Before a transfer is decided, the Contractor shall assess whether it may have an impact on the Project and, where appropriate, consult with Systemiq. Any income from a transfer shall accrue to the Project and shall be reported in the financial statement of the Project.

2.6. The Contractor shall prepare a record of transfer of ownership for any equipment, consumables and intellectual property rights. The record shall comprise information about the object of transfer, the original purchase price paid by the Contractor, price offers received, the final sales price and the name of the purchaser. The record shall be submitted to Systemiq along with the first progress report due after the sale.

2.7. If the activities of the Project do not continue after the end of the project period or after termination of the Subcontract, the Contractor shall inform Systemiq about the remaining equipment and goods that have been purchased by use of the Subcontract. Norad may require that such assets be sold. Such sale shall be completed in accordance with the procedures described above. Income from the sale shall be repaid to Systemiq or Norad unless otherwise agreed by the Parties.

3. Financial Management.

3.1. The Contractor shall keep accurate accounts of the Project's income and expenditure using an appropriate accounting- and double-entry book-keeping system in accordance with the applicable accounting- and bookkeeping policies in the jurisdiction of the Contractor.

3.2. The accounts shall be kept up to date at least on a monthly basis. Bank reconciliations and cash reconciliations shall be completed at least every month and shall be documented by the Contractor.

3.3. All income and expenditures relating to the Project must be easily identifiable and traceable within the Contractor's general accounting – and bookkeeping systems. This can be done by using separate accounts for the Project, or by recording all the Project's income and expenditures under a unique project number. Regardless of the method used, it must be possible to generate a report from the Contractor's accounting system that can be directly reconciled with the Project's financial statements in the financial report.

3.4. All income and expenditures relating to the Project must be easily verifiable. Insufficient documentation may render the expenditure ineligible.

4. Transfer of the Subcontract to a cooperating partner.

4.1. Transfer of all or part of the Head Agreement including assets to a cooperating partner or Contractor must be documented through a written Subcontract. The Subcontract shall specify that the cooperating partner or Contractor is required to comply with the provisions of this Head Agreement which is relevant to the Subcontract agreement and to cooperate with Systemiq to ensure that Systemiq is able to fulfill its overall obligations under the Agreement between Systemiq and Norad.

4.2. The Subcontract shall include provisions for results and financial reporting, audit, procurement and measures to prevent financial irregularities and sexual exploitation, abuse and harassment. Furthermore, the Subcontract shall explicitly state that:

4.2.1. both Systemiq, Norad, and the Norwegian Auditor shall be given access to control how the cooperating partner or Contractor have used the Funds as described in article 3 above.

4.2.2. The cooperating partner or Contractor agrees that Systemiq and/or Norad is entitled to claim repayment from the cooperating partner or Contractor directly and to the same extent as Systemiq from the Contractor in accordance with article 10.

4.2.3. The cooperating partner or Contractor shall accept the choice of law and settlement of disputes provisions in article 10 for any dispute arising between the Contractor and Norad.

4.3. The Contractor shall assure itself that it has the necessary competence and internal procedures to meet the requirements of the Agreement between Systemiq and Norad that are relevant for the Subcontract and shall follow Contractor's compliance with such requirements throughout the Period of the Project. The Contractor must throughout the Period of the Project obtain and assess Project management letters issued by auditors. Any significant findings must be acted upon.

4.4. The Subcontract Funds may not be transferred to a cooperating partner or Contractor who has previously been charged or sentenced for any criminal activity unless explicitly approved by Norad.

5. **Transparency.**
    5.1. Norad may make this Subcontract and other Project documentation, such as but not limited to, the application and agreed reports available to the public to promote transparency on the use of public funds.

    5.2. The Contractor shall make the Project documentation, including the Application and all agreed reports, available to anyone upon request. Requests for disclosure may only be denied if such disclosure is prohibited by confidential obligations and/or if it may be detrimental to the Contractor's legitimate interests

6. **Financial Irregularities.**
    6.1. The Contractor is required to practice zero tolerance against corruption and other financial irregularities within and related to the Project. The zero-tolerance policy applies to all staff members, consultants and other non-staff personnel and to cooperating partners and beneficiaries of the Subcontract.

    6.2. Financial irregularities refer to all kinds of:
    a. corruption, including bribery, nepotism and illegal gratuities;
    b. misappropriation of cash, inventory and all other kinds of assets;
    c. financial and non-financial fraudulent statements;
    d. all other use of Project funds which is not in accordance with the implementation plan and budget.

    6.3. In order to fulfil the zero-tolerance requirement, the Contractor shall:
    a. organize its operations and internal control systems in a way that financial irregularities are prevented and detected;
    b. do its utmost to prevent and stop financial irregularities within and related to the Project;
    c. require that all staff involved in, and any consultants, suppliers and contractors financed under the Project refrain from financial irregularities.

    6.4. The Contractor shall inform Systemiq immediately of any indication of financial irregularities in or related to the Project. The Contractor shall provide Systemiq with an account of all the known facts and an assessment of how the matter should be followed up, including whether criminal prosecution or other sanctions are considered appropriate.

    6.5. The matter will be handled by Systemiq in accordance with Norad's guidelines for handling suspicion of financial irregularities. The Contractor shall cooperate fully with Systemiq or Norad's investigation and follow-up. If requested by Systemiq or Norad, the Contractor shall, provided there is sufficient basis for taking legal steps, report the suspicions to the police, commence civil proceedings for recovery of damages or apply other appropriate sanctions against persons or entities suspected of financial irregularities. However, in cases where the Contractor is concerned that due process of law may be unavailable, the matter shall instead be included in the account and assessment for discussion of a mutually acceptable course of action.

7. **Sexual Exploitation, sexual abuse and sexual harassment.**
    7.1. Norad has zero tolerance for inaction against sexual exploitation, abuse and harassment (SEAH). The Contractor shall have a victim/survivor-centred approach to SEAH issues and take all reasonable steps to prevent, detect, and respond to SEAH within and related to the Project. This obligation applies to all staff members, consultants and other non-staff personnel, cooperating partners, and any third parties involved in activities funded by the Subcontract.
    7.2. The following definitions apply:
        7.2.1. Sexual exploitation: Any actual or attempted abuse of a position of vulnerability, differential power, or trust, for sexual purposes, including, but not limited to, profiting monetarily, socially or politically from the sexual exploitation of another.

        7.2.2. Sexual abuse: The actual or threatened physical intrusion of a sexual nature, whether by force or under unequal or coercive conditions.

7.3. Sexual harassment" Any form of unwanted sexual attention that has the purpose or effect of being offensive, frightening, hostile, degrading, humiliating or troublesome.

7.4. The Contractor shall:
- 7.4.1. Adhere to the IASC-Minimum Operation Standards on "Protection from sexual exploitation and abuse by own personnel" and/or the SEA elements of the Core Humanitarian Standard on Quality and Accountability,
- 7.4.2. have ethical guidelines that include policies on prevention and response to SEAH,
- 7.4.3. organize its operations and internal control systems in a way that SEAH is prevented, detected and responded to,
- 7.4.4. take swift action on suspicions or complaints of SEAH to stop harm occurring, investigate and report to relevant authorities (for criminal matters), after considering the rights, needs and wishes of the survivor/victim.

7.5. The Contractor shall inform Systemiq and Norad immediately of any indications of SEAH credible enough to warrant an investigation within or related to the Project as well as indications of SEAH not directly linked to the Project but of significant impact on the partnership with the donor

7.6. The Contractor shall provide Systemiq and Norad with a report of the relevant facts and an assessment of how the matter will be followed up, including whether the organisation will improve internal systems to prevent, detect and respond to SEAH, and whether criminal prosecution or other sanctions are considered appropriate, considering the rights, needs, and wishes of the survivor/victim. The reporting will be made without compromising the safety, security, privacy, and due process rights of any concerned person. The report will be handled by Norad and Systemiq in accordance with Norad's guidelines for handling notifications of sexual abuse, sexual exploitation, and sexual harassment by grant recipients.

7.7. Upon request from Norad, the Contractor shall grant Norad and Systemiq access to all relevant information and documentation related to the Contractor's adherence with this article.

8. **Recognition and Publication.** The Contractor shall acknowledge Systemiq and Norway's support to the Project in all publications and other materials issued in relation to the Project. Both logotypes will be provided upon request. All use of Norway's logotype must be approved by Norad in advance.

9. **Breach of the Agreement.** In addition to the terms and conditions of the body of the Subcontract, Systemiq may terminate the Subcontract in the event of the following:

9.1. If the Contractor fails to fulfil its obligations under this Subcontract and/or if there is suspicion of financial irregularities, Systemiq may suspend disbursement of all or part of the Subcontract.

9.2. In the event of material breach of the Subcontract, Systemiq may terminate the Subcontract with immediate effect, and/or claim repayment of all or parts of the Subcontract Funds. A repayment claim may also include interest, and any other financial gain obtained by the Contractor as a result of the financial irregularity. Norad has the same right to claim repayment of the Subcontract Funds from the Contractor as Systemiq.

9.3. Material breach of the Subcontract shall include, without limitation, the following situations:
- 9.3.1. all or part of the Subcontract funds have not been used in accordance with the Subcontract and/or approved implementation plans and budget,
- 9.3.2. the Contractor has made false or incomplete statements to obtain the Subcontract,

9.3.3. the use of the Subcontract has not been satisfactorily accounted for,
9.3.4. the Contractor has, after having been granted an extended deadline, failed to provide the agreed reports, or has knowingly provided reports that do not reflect reality,
9.3.5. the Contractor has failed to take preventive measures against sexual exploitation, sexual abuse, or sexual harassment, to detect or respond to indications thereof, or to take corrective action when sexual exploitation, sexual abuse, or sexual harassment has occurred.
9.3.6. financial irregularities, grave professional misconduct or illegal activity of any form have taken place within the Contractor,
9.3.7. the Contractor has failed to inform Systemiq of indication of financial irregularities within the Project,
9.3.8. the Contractor has changed legal personality without prior notification to Systemiq,
9.3.9. the Contractor is bankrupt, being wound up or is having its affairs administered by the courts or is subject to any analogous or corresponding procedure provided for under national legislation.

9.4. The Contractor shall inform Systemiq immediately of any circumstances that may indicate or lead to a breach of Subcontract and shall provide Systemiq with any information or documentation it may reasonably require in order to determine if a breach of the Subcontract has occurred.

9.5. Systemiq may also suspend disbursements or terminate the Subcontract with immediate effect if a material breach of another agreement between Systemiq and the Subcontract has been established.

10. **Choice of Law and Settlement of Disputes.** This Subcontract is between Systemiq and the Contractor. However, in the event of a dispute between Norad and the Contractor, the following will apply:

10.1. Should a dispute arise between Norad and the Contractor, the parties shall seek to reach an amicable solution.

10.2. Any dispute arising out of or in connection with the Subcontractor that cannot be solved amicably, shall exclusively be settled before the Norwegian courts of law with Oslo District Court as legal venue.

10.3. The Contractor accepts that Norad can, at its own sole discretion and as an alternative to the legal venue mentioned above, choose to settle the dispute by
10.3.1. the courts in the legal venue of the Contractor, or
10.3.2. arbitration in accordance with the Arbitration Rules of the Arbitration Institute of the Stockholm Chamber of Commerce. The arbitral tribunal shall be composed of three arbitrators. If the disputed amount is below an amount corresponding to NOK 10 000 000 the arbitral tribunal shall, however, be composed of a sole arbitrator. The seat of arbitration shall be Stockholm, Sweden, and the language to be used in the arbitral proceedings shall be English. The Parties agree that neither the arbitral proceedings nor the award shall be subject to any confidentiality.

10.4. The Parties agree that no other courts of law, other than as set out in this article 10, shall have jurisdiction over disputes arising out of or in connection with this Subcontractor.

ANNEX C: DRAFT CONTRACT

SYSTEMIQ LIMITED

and

[INSERT SUB-CONTRACTOR]

CONSULTING SERVICES AGREEMENT

SYSTEMIQ

Contents

SYSTEMIQ

SYSTEMIQ LIMITED ("SYSTEMIQ")

CONSULTING SERVICES AGREEMENT

CONTRACT SUMMARY

SYSTEMIQ'S COMPANY DETAILS:	REGISTERED OFFICE: 4TH FLOOR, 10-12 RUSSELL SQUARE HOUSE, RUSSELL SQUARE, LONDON, UNITED KINGDOM, WC1B 5EH COMPANY REGISTRATION NUMBER: 09950762 COUNTRY OF INCORPORATION: ENGLAND
CONSULTANT COMPANY DETAILS	[NAME] [REGISTRATION NUMBER] [REGISTERED ADDRESS
CONSULTANT REPRESENTATIVE:	NAME: [NAME] TITLE: [TITLE] EMAIL: [EMAIL]
SYSTEMIQ REPRESENTATIVE:	NAME: Mattia Romani TITLE: Partner EMAIL: Mattia.romani@systemiq.earth
COMMENCEMENT DATE:	[DAY MONTH YEAR]
CURRENCY:	[EUR/USD/GBP]
TERMINATION NOTICE PERIOD:	30 DAYS
INVOICE CREDIT TERMS:	30 DAYS FROM INVOICE DATE
FEES, SERVICES AND DELIVERABLES	TO BE SET OUT IN WORK SCHEDULES. WORK SCHEDULE NO. 1 IS AT APPENDIX 1 TO THIS AGREEMENT.

Please sign below to indicate your agreement to this Contract Summary, together with the Terms and Conditions Attached:

Signed by Mattia Romani for and on behalf of **SYSTEMIQ LIMITED**	.... Partner Date:
Signed by [NAME OF DIRECTOR] for and on behalf of [Sub-contractor Name]	.... Director Date:

PLEASE INCLUDE A COPY OF THIS WHOLE AGREEMENT (INCLUDING THE TERMS AND CONDITIONS) WHEN RETURNING A SIGNED COPY OF THIS AGREEMENT

TERMS AND CONDITIONS OF BUSINESS

1 Definitions and interpretation

1.1 In this Agreement, unless the context requires otherwise, the following words and phrases have the meanings set opposite them:

Affiliate	in relation to a Party, any corporation, firm, partnership or other legal entity which, directly or indirectly, is controlled by, controls or is under common control with that Party from time to time, where "**control**" means the power, direct or indirect, to direct or cause the direction of the management and policies of any person or entity, whether by contract, ownership of shares, membership of the board of directors, agreement or otherwise and, in any event and without limitation of the foregoing, any entity owning 50% or more of the voting securities of a second entity shall be deemed to control that second entity. The terms "**controlling**" and "**controlled**" shall have a corresponding meaning;
Agreement	the Contract Summary, these Terms and Conditions of Business, the Work Schedule at Appendix 1 and all additional Work Schedules executed by the Parties;
Background IP	all Intellectual Property Rights which subsist and which are owned by Systemiq or its licensors or the Contractor on or before the Commencement Date, and all Intellectual Property Rights which are created by Systemiq or its licensors, or the Contractor, after the Commencement Date otherwise than in the course of the production of the Deliverables for the Systemiq Client in accordance with this Agreement, including all Intellectual Property Rights in the Systemiq Tools;
Client Materials	all materials, documents, tools, equipment and other documents supplied by the Contractor in connection with the Services and Deliverables;

Commencement Date	as stated in the Contract Summary section of this Agreement;
Contributor(s)	any commercial or financial institution or other third party that contributes or provides data, content or information to EMInvest for use in or in connection with the Services.
Contributor Data	All data, content and other materials provided or made available by Contributors in connection with the Services. For the avoidance of doubt, any Contributor Data shall be considered Confidential Information under this Agreement, unless otherwise agreed by the Parties.

Confidential Information means any and all information relating to each Party and each Party's Related Parties (and/or the business carried on, or proposed or intended to be carried on, by any of the above) which is made available in connection with this Agreement to each Party (or any of each Party's Related Parties) by each other Party (or any of each Party's Related Parties), whether before, on or after the Commencement Date, including:

i. the fact that discussions and negotiations are taking place concerning the Agreement and the status of those discussions and negotiations;

ii. the existence and terms of this Agreement;

iii. all confidential or proprietary information relating to:

iv. the Systemiq Client which the Contractor receives in the course of providing services;

v. the business, affairs, customers, finances, clients, suppliers, plans, intentions, marketing materials or market opportunities of either Party or of any Related Party of each Party;

vi. the operations, systems, processes, product information, products, services, know-how, product specifications, technical information, designs, trade secrets or software business methods and business concepts of each Party or of any Related Party of each Party in whatever form, whether in oral, tangible or in documented form and, if in tangible or documented form, whether marked or identified as being proprietary or not and whether or not marked as confidential; or

vii. any other information that is identified as being of a confidential or proprietary nature,

but excluding any information referred to in clause 8.2 and any information that the Parties could not reasonably be expected to consider to be confidential or commercially sensitive. Any information, copies, findings, data, specifications or analysis derived from Confidential

	Information (including any new Intellectual Property Rights if applicable) shall also be deemed to be Confidential Information;
Contractor	[Sub-contractor Name]
Contractor Materials	means any reports, data, datasets, software, specifications, drawings, documents, content or other materials supplied as a result of the performance of the Subcontract by the Contractor to Systemiq in connection with the Services;
controller, processor, data subject, personal data, personal data breach, processing and appropriate technical measures:	as defined in the Data Protection Legislation;
Critical Incident	where EMInvest is unavailable or EMInvest and/or Contributor Data is at material risk
Data Protection Legislation	the UK Data Protection Legislation and the GDPR and any other directly applicable European Union regulation relating to privacy.
Deliverables	all documents, products, content and materials developed by Contractor in the course of the provision of the Services, including without limitation data, reports and specifications (including drafts), as identified in each Work Schedule.
Disclosing Party	a Party to this Agreement when it discloses its Confidential Information, directly or indirectly, to the other Party;
EMInvest	Database platform developed by the Contractor under this Agreement, aggregated and anonymised Contributor Data analysed to determine private markets investment risk and performance in emerging markets and developing economies (EMDEs).

Engagement	the engagement of Systemiq by the Systemiq Client to provide the Services on the terms and conditions of a Systemiq Client Services Agreement;
Fees	the fees, costs and expenses to be paid by the Systemiq to the Contractor for the provision of the Services, as set out in each Work Schedule;
High Priority Incidents	where a major EMInvest platform function is materially impaired
Intellectual Property Rights	means patents, utility models, rights to inventions, copyright and neighbouring, related and associated rights, moral rights, trade marks and service marks, trade names, business names and domain names, rights in get-up and trade dress, rights in goodwill and the right to sue for passing off, unfair competition or similar causes of action, rights in designs, rights in computer software, database rights, rights to use, and protect the confidentiality of, confidential information (including know-how and trade secrets), and all other intellectual property rights, in each case whether registered or unregistered and including all applications and rights to apply for and be granted, renewals or extensions of, and rights to claim priority from, such rights and all similar or equivalent rights or forms of protection which subsist or will subsist now or in the future in any part of the world;
Interest Rate	two per cent per annum above the base rate of the Bank of England base rate from time to time;
Normal Priority Incidents	where EMInvest platform experiences minor defects, service requests and user queries
Party	means a Party to this Agreement, and "**Parties"** shall be construed accordingly;
Receiving Party	a Party to this Agreement when it receives Confidential Information, directly or indirectly, from the other Party;
Related Party	means, in relation to a Party, any director, officer, employee, agent, professional adviser (including solicitors, auditors, insurers and accountants), contractor,

	subcontractor or Affiliate of that Party, and "**Related Parties**" shall be construed accordingly;
Security Incident	means any unathorised or unlawful access to, or loss, corruption or alteration, disclosure, unavailability or other breach of security that directly affects EMInvest, or Contributor Data.
Security Requirements	means EMInvest's cybersecurity, information security and data protection requirements, policies, standards and control baselines with which the Contractor is required to comply under this Agreement.
Services	the services to be provided by the Contractor to Systemiq and/or the Systemiq Client in accordance with this Agreement, as set out in each Work Schedule;
Sub-processor	has the meaning as set-out in the Data Protection Legislation;
Systemiq Client	**Norwegian Agency for Development Cooperation (Norad)**
Systemiq IP	all Intellectual Property Rights subsisting in the Deliverables including any Background IP incorporated into them but excluding any Systemiq Client Materials incorporated in them;
Systemiq Tools	all concepts, know-how, tools, frameworks, models and industry perspectives developed or enhanced outside of the Services;
Term	the period from the Commencement Date to the Termination Date (both days inclusive);
Termination Date	the date upon which the Engagement under this Agreement terminates for whatever reason;
UK Data Protection Legislation	all data protection legislation from time to time in force in the UK including the Data Protection Act 2018 or any successor legislation; and
Work Schedule	the project, job, task or services to be provided by the Contractor to the Systemiq Client as set out in the work schedule at Appendix 1 and all additional projects, tasks or services to be provided to the Systemiq Client by the

Contractor on the terms and conditions of this Agreement, the details of which are to be set out in the same form of the document at Appendix 1, and which shall be executed by both Parties.

Recitals

WHEREAS, Systemiq and Systemiq Client have entered into the Client Services Agreement on or around the date hereof, such agreement will govern all of the services and projects undertaken by Systemiq for the Systemiq Client and its affiliates

WHEREAS, Systemiq and the Contractor agree to enter into this consulting services agreement which shall govern the Services and Deliverables undertaken by the Contractor (in its capacity as a subcontractor to Systemiq) for the Systemiq Client ("the **Agreement**")

WHEREAS, the Parties wish to set forth the terms and conditions that will govern this Agreement, the Parties agree as follows:

1.2 In this Agreement:

1.2.1 Clause, Appendix and paragraph headings shall not affect the interpretation of this Agreement.

1.2.2 A person includes a natural person, body corporate, corporation, firm, partnership, trust, association, organisation, government, state, foundation or other unincorporated body (whether or not having separate legal personality).

1.2.3 The Appendices form part of this Agreement and shall have effect as if set out in full in the body of this Agreement. Any reference to this Agreement includes the Appendices.

1.2.4 A reference to a company shall include any company, corporation or other body corporate, wherever and however incorporated or established.

1.2.5 Unless the context otherwise requires, words in the singular shall include the plural and in the plural shall include the singular.

1.2.6 Unless the context otherwise requires, a reference to one gender shall include a reference to the other genders.

1.2.7 A reference to an employee of Systemiq as a "director" does not mean they hold the office of director for the purposes of the Companies Act 2006, but rather, that they hold a senior role as an employee of the company.

1.2.8 A reference to a statute or statutory provision is a reference to it as amended, extended or re-enacted from time to time.

1.2.9 A reference to a statute or statutory provision shall include all subordinate legislation made from time to time under that statute or statutory provision.

1.2.10 This Agreement shall be binding upon, and benefit, the Parties and their respective personal representatives, successors and permitted assigns, and references to any Party shall include that Party's personal representatives, successors and permitted assigns.

1.2.11 A reference to writing or written includes email.

1.2.12 Any obligation on a Party not to do something includes an obligation not to allow that thing to be done.

1.2.13 Any words following the terms "including", "include", "in particular", "such as", or "for example" or any similar expression shall be construed as illustrative and shall not limit the sense of the words, description, definition, phrase or term preceding those terms. General words (such as "other" and "others") do not have a restricted meaning merely because they follow words indicating a particular category or class of things.

1.2.14 The term "law" includes legislation, common law and binding judicial precedent, and the order or decree of any court or any tribunal, agency or authority of competent jurisdiction.

2 Commencement and length of Engagement

2.1 This Agreement shall commence on the Commencement Date and shall continue [until the later of [INSERT DATE] or the completion of the Services unless and until terminated earlier:

2.1.1 as provided by the terms of this Agreement; or

2.1.2 by either Party giving to the other not less than 30 days prior written notice of termination.

2.2 [OPTIONAL]The Term of this Agreement may be extended for an additional one (1) year or such other period of time as agreed between the Parties on the same terms and conditions, if mutually agreed by the Parties in writing prior to the end of the Term

3 Provision of services

3.1 The Contractor shall provide the Services to Systemiq and/or Systemiq Client on the terms and conditions of this Agreement for the duration of the Term.

3.2 The Contractor shall use reasonable endeavours to deliver the Deliverables to Systemiq and/or Systemiq Client in accordance with the relevant Work Schedule in all material respects.

3.3 The Contractor shall use reasonable endeavours to meet any performance dates specified in a Work Schedule but any such dates shall be estimates only and time for performance by the Contractor shall not be of the essence of this Agreement.

3.4 The Parties will use reasonable endeavours to meet on a regular basis at such intervals as agreed between the Parties, acting reasonably, at mutually agreed times by video conference, in person or as may otherwise be agreed by the Parties during the Engagement to discuss the progress of the Services and/or Deliverables, and to exchange feedback and to agree on the next steps in respect of any part of the Services.

3.5 The Parties agree to execute Work Schedules to record the details of all Services and Deliverables to be provided by the Contractor to Systemiq and/or Systemiq Client, the first of which is set out at Appendix 1.

4 Outside interests and protection of business interests

4.1 Each Party acknowledges and agrees that nothing in this Agreement shall prevent either Party from providing services to, or otherwise contracting with, any third party, including any third party that competes or may compete with the other Party. Neither Party shall be under any obligation to disclose to the other Party any such contracts or arrangements with third parties.

5 Contractor obligations

5.1 The Contractor represents and warrants to Systemiq that it will provide the Services in a diligent and professional manner and in accordance with the highest industry and ethical standards and will at all times comply with all applicable laws and regulations. The Contractor will be responsible for the performance of each its employees, agents, vendors and approved subcontractors, if any, and for their compliance with all of the terms and conditions of this Agreement and shall indemnify Systemiq against any loss suffered or claim by the Systemiq Client against Systemiq as a result of the Contractor's failure to provide the Services in accordance with this Agreement. Failure to comply with the obligations hereunder shall constitute a material breach of this Agreement and shall give Systemiq the right to terminate this Agreement with immediate effect, without prejudice to the right of compensation for any damage caused to Systemiq.

5.2 The Contractor shall:

5.2.1 co-operate with Systemiq in all matters relating to the Services;

5.2.2 follow all of Systemiq's reasonable instructions and procedures (including providing any authorisations to Systemiq where necessary) with respect to the Services, and secure any appropriate or necessary consents, permissions and authorisations necessary or desirable for Systemiq to provide the Services;

5.2.3 provide Systemiq with all relevant Contractor Materials in an appropriate format, as requested by Systemiq prior to the Commencement Date and from time to time during the Term;

5.2.4 if applicable, provide Systemiq, its agents, subcontractors, consultants and employees, in a timely manner and at no charge, access to, and use of, the Contractor's premises, office accommodation, information, data, documentation and other facilities as reasonably required by Systemiq;

5.2.5 ensure that all Contractor Materials are true, accurate, complete and up to date, are not defamatory and do not otherwise breach any applicable laws;

5.2.6 provide, in a timely manner, all such information and Contractor Materials as Systemiq may reasonably require, and ensure that such information and Contractor Materials are accurate and complete in all material respects; and

5.2.7 represent and warrant that they are duly constituted under the laws and regulations prevailing in their jurisdiction of incorporation, and that the representative executing this Agreement has full legal authority and is duly authorised to do so.

5.3 The Contractor acknowledges that Systemiq's ability to provide the Services to the Systemiq Client is dependent upon the full and prompt co-operation of the Contractor (which the Contractor agrees to provide) as well as the accuracy, truthfulness and completeness of any Contractor Materials provided to Systemiq. If Systemiq's performance of its obligations under the Agreement is prevented or delayed by any act or omission of the Contractor, its agents, subcontractors, consultants or employees, Systemiq shall:

5.3.1 not be liable for any costs, charges or losses sustained or incurred by the Contractor that arise directly or indirectly from such prevention or delay;

5.3.2 be entitled to recover from the Contractor any additional costs, charges, expenses or other losses that Systemiq sustains or incurs that arise directly or indirectly from such prevention or delay.

6 Fees, expenses and compensation

6.1 In consideration for the provision of the Services, Systemiq shall pay to the Contractor the Fees.

6.2 The Contractor shall raise invoices for the Fees in accordance with the payment schedule set out in the applicable Work Schedule.

6.3 All invoices raised in accordance with clause 6.2 shall be payable in full by Systemiq within 30 days of receipt, provided that Systemiq shall not be liable for any payment to the Contractor until such time as Systemiq has received full payment from the Systemiq Client for the Services.

6.4 Each Party to this Agreement will be responsible for their own legal and other costs and expenses in connection with the negotiation, preparation, execution, implementation and execution of this Agreement, save for all expenses which the Parties agree the Contractor may charge Systemiq, as recorded in the relevant Work Schedule.

7 Limitation of Liability

7.1 Nothing in the Agreement limits any liability which cannot legally be limited or excluded, including liability for:

7.1.1 death or personal injury caused by negligence; and

7.1.2 fraud or fraudulent misrepresentation.

7.2 Subject to clause 7.1 and clause 7.3, Systemiq's total liability to the Contractor for loss or damage under this Agreement, for any one event or series of events, shall not exceed the sum of the value of Fees payable by Systemiq to the Contractor for services provided under this Agreement.

7.3 Subject to clause 7.1, neither Party shall be liable to the other Party, whether in contract, tort (including negligence), breach of statutory duty, or otherwise for:

7.3.1 loss of profits;

7.3.2 loss of sales or business;

7.3.3 loss of agreements or contracts;

7.3.4 loss of anticipated savings;

7.3.5 loss of use or corruption of software, data or information;

7.3.6 loss of or damage to goodwill; or

7.3.7 indirect or consequential loss.

7.4 All warranties, conditions and other terms, express or implied (by statute or otherwise) are, unless expressly set out in this Agreement, excluded from this Agreement to the fullest extent permitted by law.

7.5 Unless the Contractor notifies Systemiq that it intends to make a claim in respect of an event giving rise to liability within the notice period set out in this clause 7.5, Systemiq shall have no liability for that event. The notice period for such an event shall start on the day on which the Contractor became, or ought reasonably to have become, aware of the event having occurred and shall expire 6 months from that date. The notice must be in writing and must identify the event and the grounds for the claim in reasonable detail.

8 Confidential information

8.1 Each Party undertakes that it shall not at any time disclose to any person (without the prior written consent of the other Party) the terms of this Agreement, the fact Systemiq is providing the Services to the Systemiq Client, the Deliverables, and any Confidential Information, except as permitted by this clause 8.

8.2 Confidential Information shall not include information that:

8.2.1 is at the time of its disclosure, or becomes, generally available to the public other than as a direct or indirect result of a breach by the Receiving Party of its obligations under this Agreement;

8.2.2 it was available to the Receiving Party on a non-confidential basis prior to disclosure by or on behalf of the Disclosing Party;

8.2.3 it was, is, or becomes available to the Receiving Party on a non-confidential basis from a person who, to the Receiving Party's knowledge, is not under any confidentiality obligation in respect of that information;

8.2.4 it was lawfully in the possession of the Receiving Party before the information was disclosed by the Disclosing Party;

8.2.5 it is developed by or for the Receiving Party independently of the information disclosed by the Disclosing Party;

8.2.6 the Parties agree in writing that the information is not confidential; and

8.2.7 any other information which the Receiving Party could not reasonably be expected to consider confidential.

8.3 A Receiving Party may disclose Confidential Information to the minimum extent required by:

8.3.1 an order of any court of competent jurisdiction or any regulatory, judicial, governmental or similar body or any taxation authority of competent jurisdiction;

8.3.2 the rules of any listing authority or stock exchange on which its shares or those of its Affiliates are listed or traded; or

8.3.3 the laws or regulations of any country to which its affairs or those of any of its Affiliates are subject; or

8.3.4 to its and its Affiliates employees, officers, representatives, contractors, subcontractors or advisers, who need to know such information for the purposes of exercising the Party's rights or carrying out its obligations under, or in connection with, this Agreement or for compliance with applicable law. Each Party shall ensure that all such Parties to whom it discloses the other Party's Confidential Information under a duty to keep such information confidential on reasonably equivalent terms to those set out in this clause 8.

8.4 The Receiving Party shall at any time upon the Disclosing Party’s written request, and in any event on or before the Termination Date, return to the Disclosing Party, or at its election destroy all documents and materials containing or based on the Disclosing Party’s Confidential Information, save that the Receiving Party may retain a copy for its records or as may be required in accordance with applicable law or the rules of any listing authority or stock exchange to which it (or its Affiliates) is subject. The provisions of this Agreement shall continue to apply to any documents and materials retained by the Receiving Party pursuant to this clause 8.4.

8.5 The Contractor acknowledges and agrees all Deliverables are for the Systemiq Client’s and/or Systemiq’s internal use only and may not be relied upon by any third Parties or disclosed to any third Parties except as provided for in this clause 8 and clause 9.

8.6 No Party shall use the other Party's Confidential Information for any purpose other than to exercise its rights and perform its obligations under, or in connection with, this Agreement.

8.7 Neither Party shall release any press releases, announcements, public statement, social media post or other publicity relating to this Agreement, the Engagement, the Services or the Deliverables without the prior written consent of the other Party.

9 Intellectual property

9.1 Systemiq and its licensors shall retain ownership of all Background IP and all Systemiq IP, and nothing in this Agreement will operate to transfer or assign any rights in such Background IP or Systemiq IP to the Contractor or any third Party.

9.2 The Contractor and its licensors shall retain ownership of all Intellectual Property Rights in the Contractor Materials. Nothing in this Agreement will operate to transfer or assign such rights to Systemiq or any third Party.

9.3 Systemiq grants to the Contractor, or shall procure the direct grant to the Contractor and its Affiliates of, a fully paid-up, worldwide, non-exclusive, non-transferable, revocable, royalty-free licence to copy Systemiq IP for the sole purpose of providing the Services and the Deliverables in the course of the Contractor's business on a perpetual basis.

9.4 The Contractor grants Systemiq a fully paid-up, worldwide, non-exclusive, royalty-free licence to use, display, reproduce, publish, copy, excerpt, distribute, create derivative works from and otherwise disseminate, in whole or in part, the Contractor Materials for the Term for the purpose of providing the Services to the Systemiq Client in accordance with this Agreement. Systemiq may grant sublicences of this licence to its Substitutes or to any other Party as the Contractor may agree in writing.

9.5 All rights (including Intellectual Property Rights) in any documents, information, products, data or other materials provided by any third Parties pursuant to the Services shall remain vested in the licensors thereof and the Contractor agrees to comply with any licence terms relating to the Contractor's use of the same, where notified to the Contractor in writing.

9.6 Intellectual Property Rights financed in whole or in part from this Subcontract shall, in the spirit of securing such rights as a common global good, be managed to maximise public accessibility and allow the broadest possible use. Deliverables and/or EMInvest produced as a result of this Subcontract shall, as far as possible and appropriate, be placed in the public domain for non-commercial use.

9.7 Contributor data shall remain the property of the relevant contributors at all times. The Contractor shall process Contributor Data solely on Systemiq's documented instructions and only to the extent necessary to perform the Services, and shall not use, disclose, sell, licence, exploit or otherwise process Contributor Data for any other purpose. Except for the limited right to process Contributor Data strictly in accordance with this clause and the Contract, the Contractor acquires no right, title or interest (including any intellectual property rights) in or to any Contributor Data.

10 Cyber Security and IT requirements

10.1 The Contractor shall maintain documented operational security processes, including vulnerability management, patch management, intrusion prevention and incident management procedures. The Contractor shall notify Systemiq without undue delay, and in any event within seventy-two (72) hours of becoming aware of any actual or suspected Security Incident affecting EMInvest and/or Contributor Data. The Contractor shall conduct external penetration testing of the systems used to provide the Services at least annually.

10.2 The Contractor shall maintain and regularly test appropriate business continuity and disaster recovery plans and arrangements designed to ensure the resilience and timely recovery of the Services.

10.3 The Contractor shall disclose to Systemiq, any subcontractor or subprocessor that will process or have access to EMInvest. The Contractor shall ensure that each such subcontractor or subprocessor is bound by written contractual obligations imposing security, confidentiality and data protection obligations no less onerous than those imposed on the Contractor under this Agreement. The Contractor shall remain fully responsible for the acts and omissions of its subcontractors and subprocessors. No subprocessor shall be appointed or replaced without the Systemiq's prior written approval, such approval shall not be unreasonably withheld or delayed.

10.4 The Contractor shall conduct appropriate background checks, to the extent permitted by applicable law, on all personnel with access to production systems or EMInvest and shall ensure that all personnel assigned to deliver the Services are subject to written confidentiality obligations no less onerous than those set out in this Agreement.

10.5 The Contractor shall design, develop, implement and maintain EMInvest to include the following minimum security capabilities:

10.5.1 encrypt all EMInvest and Contributor Data at rest using AES-256 or an equivalent industry-recognised encryption standard, and encrypt all EMInvest and/or Contributor Data in transit using secure cryptographic protocols;

10.5.2 implement role-based access controls on the principle of least privilege, including strong authentication mechanisms and controls designed to detect, prevent and mitigate any Security Incident by privileged users or administrators;

10.5.3 host EMInvest in a secure environment in which EMInvest and Contributor Data is logically or physically segregated from the data of any other customer and stored only within the agreed hosting locations with Systemiq;

10.5.4 maintain comprehensive system, access and activity logs and make such logs available to Systemiq or the Systemiq Client upon reasonable request, subject to applicable law and the Contractor's legitimate security requirements;

10.5.5 maintain regular backup procedures and tested recovery capabilities sufficient to support the availability and recovery requirements set out in this Agreement;

10.5.6 provide Systemiq with the ability, upon request and upon expiry or termination of this Agreement, to export all EMInvest and Contributor Data in commonly used, machine-readable formats, securely delete such data upon Systemiq's written instruction, and provide all reasonable assistance required to facilitate the orderly transfer of EMInvest and Contributor Data to a future host; and

10.5.7 maintain and operate a secure software development lifecycle, including documented secure development procedures, code review, dependency and vulnerability scanning as part of the software development pipeline, and segregation of development, testing and production environments. The Contractor shall not use live financial or production data in any non-production environment unless expressly authorised by Systemiq and protected by equivalent security controls.

10.6 Prior to the Commencement Date, the Contractor shall provide evidence demonstrating compliance with this Clause 10, including details of its information security certifications, a summary of its information security controls, a list of all subcontractors and subprocessors that will process or have access to EMInvest, and a summary of the findings and remediation status of its most recent external penetration test. The Contractor shall promptly notify Systemiq of any material change to such information.

10.7 The Contractor acknowledges that compliance with this Clause 10 and the provision of satisfactory evidence of such compliance are material obligations under this Agreement. The Contractor shall cooperate with Systemiq in agreeing any additional security or data protection measures reasonably required before the Commencement Date or during the Term.

10.8 The Contractor is liable to Systemiq for all losses, costs, damages and expenses arising from any Security Incident to the extent caused by the Contractor, its personnel or its Subprocessors. Any limitation, exclusion or cap agreed elsewhere in this Agreement shall not exclude or limit the Partner’s liability to the extent prohibited by law.

11 Performance Standards

11.1 The Contractor shall perform the Services in accordance with the service levels set out in the RfP, as may be amended by agreement between the Parties from time to time.

11.2 Without limiting Clause 11.1, the Contractor shall ensure that the Services achieve, as a minimum, the following performance standards:

11.2.1 Platform availability of not less than 99.5% in each calendar month, excluding agreed planned maintenance;

11.2.2 planned maintenance to be scheduled outside agreed peak operating periods and notified to Systemiq at least 14 days in advance;

11.2.3 response to Critical Incidents, including where EMInvest is unavailable or EMInvest and/or Contributor Data is at material risk, within 4 hours of notification;

11.2.4 response to High Priority Incidents, including where a major EMInvest function is materially impaired, within 1 Business Day;

11.2.5 response to Normal Priority Incidents, including minor defects, service requests and user queries, within 3 Business Days;

11.2.6 operation of submission cycles in accordance with the agreed annual timetable, including achievement of all agreed publication deadlines;

11.2.7 validation of submitted data and communication of identified errors to Contributors within 3 Business Days of submission;

11.2.8 delivery of each data quality assurance report within 2 weeks following completion of the relevant submission cycle; and

11.2.9 notification to Systemiq of any actual or suspected Security Incident affecting EMInvest and/or Contributor Data in accordance with Clause 11.2.

11.3 The Contractor shall monitor its performance against the Performance Standards and shall provide performance reports to Systemiq at the intervals agreed between the Parties. Such reports shall include details of service availability, incident response performance, security incidents, maintenance activities, and any failures to meet the Performance Standards together with corrective actions taken or proposed.

11.4 Where the Contractor fails to meet any Performance Standard, the Contractor shall promptly investigate the cause of the failure, provide Systemiq with a written remediation plan, implement all reasonable corrective measures without delay, and take such further steps as are reasonably required to prevent recurrence.

11.5 Persistent, repeated or material failure by the Contractor to achieve the Performance Standards shall constitute a material breach of this Agreement and shall entitle Systemiq to exercise any remedies available under this Agreement, including the application of any agreed service credits, the conduct of continuation reviews and, where applicable, liability and termination rights as per clauses 7, 10 and 15.

12 Data protection

To the extent that any Personal Data is processed, the Parties will each comply with their respective obligations under the Data Protection Legislation.

13 Insurance

13.1 During this Agreement, both Parties shall maintain in force insurance policies with reputable insurance companies, against risks that would reasonably be insured against in connection with the risks associated with this Agreement, including cover for data breaches and cybersecurity incidents. The Contractor shall provide evidence of such insurance upon Systemiq's reasonable request.

14 Bribery and Anti-Corruption

14.1 The Parties each agree:

14.1.1 to comply with all applicable laws, regulations, and sanctions relating to anti-bribery and anti-corruption including but not limited to the applicable requirements of the Bribery Act 2010;

14.1.2 not engage in any activity, practice or conduct which would constitute an offence under sections 1, 2 or 6 of the Bribery Act 2010 if such activity, practice or conduct had been carried out in the UK;

14.1.3 not engage in any activity, practice or conduct which would constitute either:

(a) a UK tax evasion facilitation offence under section 45(1) of the Criminal Finances Act 2017; or

(b) a foreign tax evasion facilitation offence under section 46(1) of the Criminal Finances Act 2017;

14.1.4 to promptly report to the other Party any request or demand from a third Party to facilitate the evasion of tax within the meaning of Part 3 of the Criminal Finances Act 2017 or any suspected tax evasion offences or facilitation of tax evasion offences, whether under UK law or under the law of any foreign country, in connection with the performance of this Agreement; and

14.1.5 to promptly report to the other Party any request or demand for any undue financial or other advantage of any kind received by it in connection with the performance of this Agreement.

15 Termination

15.1 Without affecting any other right or remedy available to it, either Party may terminate this Agreement with immediate effect by giving written notice to the other Party if:

15.1.1 the other Party commits a material breach of any term of this Agreement and (if such breach is remediable) fails to remedy that breach within a period of 30 days after being notified in writing to do so;

15.1.2 the other Party repeatedly breaches any of the terms of this Agreement in such a manner as to reasonably justify the opinion that its conduct is inconsistent with it having the intention or ability to give effect to the terms of this Agreement;

15.1.3 the other Party suspends, or threatens to suspend, payment of its debts or is unable to pay its debts as they fall due or admits inability to pay its debts or (being a company or limited liability partnership) is deemed unable to pay its debts within the meaning of section 123 of the Insolvency Act 1986 (**IA 1986**) as if the words "it is proved to the satisfaction of the court" did not appear in sections 123(1)(e) or 123(2) of the IA 1986;

15.1.4 the other Party makes a resolution for its winding up, makes an arrangement or composition with its creditors or makes an application to a court of competent jurisdiction for protection from its creditors or an administration or winding-up order is made or an administrator or receiver is appointed in relation to the other Party;

15.1.5 the other Party suspends or ceases, or threatens to suspend or cease, carrying on all or a substantial part of its business;

15.1.6 the other Party has in the reasonable opinion of the terminating Party conducted its affairs (whether directly or indirectly) in a manner that is likely to, or will, have a negative effect on the reputation of the terminating Party or any aspect of its business; or

15.1.7 the other Party commits a breach of clause 14 (Bribery and Anti-Corruption).

15.2 Systemiq may terminate this Agreement (in whole or in part) for convenience with effect from the end of any project stage by giving the Contractor written notice. Without affecting any other right or remedy available to it, Systemiq may also terminate this Agreement with immediate effect (or on such shorter notice as it specifies) by giving written notice to the Contractor if: (a) the Systemiq Client Services Agreement is terminated; and/or (b) project funding is reduced, suspended or withdrawn (including by the relevant Systemiq Client). On termination, the Contractor shall be entitled only to payment of Fees for Services and Deliverables properly performed and accepted by Systemiq up to the effective date of termination (pro-rated for any portion of a month, where applicable), and no payment shall be due for unperformed work.

15.3 Systemiq shall only be liable to pay the Contractor once Systemiq is paid by the Systemiq Client in full. To the fullest extent permitted by law, Systemiq shall have no liability for any loss of profit, anticipated savings, or any indirect or consequential loss arising out of or in connection with such termination. Following termination, the Contractor shall promptly deliver to Systemiq all work-in-progress, materials and Deliverables (whether complete or not) and shall provide reasonable transition assistance on request.

16 Obligations on termination and survival

16.1 On termination or expiry of this Agreement, all existing Work Schedules shall terminate automatically.

16.2 Any provision of this Agreement that expressly or by implication is intended to come into or continue in force on or after termination of this Agreement shall remain in full force and effect.

16.3 Termination or expiry of this Agreement shall not affect any rights, remedies, obligations or liabilities of the Parties that have accrued up to the date of termination or expiry, including the right to claim damages in respect of any breach of the Agreement which existed at or before the date of termination or expiry.

17 Force majeure

17.1 **Force Majeure Event** means any circumstance not within a Party's reasonable control including, without limitation:

17.1.1 acts of God, flood, drought, earthquake or other natural disaster;

17.1.2 epidemic or pandemic, or any law or any action taken by a government or public authority as a result of an epidemic or pandemic;

17.1.3 terrorist attack, civil war, civil commotion or riots, war, threat of or preparation for war, armed conflict, imposition of sanctions, embargo, or breaking off of diplomatic relations;

17.1.4 nuclear, chemical or biological contamination or sonic boom;

17.1.5 any law or any action taken by a government or public authority, including without limitation imposing an export or import restriction, quota or prohibition, or failing to grant a necessary licence or consent;

17.1.6 collapse of buildings, fire, explosion or accident;

17.1.7 any labour or trade dispute, strikes, industrial action or lockouts (other than in each case by the Party seeking to rely on this clause, or companies in the same group as that Party);

17.1.8 non-performance by suppliers or subcontractors (other than by Affiliates of the Party seeking to rely on this clause); and

17.1.9 interruption or failure of utility service.

17.2 Provided it has complied with clause 17.4, if a Party is prevented, hindered or delayed in or from performing any of its obligations under this Agreement by a Force Majeure Event (**Affected Party**), the Affected Party shall not be in breach of this Agreement or otherwise liable for any such failure or delay in the performance of such obligations. The time for performance of such obligations shall be extended accordingly.

17.3 The corresponding obligations of the other Party will be suspended, and its time for performance of such obligations extended, to the same extent as those of the Affected Party.

17.4 The Affected Party shall:

17.4.1 as soon as reasonably practicable after the start of the Force Majeure Event notify the other Party in writing of the Force Majeure Event, the date on which it started, its likely or potential duration, and the effect of the Force Majeure Event on its ability to perform any of its obligations under the Agreement; and

17.4.2 use all reasonable endeavours to mitigate the effect of the Force Majeure Event on the performance of its obligations.

17.5 If the Force Majeure Event prevents, hinders or delays the Affected Party's performance of its obligations for a continuous period of more than 90 days, the Party not affected by the Force Majeure Event may terminate this Agreement by giving one month's written notice to the Affected Party.

18 Non-solicitation

18.1 The Contractor shall not, without the prior written consent of Systemiq, at any time from the Commencement Date to the expiry of six months after the Termination Date, solicit or entice away from Systemiq or employ or attempt to employ any person who is, or has been, engaged as an employee, officer, subcontractor or Substitute of Systemiq in the provision of the Services as set out in the Statement of Work.

18.2 In the event that the Contractor breaches clause 18.1, the Contractor will pay to Systemiq an amount equivalent to 20% of the then current annual remuneration of the Systemiq's employee, officer, subcontractor or Substitute or, if higher 20% of the annual remuneration to be paid by the Contractor to such person.

18.3 A general advertisement or notice of a job listing or opening or other similar general publication of a job search or availability to fill employment positions, including on the internet, shall not be construed as a solicitation or inducement for purposes of clause 18, and the hiring of any such employee, officer, subcontractor or Substitute who freely responds thereto shall not be a breach of this clause 18.

19 Compliance with Client Services Agreement

19.1 The Contractor acknowledges that Systemiq, may have undertaken certain obligations to a Systemiq Client under a Client Services Agreement, including without limitation, with regards to confidentiality, use of Systemiq's Client names, non-solicitation of employees, assignment and/or ownership of intellectual property rights, cyber security and IT requirements, and termination, which shall be set forth in such Client Services Agreement to the extent set forth in the relevant Client Service Agreement, the Contractor agrees to comply with all of the obligations applicable in such Client Services Agreement(s). The flow-down requirements are incorporated into and form part of this Contract and are attached as Annex B.

20 Assignment

20.1 The Contractor shall not assign, transfer, mortgage, charge, subcontract, delegate, declare a trust over or deal in any other manner with any of its rights and obligations under this Agreement.

20.2 Systemiq may at any time assign, mortgage, charge, delegate, declare a trust over or deal in any other manner with any or all of its rights under this Agreement, provided that Systemiq gives prior written notice of such dealing to the Contractor.

21 Variation

21.1 No variation of this Agreement shall be effective unless it is in writing and signed by the Parties (or their authorised representatives).

22 Waiver

22.1 A waiver of any right or remedy under this Agreement or by law is only effective if given in writing and shall not be deemed a waiver of any subsequent right or remedy.

22.2 A failure or delay by a Party to exercise any right or remedy provided under this Agreement or by law shall not constitute a waiver of that or any other right or remedy, nor shall it prevent or restrict any further exercise of that or any other right or remedy. No single or partial exercise of any right or remedy provided under this Agreement or by law shall prevent or restrict the further exercise of that or any other right or remedy.

22.3 A Party that waives a right or remedy provided under this Agreement or by law in relation to one Party, or takes or fails to take any action against that Party, does not affect its rights in relation to any other Party.

23 Rights and remedies

23.1 The rights and remedies provided under this Agreement are in addition to, and not exclusive of, any rights or remedies provided by law.

24 Severance

24.1 If any provision or part-provision of this Agreement is or becomes invalid, illegal or unenforceable, it shall be deemed deleted, but that shall not affect the validity and enforceability of the rest of this Agreement.

24.2 If any provision or part-provision of this Agreement is found to be invalid, illegal or unenforceable but would be valid, legal or enforceable if some part of the provision were deleted, the provision in question shall apply with such amendment, modification, abrogation, substitution, variation or compromise as may be necessary to make it valid, legal and enforceable.

24.3 If any provision or part-provision of this Agreement is deemed deleted under clause 24.1 (and if clause 24.2 does not apply) the Parties shall negotiate in good faith to agree a replacement provision that, to the greatest extent possible, achieves the intended commercial result of the original provision.

25 Entire agreement

25.1 This Agreement constitutes the entire agreement between the Parties and supersedes and extinguishes all previous agreements, promises, assurances, warranties, representations and understandings between them, whether written or oral, relating to its subject matter, save for any non-disclosure or confidentiality agreements entered into between the Parties (**NDA**).

25.2 Each Party agrees that it shall have no remedies in respect of any statement, representation, assurance or warranty (whether made innocently or negligently) that is not set out in this Agreement. Each Party agrees that it shall have no claim for innocent or negligent misrepresentation or negligent misstatement based on any statement in this Agreement.

26 Conflict

26.1 If there is an inconsistency between any of the provisions of this Agreement and the provisions of the NDA, a Work Schedule or the Contract Summary, the provisions of this Agreement shall prevail.

27 No partnership or agency

27.1 Nothing in this Agreement is intended to, or shall be deemed to, establish any partnership or joint venture between any of the Parties, constitute any Party the agent of another Party, or authorise any Party to make or enter into any commitments for or on behalf of any other Party.

27.2 Each Party confirms it is acting on its own behalf and not for the benefit of any other person.

28 Third Party rights

28.1 This Agreement does not give rise to any rights under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this Agreement.

29 Notices

29.1 Any notice or other communication given to a Party under, or in connection with, this Agreement shall be in writing and shall be:

29.1.1 delivered by hand or by pre-paid first-class post or other next business day delivery service at its registered office (if a company) or its principal place of business (in any other case); or

29.1.2 sent by email to:

SYSTEMIQ: Legal@systemiq.earth, with a copy to [INSERT PARTNER EMAIL ADDRESS]

Contractor: [INSERT EMAIL ADDRESS]

29.2 Any notice or communication shall be deemed to have been received:

29.2.1 if delivered by hand, at the time the notice is left at the proper address;

29.2.2 if sent by pre-paid first-class post or other next business day delivery services, at 9:00am on the second business day after posting; or

29.2.3 if sent by email, at the time of transmission, or, if this time falls outside business hours in the place of receipt, when business hours resume. In this clause 29.2, business hours means 9.00am to 5.00pm Monday to Friday on a day that is not a public holiday in the place of receipt. If the sender receives a server-generated response informing the sender that the email has not been delivered, that notice is not deemed received unless the sender is subsequently informed by that server, the intended recipient or the person for whose attention it was marked that it has been delivered.

29.3 This clause does not apply to the service of any proceedings or any documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

30 Counterparts

30.1 This Agreement may be executed in any number of counterparts, each of which shall constitute a duplicate original, but all the counterparts shall together constitute the one Agreement.

30.2 Transmission of an executed counterpart of this Agreement or the executed signature page of a counterpart of this Agreement by email (in PDF, JPEG or other agreed format) shall take effect as the transmission of an executed "wet-ink" counterpart of this Agreement.

30.3 No counterpart shall be effective until each Party has executed and delivered at least one counterpart.

31 Dispute Resolution Procedure

31.1 If a dispute arises out of, or in connection with, this Agreement or the performance, validity or enforceability of it (**Dispute**) then, subject to clause 31.2, the Parties shall follow the procedure set out in this clause:

31.1.1 either Party shall give to the other written notice of the Dispute, setting out its nature and full particulars (**Dispute Notice**), together with relevant supporting documents. On service of the Dispute Notice, the Contractor Representative and the Systemiq Representative (each of which is identified in the Contract Summary) shall attempt in good faith to resolve the Dispute; and

31.1.2 if Systemiq Representative and the Systemiq Representative are for any reason unable to resolve the Dispute within 30 days of service of the Dispute Notice, the Dispute shall be referred to more senior officers (if any) of each of the Contractor and Systemiq who shall attempt in good faith to resolve it.

31.2 No Party may commence any court proceedings under clause 33 in relation to the whole or part of the Dispute until the Parties have attempted to resolve the Dispute in the manner set out in clause 31.1, save that nothing shall prevent either Party from seeking urgent injunctive relief and provided that the right to issue proceedings is not prejudiced by completing such process.

32 Governing law

This Agreement and any dispute or claim (including non-contractual disputes or claims) arising out of, or in connection with, it or its subject matter or formation shall be governed by and construed in accordance with the law of England.

33 Jurisdiction

33.1 Each Party irrevocably agrees that the courts of England shall have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims) arising out of, or in connection with, this Agreement or its subject matter or formation.

This Agreement has been entered into on the date stated at the beginning of it.

SYSTEMIQ

APPENDIX 1 | WORK SCHEDULE NO.1

Work Schedule Number: No. 1

Date: [ ]

This Work Schedule is an Appendix to the agreement for the provision of services entered into between Systemiq Limited ("**Systemiq**") and [name of company"] ("**Contractor**") to which this Appendix 1 is attached(the "**Agreement**").

1.	The Services	[ ]
2.	Deliverables	[insert deliverables, but limit this to items you can guarantee you can produce]
3.	Timetable	[*insert timetable*]
4.	Fees	[insert] (exclusive VAT) [plus the following expenses: [LIST ANY EXPENSES]
5.	Instalment Dates and Amounts:	[INSERT]
6.	Invoice payment terms	Invoices are payable in accordance with clause 6 of the Services Agreement.

The Parties agree that the Services set out in this Work Schedule shall be provided on the terms and conditions of the Agreement.

Signed for and on behalf of [Sub-contractor Name]:	**Signed for and on behalf of Systemiq Limited:**
Signature:	Signature: ....
Name:	Name: ....
Position:	Position: ....
Date:..	Date:..