An Coimisiún um Rialáil Fóntas
Commission for Regulation of Utilities

Request for Tenders for the establishment of a Single Member Framework Agreement for the Provision of ICT Managed Services 2026-30

CRU File Ref: 011-03-609

Tender Procedure: Open Procedure

Tender Deadline 12.00 noon 3 March 2026

Contents

Definitions

Capitalised terms have the meaning given to them in the Framework Agreement or Statement of Work (SOW), unless they are defined below in this RFT in which case they have the meaning given to them in this RFT. In addition, capitalised terms not defined below or in the Framework Services Agreement or Statement of Work (SOW) have the meaning given to them in the Requirement and Specifications.

Approved Assumption means, if applicable, any assumptions, approved in writing by the Contracting Authority, with the result that a Tenderer may include such approved assumption in its Tender (though the Contracting Authority will not be bound by any Approved Assumptions and no Approved Assumptions will be incorporated in the Framework Agreement, unless specified otherwise by the Contracting Authority when approving the Approved Assumption) (and, if the Competition is split into Lots, includes, as the context so admits or requires, the Approved Assumptions in respect of any one, more or all Lots).

Award Criteria mean, as the context so admits or requires, any one, more or all of the Award Criteria set out in part 3.3 of the RFT (and, if the Competition is split into Lots, includes, as the context so admits or requires, any one, more or all of the Award Criteria in respect of any one, more or all Lots).

Competition means the public procurement competition provided for by this RFT.

Contracting Authority means the CRU.

Contract Comments Deadline has the meaning given to it in paragraph 2.3.2.

Contractor means the successful Tenderer who enters into a Framework Services Agreement with the Contracting Authority (and, if the Competition is split into Lots, includes, as the context so admits or requires, the Contractor in respect of any one, more or all Lots.

CRU means the Commission for Regulation of Utilities.

ESPD means the European Single Procurement Document ("**ESPD**")

Exclusion Grounds means the circumstances and grounds set out in Article 57 of the Procurement Regulations.

Evaluation Committee means the evaluation committee appointed by the Contracting Authority, as provided for by part 3.7 (and, if the Competition is split into Lots, includes, as the context so admits or requires, the Evaluation Committee in respect of any one, more or all Lots, each of which may be the same or different to that for other Lots).

Framework means the framework established between the Contracting Authority and the party to the Framework Agreement**.**

Lots means, if the Competition is split into Lots, the Lots more particularly described in paragraph 1.2 (and includes, as the context so admits or requires, any one, more or all Lots).

Preferred Tenderer means the Tenderer provisionally appointed by the Contracting Authority as the Preferred Tenderer following the evaluation of Tenders (and, if the Competition is split into Lots, includes, as the context so admits or requires, the Preferred Tenderer for any one, more or all Lots).

Procurement Directive means Directive 2014/24/EU of the European Parliament and of the Council on Public Procurement.

Procurement Regulations means S.I. No. 284/2016 European Union (Award of Public Authority Contracts) Regulations 2016.

Requirements and Specifications means the requirements and specifications in respect of the Services as set out in Appendix 1 of this RFT (and, if the Competition is split into Lots, includes, as the context so admits or requires, the Requirements and Specifications for any one, more or all Lots).

RFT means this request for Tenders, together with any written clarifications in respect of it issued by the Contracting Authority.

Selection Criteria mean, as the context so admits or requires, any one, more or all of the selection criteria set out in part 3.2 of the RFT (and, if the Competition is split into Lots, includes, as the context so admits or requires, any one, more or all of the Selection Criteria in respect of any one, more or all Lots).

Services means the Services to be performed under the Statement of Work (SOW), awarded pursuant to a Framework Agreement, as more particularly described in the Requirement and Specifications (and, if the Competition is split into Lots, includes, as the context so admits or requires, the Services in respect of any one, more or all Lots).

Statement of Work (SOW), means the terms to be entered into between the Contractor and Contracting Authority, pursuant to the Services Framework Agreement, a copy of which is set out in draft form in Appendix 5 (Schedule 7) of this RFT.

SME means small and medium enterprises.

Standstill Period has the meaning given to it in paragraph 3.5.1.

Tender means a tender submitted by a Tenderer in response to this RFT, together with any written clarifications in respect of it submitted by the Tenderer to the Contracting Authority in accordance with this RFT (and includes, as the context so admits or requires, any one, more or all Tenders) (and, if the Competition is split into Lots, includes, as the context so admits or requires, any one, more or all Tenders in respect of any one, more or all Lots).

Tender Deadline has the meaning given to it in paragraph 2.6.5.

Tenderer means any person who has submitted, or intends to submit, a Tender in response to this RFT and, where the Tenderer is a consortium or group, reference to a Tenderer includes the members of that consortium or group (and includes, as the context so admits or requires, any one, more or all of the Tenderers) (and, if the Competition is split into Lots, includes, as the context so admits or requires, the Tenderers in respect of any one, more or all Lots).

Term has the meaning given to it in paragraph 1.4.

Part 1: Introduction

1.1 The Contracting Authority invites Tenders in response to this RFT from Tenderers for the provision of the Services as described in Appendix 1 to this RFT. In summary, the Services comprise a Single Member Framework Agreement for the provision of ICT Managed Services, Ad-hoc Project Work and Managed Security Operations Centre (SOC) Services. The open procedure is being used for this Competition.

1.2 Not Used

1.3 Variant Tenders are not permitted.

1.4 Any Services Framework Agreement that may result from this Competition will be issued for a term of 24 months ("**Term**").

1.5 The Contracting Authority will have the right to extend the Term for a period or periods of up to a total of 24 Months with a maximum of 1 (one) such extension on the same terms and conditions, subject to the Contracting Authority's obligations at law.

1.6 The Contracting Authority estimates that the expenditure on the Services to be covered by the proposed Services Framework Agreement for the Term (including any potential extension of the Term) is in the order of approximately: up to a sum in the order of €3.5 million (excl. VAT). Tenderers must understand that this figure is an estimate only based on current and future expected usage.

1.7 Contracting Authority policy seeks to encourage participation on a fair and equal basis by SMEs in this Competition. SMEs that believe the scope of this Competition is beyond their technical or business capacity are encouraged, subject to part 2.5, to explore the possibilities of forming relationships with other SMEs or with larger enterprises. Through such relationships they can participate and contribute to the successful implementation of any Services Framework Agreement that may result from this Competition and thereby increase their social and economic benefits.

1.8 Larger enterprises are also encouraged, subject to part 2.5, to consider the practical ways that SMEs can be included in their proposals to maximise the social and economic benefits of any Services Framework Agreement that may result from this Competition.

1.9 Tenderers are responsible for communicating the terms of the RFT (including clarifications) to their members, subcontractors and other persons involved in their Tender.

1.10 **Submission of Tenders:**

Tenderers are required to complete and submit a separate tender response document ("**Tender Response Document" / "TRD**") as per requirements as set out in 2.6 of this RFT.

Tender Response Format

Tenderers should note that it is a **mandatory requirement** of this Competition for Tenderers to complete, the Tender Response Document provided as a separate attachment to this RFT. The purpose of the TRD is to simplify and streamline the tender response process for all Tenderers and to simplify and streamline the evaluation process for the Contracting Authority.

The TRD comprises of;

1. **Document A** - Qualification Response Document (Selection Criteria and required compliance declarations)
2. **Document B** - Non Cost Award Criteria Response Document
3. **Document C** - Cost Award Criteria Response Document
4. European Single Procurement Document (**ESPD**)

Note: Use of the European Single Procurement Document

Tenderers are required to complete and submit with their Tender Response an electronic version of the European Single Procurement Document ("ESPD"). In accordance with Directive 2014/24/EU, tenderers may have compiled a European Single Procurement Document (ESPD), either electronically via the eESPD on eTenders or as a separate uploaded attachment with the tender response.

Tenderers may submit an eESPD which has already been used in a previous procurement procedure provided that they confirm that:

(i) the information contained in it continues to be correct and

(ii) that they satisfy the Selection Criteria for this Competition as set out at part 3.2 below.

The TRDs must be submitted in accordance with the submission requirements in paragraph 2.6.1 of this RFT. The Tenderer's response in the Tender Response Document must also address all of the requirements of this RFT.

Part 2: Instructions to Tenderers

2.1: Important Notice

2.1.1 The Contracting Authority has prepared this RFT for the sole purpose of inviting Tenders from the Tenderers for the Services.

2.1.2 The information set out in the RFT is being made available on condition that it is only used in connection with this Competition and for no other purpose whatsoever. It is provided as a guide only and does not purport to contain all the information that a Tenderer may require in connection with any Services Framework Agreement. In no circumstances shall the Contracting Authority or its advisers, consultants, contractors and/or agents incur or have any liability or responsibility arising out of or in respect of this RFT or its issue.

2.1.3 The information provided in the RFT is offered in good faith for the guidance of Tenderers but no warranty or representation, express or implied, is given as to the accuracy or completeness of any of the information set out in the RFT or on which the RFT is based or issued pursuant to the RFT.

2.1.4 The Contracting Authority and its advisers, consultants, contractors and/or agents shall not under any circumstances whatsoever have any liability for the accuracy, adequacy or completeness of the RFT or for any other written or other communication made available during the course of the Competition including, without limitation, for any loss, damage, cost or expense incurred or arising as a result of reliance on such information or communication. Where information in the RFT is cited from a third party source, such information has not been independently verified.

2.1.5 The Contracting Authority reserves the right to amend the RFT, its requirements and any information contained in it at any time by notice, in writing, to the Tenderers.

2.1.6 The Contracting Authority reserves the right to take such steps as it considers appropriate, including (but not limited to):

(a) changing the basis of, or the procedures (including the timetable) relating to, the tender process;
(b) rejecting any, or all, of the Tenders;
(c) not inviting a Tenderer to proceed further;
(d) not furnishing a Tenderer with additional information; or
(e) abandoning the Competition.

2.1.7 Nothing in the RFT is, or may be relied upon as, a promise or representation as to the Contracting Authority's ultimate decision in relation to the award of the Services Framework Agreement which is the subject of this Competition, or as a representation of fact or promise as to the future. None of the information contained in the RFT shall impose any legal obligations on the Contracting Authority and there is and will be no collateral contract imposing obligations on the Contracting Authority. No contractual rights as against the Contracting Authority will exist unless, and until, a formal written Services Framework Agreement / SOW has been executed by or on behalf of the Contracting Authority with the Contractor concerned and it has taken legal effect in accordance with its terms.

2.1.8 The Contracting Authority and its advisers, consultants, contractors and/or agents do not accept or have any responsibility for the legality, validity, effectiveness, adequacy or enforceability of any documentation executed, or which may be executed, in relation to the Services.

2.1.9 The Contracting Authority is not obliged to appoint any of the Tenderers to undertake the Services and reserves the right not to proceed with the award process and to withdraw from the process at any time. No contract to be entered into with a Contractor will contain any representation or warranty from the Contracting Authority in respect of the RFT.

2.1.10 The RFT is being made available by the Contracting Authority to Tenderers on the terms set out in the RFT only. The RFT is not being distributed to the public nor has it been filed, registered or approved in any jurisdiction. Its possession or use in any manner contrary to any applicable law is expressly prohibited. Tenderers shall inform themselves concerning, and shall observe, any applicable legal requirements.

2.1.11 Each Tenderer's downloading or acceptance of delivery of the RFT constitutes its agreement to, and acceptance of, the terms set forth in this important notice and the RFT.

2.1.12 The Contracting Authority does not bind itself to accept the lowest priced or any Tender.

2.1.13 The RFT does not constitute an offer or commitment to enter into a Services Framework Agreement .

2.1.14 Any notification of Preferred Tenderer status by the Contracting Authority is provisional and shall not give rise to any enforceable rights or legitimate interest of the Preferred Tenderer and may be withdrawn at the discretion of the Contracting Authority.

2.1.15 The award of a Services Framework Agreement does not confer exclusivity on the Contractor, unless (and in that case only to the extent that), if applicable, the contrary is expressly stated in the Services Framework Agreement .

2.1.16 The Contracting Authority may (but is not obliged to) issue an updated version of this RFT in which case the most recent version will supersede and replace any earlier version. This RFT supersedes and replaces any and all previous documentation, communications and correspondence between the Contracting Authority and Tenderers, and Tenderers should place no reliance on such previous documentation and correspondence.

2.1.17 In this important notice, references to the RFT includes all information contained in the RFT, any accompanying documentation, and/or information and/or opinions made available during the remainder of the Competition by or on behalf of the Contracting Authority and/or its advisers, consultants, contractors, servants and/or agents in connection with the RFT or the Services including, without limitation, the information made available in response to any queries submitted by Tenderers.

2.2: Compliant Tenders

2.2.1 Tenderers must participate in this Competition subject to, and in accordance with, the requirements of this RFT and in accordance with any other requirements communicated from time to time to Tenderers by the Contracting Authority.

2.2.2 A Tenderer which fails to fully comply with the RFT or any other requirements communicated from time to time to the Tenderer by the Contracting Authority to the satisfaction of the Contracting Authority may, subject to paragraph 2.2.3, be treated as failing to comply with mandatory conditions of this RFT and may, at the absolute discretion of the Contracting Authority and subject to paragraph 2.2.3, be rejected and eliminated from this Competition.

2.2.3 If a Tenderer's Tender fails to comply in any respect with any of the requirements set out in the RFT (whether or not stated to be mandatory or similar) or the Contracting Authority considers the Tender be ambiguous or require clarification or amplification in any respect, the Contracting Authority is entitled (but is not obliged), subject to applicable law, to take such action as it considers appropriate including:

(a) to reject the relevant Tenderers' Tender which is non-compliant with any requirement of the RFT (whether or not stated to be mandatory or similar) and eliminate the Tenderer; or

(b) without prejudice to the Contracting Authority's right (where there is non-compliance) to reject the Tenderer's Tender in a given case as non-compliant:

(i) to meet with, raise issues and/or seek clarification, amplification or supplementary information from the Tenderer in respect of the Tender and/or the non-compliance;

(ii) to request the Tenderer to provide the Contracting Authority with information on items or items or documents which have not been provided or have been provided in an incorrect form or on an incorrect basis or are incomplete or erroneous; and/or

(iii) to waive a requirement which, in the opinion of the Contracting Authority, is appropriate in the circumstances (particularly if it is minor and/or procedural) and to proceed to evaluate such Tender in accordance with the RFT,

provided that no material amendments may be made to a Tender in a given case where this would give rise to a breach of applicable law.

2.2.4 Tenderers are required to comply with and facilitate any requests in this respect within such timeline as the Contracting Authority may, in its absolute discretion, stipulate.

2.2.5 The Contracting Authority has final determination on whether a Tender is compliant or non-compliant.

2.3: Services Framework Agreement

2.3.1 Tenderers should note the terms and conditions of the Services Framework Agreement at Appendix 5 to this RFT.

2.3.2 Tenderers are permitted to submit, not later than 12 noon local Irish time on **16 February 2026** or such revised date as is published by the Contracting Authority on e-Tenders ("**Contract Comments Deadline**"), comments on the Services Framework Agreement . The comments should set out the Tenderer's concern with any specific provisions and suggested amendment to them. Comments such as "subject to further discussion" or "subject to negotiations" should not be made as they do not give the Contracting Authority any insight as to the Tenderer's concern and, as a result, will not inform any possible changes to be made by the Contracting Authority to the Services Framework Agreement . The Contracting Authority, following receipt of any comments, will consider the comments submitted by Tenderers and then, prior to the Tender Deadline, either (at its discretion):

(a) issue a revised draft of the Services Framework Agreement reflecting such changes to it as the Contracting Authority wishes to make; or

(b) confirm that the original draft of the Services Framework Agreement continues to apply unamended.

The Contracting Authority normally does not expect to give Tenderers a further opportunity to submit additional comments on the Services Framework Agreement after this prior to submission of Tenders, but it reserves the right to do so (in which case this paragraph 2.3.3 will apply again).

2.3.3 Tenderers should note that public procurement rules constrain the Contracting Authority's ability to make changes at the Preferred Bidder stage. Accordingly, Tenderers should use the opportunity to submit comments prior to the Contract Comments Deadline.

2.3.4 Tenderers are required, when submitting their Tenders, to confirm their acceptance of the most recent version (published prior to the Tender Deadline) of the terms and conditions of the Services Framework Agreement by signing the Tenderer's statement at Appendix 3.

2.4: Acceptance of RFT Requirements

2.4.1 By downloading this RFT, submitting a Tender in response to this RFT and/or by participating in this Competition, each Tenderer (including, without limitation, every individual member of a Tenderer) irrevocably and unconditionally accepts, and agrees to, the terms and conditions of this RFT and is legally bound by it.

2.4.2 All Tenderers MUST return, with their Tender, a scanned signed copy of the Tenderer's statement, as set out in Appendix 3, printed on the Tenderer's letterhead. The Contracting Authority must be able to read the scanned signature of the Tenderer. If possible, please sign documents using blue ink. If the Contracting Authority cannot read the scanned signature, Tenderers may be requested to re-submit. Tenderers may not amend the Tenderer's statement.

2.5: Consortia, Prime/Subcontractors and Reliance on Third Parties

2.5.1 Where a group of undertakings (in whatever form and regardless of the legal relationship between them) come together to submit a Tender in response to this RFT, the Contracting Authority will deal with all matters relating to this Competition through a single nominated entity authorised to represent all members of the group of undertakings.

2.5.2 The Tenderer must clearly set out the name, title, telephone number, postal address, facsimile number and e-mail address of the nominated contact personnel of the entity authorised to represent the Tenderer and to whom all communications shall be directed and accepted until this Competition has been completed or terminated. Correspondence from any other person (including from any subcontractor) will normally not be accepted, acknowledged or responded to.

2.5.3 With regard to criteria relating to economic and financial standing and to criteria relating to technical and professional ability, a Tenderer or a member or subcontractor of a Tenderer may, where appropriate and for a particular contract, rely on the capacities / resources of other entities, regardless of the legal nature of the links which it has with them (including, for example, but not limited to, reliance on a parent company's resources / capacities).

2.5.4 However, criteria relating to the educational and professional qualifications or to the relevant professional experience, capacities / resources of other entities may only be relied upon where the latter will perform the Services for which these capacities / resources are required.

2.5.5 Where an economic operator relies on the capacities of other entities with regard to criteria relating to economic and financial standing, the Contracting Authority may require that the Tenderer and those entities be jointly liable for the execution of a Services Framework Agreement.

2.5.6 Where a Tenderer or a member or subcontractor of a Tenderer wants to rely on the capacities of other entities, the Tenderer must prove to the Contracting Authority that it will have at its disposal the resources necessary, including by producing a letter from such supporting entity confirming that it is committed to providing the necessary resources / capacities (including details of the resources which will be made available and the basis upon which those resources will be made available).

2.5.7 A guarantee or other form of contractual commitment in favour (at the Contracting Authority's discretion) of either or both the Contractor and Contracting Authority may, at the Contracting Authority's discretion, be required at contract execution stage from such supporting entities as a condition of contract award.

2.5.8 Where any Tenderer (or member or subcontractor of the Tenderer) is relying on the resources of another undertaking, then the ESPD must be provided both in respect of that organisation and in respect of the entity whose resources / capacity is being relied upon by that organisation.

2.5.9 The Contracting Authority:

(a) shall require that the Tenderer replaces an entity which does not meet a relevant Selection Criterion, or in respect of which there are compulsory grounds for exclusion under Article 57 of the Procurement Regulations, and

(b) may (at its discretion) require that the Tenderer substitutes an entity in respect of which there are non-compulsory grounds for exclusion under Article 57 of the Procurement Regulations.

2.6: Tender Submission Requirements

2.6.1 Tenderers, subject to paragraph 2.2.3, are required, in particular, to:

(a) Follow the format of this RFT and respond to each element in the order as set out in this RFT.

(b) Complete and submit with their Tender the European Single Procurement Document ("**ESPD**"). **Note:** A tenderer may reuse an ESPD response submitted previously for another competition where the tenderer confirms where it confirms that the information contained in that ESPD continues to be correct.

(c) Submit all documentation which this RFT requires to be submitted with their Tender.

(d) Conform and comply with all instructions and requirements set out in this RFT.

(e) Submit the statement required under paragraph 2.4.2.

(f) Submit the statement required under paragraph 2.3.4.

(g) Not alter or edit this RFT in any way.

2.6.2 Tenderers should note that where a Tenderer or a member or subcontractor of a Tenderer is relying on the capacity or resources of other entities in accordance with paragraph 2.5, it must:

(a) complete and submit a separate ESPD in respect of each such entity which is being relied upon; and

(b) provide a letter from such supporting entity demonstrating that it is committed to providing the necessary resources / capacities (including details of the resources / capacity which will be made available and the basis upon which those resources will be made available).

2.6.3 Tenders must be submitted via the electronic post-box available on www.etenders.gov.ie. Only Tenders submitted to the electronic post-box will be accepted. Tenders submitted by any other means (including but not limited to by email, fax, post or hand delivery) will NOT be accepted.

2.6.4 Tenderers must ensure that they give themselves sufficient time to upload and submit all required Tender documentation before the Tender Deadline. Tenderers should take into account the fact that upload speeds vary. There is a maximum of 2GB for the total (combined) documents sent to the electronic post-box; the maximum size for a single file uploaded to the eTenders platform is 250MB. In order to submit a document to the electronic post-box, please note that you must click "submit response". After submitting you can still modify and re-send your response up until the response deadline. Tenderers should be aware that the 'submit response' button will be disabled automatically upon the expiration of the response deadline.

2.6.5 Tenders must be received not later than 12 noon local Irish time on **3 March 2025**, or such revised date as is published by the Contracting Authority on e-Tenders ("**Tender Deadline**").

2.6.6 Other than in exceptional circumstances (as determined by the Contracting Authority), Tenders that are received late will not be considered in this Competition. The Contracting Authority may accept a Tender or, if applicable, part of a Tender that is not submitted by the Tender Deadline where the Contracting Authority considers that the principle of proportionality, in exceptional circumstances, requires the acceptance of the Tender or omitted part of the Tender and doing so would not breach the principles of transparency and equal treatment. Where the Tenderer has acted responsibly and in accordance with the RFT, and something occurs that is not within its control (albeit that it need not necessarily be entirely outside its control) which has frustrated due compliance with a deadline (such as failure to achieve deadlines as a result of power or Internet failure, or force majeure, or where the lateness is due to the fault of the Contracting Authority), this, absent some clear or identifiable fault on the part of the Tenderer, may *prime facie* constitute exceptional circumstances where the Contracting Authority may consider exercising its discretion under this provision, but depending on the facts, other circumstances may be "exceptional circumstances" where the Contracting Authority may consider that proportionality would require acceptance of the late submission. The decision of the Contracting Authority whether or not to accept a late Tender (or part of it) is final.

2.6.7 Tenders must be submitted in English. All financial information submitted should be denominated in Euros (EUR).

2.6.8 Each Tenderer is, subject to paragraph 2.18.1, limited to submitting one Tender in its own capacity and one Tender as part of a consortium/group of undertakings under this RFT.

2.6.9 All Tenders submitted in soft copy must be compiled such that they can be read immediately using PDF or Microsoft Word. The Contracting Authority is not responsible for corruption in electronic documents. Tenderers must ensure electronic documents are not corrupt. Tenders, subject to paragraph 2.6.6, may not be re-submitted after the deadline for submissions if they cannot be read immediately using PDF or Microsoft Word.

2.6.10 Tenderers must disclose all relevant information in their Tenders and otherwise. Tenderers that, or that attempt to, withhold any information that the Tenderer knows to be relevant, or to mislead the Contracting Authority, may, at the Contracting Authority's absolute discretion, be rejected and eliminated from this Competition.

2.6.11 If a Services Framework Agreement is awarded to a Tenderer that has knowingly withheld relevant information or misled the Contracting Authority, the Services Framework Agreement may, at the Contracting Authority's absolute discretion, be rendered null and void.

2.7: Queries and Clarifications

2.7.1 Each Tenderer must fully satisfy itself as to the nature and requirements of the RFT. In addition, if a Tenderer considers that any aspect of the RFT is not clear or is ambiguous or contains errors, or if a Tenderer has any queries regarding the scope of the Services or the manner in which the evaluation will be undertaken or the manner in which any of the Award Criteria (including any sub-criteria), minimum requirements or other requirements will be applied, this must be raised with the Contracting Authority in accordance with this paragraph.

2.7.2 All queries relating to any aspect of this Competition or of this RFT must be directed to the messaging facility on www.etenders.gov.ie. Queries will be accepted no later than 17.00 hours local time on **16 February 2026** (or such later date published by the Contracting Authority on eTenders). For the avoidance of doubt, Tenderers may not contact the Contracting Authority directly regarding any aspect of this Competition.

2.7.3 All responses to queries will be issued by the Contracting Authority via the messaging facility on www.etenders.gov.ie. Where appropriate, queries may be amalgamated. Tenderers should note that, subject to paragraphs 2.7.4 and 2.7.5, the Contracting Authority will not respond to individual Tenderers privately.

2.7.4 If a Tenderer believes a query and/or the response relates to a confidential aspect of its Tender, it must mark the query as "confidential". If the Contracting Authority, at its absolute discretion, is satisfied that the query and/or its response should be properly regarded as confidential, the nature of the query and its response shall, subject to paragraph 2.7.5, be kept confidential.

2.7.5 If the Contracting Authority is of the opinion that it would be inappropriate to answer the query/request on a confidential basis it will notify the Tenderer and require the Tenderer to either withdraw or reformulate the query or to raise any objection within two (2) days of such notification and state the grounds for its objection. If the Tenderer does not withdraw or reformulate the query/request or raise any objection within the specified period, or the Contracting Authority is of the opinion that, notwithstanding the objection of the Tenderer, the query/request is not confidential, the Contracting Authority may issue the query and its response to all of the Tenderers.

2.7.6 The Contracting Authority reserves the right to issue or seek written clarifications.

2.7.7 The Contracting Authority reserves the right, at any time before the Tender Deadline, to update or amend the information contained in this document and/or to extend the Tender Deadline. Participating Tenderers will be informed of any such amendment or extension through the eTenders website.

2.7.8 Tenderers should ensure that they register their interest in this Competition, by clicking "Express Interest", in the CfT (Call for Tenders) Workspace on www.etenders.gov.ie, in order to receive all responses to queries and other updates in relation to this Competition.

2.7.9 The Contracting Authority does not accept responsibility for any communications issued by it which are missed or not received by a Tenderer or for communications issued by Tenderers which are not received by the Contracting Authority. The onus is on a Tenderer to follow up with the Contracting Authority if no response is received. The Contracting Authority may not follow up on out of office or message failure notices received. Accordingly, Tenderers should ensure that valid contact details have been provided when registering for the eTenders website and that such emails are monitored.

2.8: Tendering Costs

2.8.1 All costs and expenses incurred by Tenderers relating to or arising out of or in connection with their participation in this Competition (including, but not being limited to, site visits, field trials, demonstrations and/or presentations) shall be borne by and are a matter for discharge by the Tenderers exclusively. This applies in all cases whatsoever, including where the Competition is terminated and/or errors are made in the running and decision making in the Competition.

2.9: Confidentiality

2.9.1 All documentation, data, statistics, drawings, information, patterns, samples or material disclosed or furnished by the Contracting Authority to Tenderers during the course of this Competition:

(a) is furnished for the sole purpose of replying to this RFT only;

(b) may not be used, communicated, reproduced or published for any other purpose without the prior written permission of the Contracting Authority;

(c) shall be treated as confidential by the Tenderer and by any third parties (including subcontractors) engaged or consulted by the Tenderer; and

(d) must be returned immediately to the Contracting Authority upon cancellation or completion of this Competition if so requested by the Contracting Authority.

2.10: Pricing

2.10.1 All Tenderers must complete the Pricing Schedule at Appendix 2 to this RFT.

2.10.2 All prices quoted must be all-inclusive (i.e. including but not being limited to shipping, packaging, delivery, ancillary costs and all other costs/expenses), be expressed in Euro and exclusive of VAT. The VAT rate(s) where applicable should be indicated separately.

2.10.3 Tenderers must confirm that all prices quoted in the Tender will remain valid for 160 days commencing from the Tender Deadline. This period may be extended where the Tender validity period is extended pursuant to paragraph 2.23.3.

2.10.4 Any currency variations occurring over the term of the Services Framework Agreement shall be borne by the Tenderer.

2.10.5 Payments for Services provided pursuant to this RFT shall be subject to and made in accordance with the Services Framework Agreement at Appendix 5 to this RFT.

2.10.6 Not Used

2.10.7 Where the Contracting Authority is concerned that a Tenderer's rates and/or price may be abnormally low, the Contracting Authority may (but, except, if applicable, to the extent required under applicable law, is not obliged to), at its sole discretion:

(a) request further explanation and evidence, either in writing or in the form of additional financial analysis, of those parts of the Tender which it considers may contribute to the prices and/or rates being abnormally low;

(b) take account of the further explanation and evidence submitted by the Tenderer in response to the request; and

(c) subsequently verify the parts of Tender that the Contracting Authority believes to be abnormally low with the Tenderer.

2.10.9 The Contracting Authority reserves the right (but, except, if applicable, to the extent required under law, is not obliged to) to reject a Tender which is considered to be abnormally low, in particular, where:

(a) the Tenderer fails to provide the information requested;

(b) the further explanation and evidence provided by the Tenderer does not satisfactorily explain the abnormally low price or rates; and/or

(c) the abnormally low rates or prices are due to a failure to (or proposed failure as evident from the Tender) to comply with provisions for employment protection and working conditions applicable to the place where any work is to be carried out or where any products or Services are to be supplied; and/or

(d) the abnormally low rates or price are a result of the Tenderer's non-compliance (or proposed non-compliance as evident from the Tender) with one or more of the conditions and/or requirements of this Competition as set out in the RFT or the Services Framework Agreement.

2.11: Environmental, Social and Labour Law

2.11.1 In the performance of any Services Framework Agreement awarded, the Contractor and its subcontractors (if any) shall be required to comply with all applicable obligations in the field of environmental, social and labour law that apply at the place where the Services are provided that have been established by EU law, national law, collective agreements or by international, environmental, social and labour law listed in Annex X of the Procurement Directive.

2.11.2 The Contractor shall be required to comply fully with the provisions of Council Directive 2001/23/EC of 12 March 2001 on the approximation of the laws of the Member States relating to the safeguarding of employees' rights in the event of

transfers of undertakings, business or parts of undertakings or business and as implemented in Irish law by Statutory Instrument S.I. No. 131 of 2003, the European Communities (Protection of Employees on Transfer of Undertakings) Regulations 2003 and, in particular, to indemnify and hold harmless the Contracting Authority for any claim arising or loss or costs incurred as a result of its failure or incapacity to fulfil its obligations under the said directive and statutory instrument. The Services Framework Agreement may contain more detailed provisions in such regard.

2.11.3 The Protection of Employees (Temporary Agency Work) Act 2012 (the "**2012 Act**") provides that an agency worker (as defined in the 2012 Act) is entitled to the same basic working and employment conditions as those which apply to employees recruited directly by the hirer (as defined in the 2012 Act) to do the same or a similar job. Where the provision of the Services will involve the provision to the Contracting Authority of agency workers (within the meaning of the 2012 Act), Tenderers should ensure that they consider and have regard to their obligations under the 2012 Act when pricing their Tender. The Contracting Authority shall have no liability for any increase in salaries or costs that may be payable as a result of the application of the 2012 Act to the provision of the Services as relevant to the Contracting Authority.

2.12: Publicity

2.12.1 No publicity regarding this Competition or any Services Framework Agreement pursuant to this Competition is permitted by a Tenderer or other person unless and until the Contracting Authority has given its prior written consent to the relevant communication. This does not limit or affect the Contracting Authority's right to publicise any elements of this Competition.

2.13: Registrable Interest

2.13.1 Any registrable interest involving any Tenderer or member or subcontractor of a Tenderer and the Contracting Authority, members of the Government of Ireland, members of the legislative body of Ireland or employees and officers of the Contracting Authority and their relatives must be fully disclosed in the Tender or, in the event of this information only coming to the notice of the Tenderer or member or subcontractor of the Tenderer after the submission of a Tender, must be communicated to the Contracting Authority immediately upon such information becoming known to the Tenderer or member or subcontractor of the Tenderer.

2.13.2 The terms "registrable interest" and "relative" shall be interpreted as per Section 2 of the Ethics in Public Office Acts 1995 and 2001 (as amended).

2.13.3 The Contracting Authority will, at its absolute discretion, decide on the appropriate course of action which may, in appropriate circumstances, include eliminating a Tenderer from this Competition or terminating any Services Framework Agreement / Statement of Work entered into by a Tenderer.

2.14: Anti-Competitive Conduct

2.14.1 Tenderers' attention is drawn to the Competition Act 2002 (as amended, the "2002 Act"). The 2002 Act makes it a criminal offence for Tenderers to collude on prices or terms in a public procurement Competition.

2.14.2 Collusion, or any attempt by interested parties and/or Tenderers to influence, in any way, the Competition, will result in the disqualification of that/those interested parties/Tenderer(s). Examples of such improper influence are collusion, price fixing, bid rotation or market division.

2.15: Industry Terms Used in RFT

2.15.1 Where reference is made to a particular item, source, process, trademark, or type in this RFT then all such references are to be given the meaning generally understood in the relevant industry and operational environment.

2.16: Freedom of Information

2.16.1 Tenderers should be aware that, under the Freedom of Information Act 2014 and the European Communities (Access to Information on the Environment) Regulations 2007 to 2014, information provided by them during this Competition may be liable to be disclosed.

2.16.2 Tenderers are asked to consider if any of the information supplied by them in their Tender should not be disclosed because of its confidentiality or commercial sensitivity. If Tenderers consider that certain information is not to be disclosed because of its confidentiality or commercial sensitivity Tenderers must, when providing such information, clearly identify such information and specify the reasons for its confidentiality or commercial sensitivity. If Tenderers do not identify information as confidential or commercially sensitive, it is liable to be released in response to a Freedom of Information request without further notice to or consultation with the Tenderer. The Contracting Authority will, where possible, consult with Tenderers about confidentiality or commercially sensitive information so identified before making a decision on a request received under the Freedom of Information Acts.

2.16.3 The final decision on any Freedom of Information request rests with the Contracting Authority, subject to applicable law.

2.16.4 Tenderers should seek their own legal advice on the applicability of the Freedom of Information Act 2014.

2.16.5 The Contracting Authority is not liable or responsible under any circumstances whatsoever for any loss, damage or suffering of any kind suffered as a result of disclosure of such information before, during or after this Competition and process.

2.17: Tax Clearance

2.17.1 It will be a condition of any Services Framework Agreement pursuant to this Competition that the Contractor shall, for the term of such Services Framework Agreement, comply with all EU and domestic tax laws. Tenderers are referred to www.revenue.ie for further information. Prior to the award of any Services Framework Agreement arising out of this Competition, the Contractor shall be required to supply its Tax Clearance Access Number and Tax Reference Number to facilitate online verification of their tax status by the Contracting Authority. By supplying these numbers the Tenderer acknowledges and agrees that the Contracting Authority has the permission of the Tenderer to verify its tax cleared position online. A Tenderer may be rejected if it does not have tax clearance from the Irish Revenue Commissioners or cannot procure such with such period determined by the Contracting Authority (at its discretion).

2.18: Conflicts of Interest

2.18.1 Any conflict of interest or potential or perceived conflict of interest on the part of a Tenderer, member, subcontractor or individual employee(s) or agent(s) of a Tenderer or member or subcontractor(s) must be fully disclosed to the Contracting Authority as soon as the conflict or potential or perceived conflict is or becomes apparent. In the event of any actual or potential or perceived conflict of interest (including prior involvement or advice to the Contracting Authority in connection with the preparation

of this RFT or for this Competition or participation in more than one Tender), the Contracting Authority will invite Tenderers to propose means by which the conflict of interest will be removed or properly addressed to the satisfaction of the Contracting Authority. The Contracting Authority will, at its absolute discretion, decide on the appropriate course of action, which may in appropriate circumstances include eliminating a Tenderer from this Competition or terminating any Services Framework Agreement entered into by a Tenderer or permitting a Tenderer to continue in the Competition but subject to such conditions (for example, a requirement to cease using a particular subcontractor or member of a Tenderer or a restriction on participating in more than one Tender) and/or the implementation of such measures and protections (for example, Chinese walls and other protections) as the Contracting Authority may require at their discretion.

2.18.2 A Tender must, in particular, disclose if it, or any of its members or sub-contractor(s) or other parties that are to be identified in its Tender, has any economic, legal, commercial or financial relationship with another Tenderer or member or sub-contractor(s) of another Tenderer submitting a separate Tender. In such an instance, the Tenderer must notify the Contracting Authority as to the identity of the other Tenderer and the economic, legal commercial or financial relationship in question as soon as possible and in any event prior to the submission of their Tender so that the Contracting Authority can determine whether it considers this to constitute a conflict of interest or whether it may give rise to a risk of collusion or distortion of competition arising.

2.18.3 The Tenderer is required in such event to provide an accompanying statement stating that it is aware of the proposed multiple participation and that it has been brought to the attention of all concerned whilst, at the same time, maintaining the integrity of this Competition and confidentiality. The Tenderer is also required in such an event to propose suitable protections and procedures to be put in place by the Tenderer to protect against or minimise any potential conflict, collusion or distortion of competition arising.

2.18.4 Tenderers which are a group of firms should inquire whether the other members and/or subcontractor(s) of the Tenderer are involved in any other Tenderer's Tender, for example, as a member and/or proposed subcontractor(s).

2.18.5 The Contracting Authority reserves the right at its absolute discretion to refuse to allow a consortium member or sub-contractor to be part of another competing Tenderer and/or to disqualify a Tenderer in the event that there is a breach of this requirement.

2.19: Withdrawal from Competition

2.19.1 Tenderers are required to notify the Contracting Authority immediately via the e-Tenders website, if at any stage they decide to withdraw from this Competition.

2.20: Site Visit

2.20.1 Not Used.

2.21: Insurance

2.21.1 The successful Tenderer shall be required to hold for the term of the Services Framework Agreement the following insurances:

Type of Insurance	Indemnity Limit

Employer's Liability	€13 million limit for any one claim or series of claims arising out of a single occurrence, per insurance year
Public Liability	€6.5 million limit for any one claim or series of claims arising out of a single occurrence, per insurance year
Cyber Liability	€1 million minimum cover for each and every claim
Professional Indemnity	€2.5 million for any one claim or series of claims arising out of a single occurrence, per insurance year (for each and every claim excluding defence costs)

2.21.2 By signing the Tenderer's statement at Appendix 3, Tenderers confirm, that if awarded a Services Framework Agreement under this Competition, they will, from the effective date of the Services Framework Agreement (as defined in Services Framework Agreement), obtain and hold the types and levels of insurance as specified at paragraph 2.21.1. A formal confirmation from the Tenderer's insurance company or broker to this effect will be requested from the Preferred Tenderer(s) prior to the award of (and shall be a condition of) any Services Framework Agreement.

2.21.3 The Contractor will, during the term of the Services Framework Agreement, be required to:

(a) immediately advise the Contracting Authority of any material change to its insured status;

(b) produce proof of current premiums paid upon request; and

(c) produce valid certificates of insurance upon request.

2.22: Change in Circumstances

2.22.1 If, as a result of a change in events, circumstances or otherwise, any information given by a Tenderer to the Contracting Authority in the Tender or otherwise, was (when submitted) or has become (by reference to facts as they then stand) untrue, different, incomplete or misleading, the Tenderer must so inform the Contracting Authority in writing as soon as it becomes aware of this. This includes, without limitation, information in relation to a Tenderer's financial and economic standing.

2.22.2 If it comes to the Contracting Authority's attention that:

(a) there has been a change in events or circumstances concerning a Tenderer that could affect the Contracting Authority's assessment of that Tenderer's Tender; or

(b) information submitted by a Tenderer was (when submitted) or has become (by reference to facts as they then stand) untrue, different, incomplete or misleading,

the Contracting Authority may (but is not obliged to) revise its assessment of the Tenderer's Tender, as the case may be, on the basis of the information then available to the Contracting Authority and, at its absolute discretion (but subject to applicable law), reject the Tenderer's Tender and eliminate the Tenderer from the Competition or revise any pass / fail assessment and/or adjust the scores awarded to the Tenderer under the relevant criteria.

2.23: Additional Conditions

Applicable Law

2.23.1 The RFT and any matter or disputes related to or in any way connected with or arising out of the RFT or the Competition are governed by and construed in all respects in accordance with the laws of Ireland and subject to the exclusive jurisdiction of the Irish Courts of Ireland.

Open Tenders

2.23.2 All Tenders must remain open and valid for 160 days from the date for submission of Tenders. No Tender may be withdrawn after the deadline for submission of Tenders. Tenderers, by submitting Tenders, irrevocably agree to this.

2.23.3 Whilst Tenders are only required to remain open and valid for 160 days from the date for submission of Tenders, the Contracting Authority may (but is not obliged to) request Tenderers to extend the period for which they remain open for a longer period of time. If a Tenderer refuses such a request, the Tenderer will be deemed to have withdrawn its Tender (but the Contracting Authority may continue to award the Services Framework Agreement to any Tenderer who has agreed to extend the validity of their Tender).

Compliant Tenders and Assumptions

2.23.4 Tenderers must submit a fully compliant Tender which is not qualified in any way (though this does not limit or affect the right to include Approved Assumptions) and must not include or be accompanied by any statement that could be construed as rendering the Tender equivocal or ambiguous or placing it on a different footing from other Tenders.

2.23.5 Without limitation, this includes any attempt by Tenderers to base their Tender on one or more assumptions (other than an Approved Assumption), such that that the Tender will be affected if those assumptions are not correct. For the avoidance of doubt:

(a) any Tender qualified by such assumptions (other than an Approved Assumption) may be rejected; and

(b) without limiting or affecting paragraph 2.23.5(a) of this RFT, the Contracting Authority will not be bound by any assumptions made by a Tenderer and no assumptions will be incorporated in the Services Framework Agreement (even if approved by the Contracting Authority as an Approved Assumption through the query process, unless specified otherwise by the Contracting Authority when approving the assumption).

2.23.6 The Contracting Authority decision on whether a Final Tender complies with this ISFT will be final.

Specification of Standards

2.23.7 Where reference is made to an international, European, British or other national standard, then a Tenderer may propose an equivalent to any of these, provided that its proposal offers equivalent guarantees of safety, suitability and fitness for purpose to those specified.

Canvassing

2.23.8 Tenderers must not canvass directly or indirectly any member, officer or employee of the Contracting Authority, its advisers, or any member of the Evaluation Committee. Tenderers must not offer, give or agree to give to any member of the Contracting Authority (or its officers, advisers or employees or advisers or any member of the Evaluation Committee) any gift, or consideration of any kind as an inducement or reward in relation to the obtaining or execution of any Services Framework Agreement. Any breach of this paragraph will entitle the Contracting Authority to immediately disqualify the Tenderer concerned from the Competition and/or cancel and terminate the Services Framework Agreement or any existing contracts that the Tenderer has with the Contracting Authority. The Contracting Authority may recover any loss of expense resulting from any such termination.

Own Advice

2.23.9 Tenderers are responsible for obtaining their own financial, taxation, legal, technical, investment and other appropriate advice, and undertaking their own due diligence, in relation to this process, the RFT, the Services Framework Agreement, Competition and all information provided or made available to them, at their own cost and expense.

Compliance with Law

2.23.10 Tenderers (and their members, subcontractors and others involved in their bid) must comply with all relevant laws and regulations that are applicable to them in the context of this Competition.

2.23.11 Any Tenderer that fails to comply with such laws and regulations to the satisfaction of the Contracting Authority may be treated as failing to comply with the conditions of this Competition and may, at the discretion of the Contracting Authority and subject to paragraph 2.2.3, be rejected and eliminated from this Competition.

Exclusion of Liability

2.23.12 No representation, warranty or undertaking, express or implied, in respect of any error or misstatement by or on behalf of the Contracting Authority is made or given to any Tenderer and no responsibility or liability is accepted by the Contracting Authority for the accuracy or completeness of the RFT or omissions from it.

2.23.13 Under no circumstances will the Contracting Authority or its advisers, consultants, contractors and/or agents accept or have any liability whatever in respect of any liability, damage or loss (including, without limitation, bid costs, loss of opportunity, loss of profit or damage to reputation) suffered or incurred by a Tenderer, Tenderer member or subcontractor or anyone else arising out of or in respect of or in connection with the Competition, even where caused due to errors or negligence in the Competition and process or the termination of the Competition (in whole or in part). This paragraph operates to the fullest extent permitted by applicable law.

Errors

2.23.14 If a Tenderer discovers any error or omissions or lack of clarity in the RFT, the Tenderer must immediately notify the Contracting Authority in writing of such error, omission or lack of clarity which will be resolved by the Contracting Authority in such manner as it considers appropriate.

Legal Obligations

2.23.15 Legal and contractual obligations are imposed on Tenderers who download or respond to the RFT and the Contracting Authority reserves the right to enforce such obligations. However, the RFT does not give rise to any enforceable contractual obligations against the Contracting Authority and no collateral contract is entered between the Contracting Authority and any Tenderer in such respect.

Waiver

2.23.16 The failure or neglect by the Contracting Authority to enforce any provision of the RFT is not (and will not be deemed to be) a waiver of that provision and does not prejudice the Contracting Authority's right to take subsequent action in respect of such provision.

Amendments

2.23.17 The Contracting Authority reserves, at its absolute discretion, the right, at any time until the conclusion or termination of the process, to amend or modify any documents, information, data, procedures, rules and/or timelines in or related to the RFT or process in any respect by way of clarification, addition, deletion or otherwise. The Contracting Authority will inform Tenderers of any such amendments or modifications, if appropriate.

Reserved rights

2.23.18 The publication of the RFT does not warrant or imply that any Tenderer will be awarded a contract or any tenderer will be awarded or invited to enter into the contract on any particular conditions.

2.23.19 Not Used.

2.23.20 The Contracting Authority reserves the right, for any reason whatsoever at its absolute discretion:

(a) to reject any and all Tenders;

(b) not to proceed with any evaluation;

(c) not to select any Tenderer or Tender;

(d) not to provide a Tenderer with any additional information;

(e) not to implement any arrangement contemplated by the RFT;

(f) to suspend the process;

(g) not to award any contract;

(h) to procure the Services by alternative means;

(i) to use the negotiated procedure without a further call for competition where no Tenders or no suitable Tenders are made; and/or

(j) to terminate the RFT, the process and/or the Competition at any time and without reason.

2.23.21 The Contracting Authority may (but are not obliged to), in order to verify information provided or implied in a Tender, contact and visit a Tenderer and any or all of its members, subcontractors, members, suppliers, funders, insurers and/or referees which might be provided in the Tender and may conduct any investigations and site visits (including to third party suppliers) (either itself or through such third parties as they may, at their absolute discretion, consider appropriate) it considers necessary in connection with responses, including by reference to information independently sourced from the market or otherwise. The Tenderers, on request, must facilitate same. This applies all the way up until Service Framework Agreement execution by the Contracting Authority.

Part 3: Selection and Award Criteria

3.1: Compliant Tenders

3.1.1 Only those Tenderers who have submitted, subject to paragraph 2.2.3, a compliant Tender will be eligible to be evaluated.

3.1.2 The Contracting Authority may (but is not obliged to) decide to assess Tenders against the Award Criteria before verifying the absence of Exclusion Grounds and the fulfilment of the Selection Criteria.

3.1.3 However, notwithstanding anything to the contrary in this part 3.1, the Contracting Authority reserves the right to ask Tenderers at any moment during the Competition (including at Preferred Tenderer stage) to submit any or all of the following for the purposes of verification of the status of the Tenderer (including any member or subcontractor):

(a) a declaration in the form attached at Appendix 4 (**Replicated in Tender Response Document A**);

(b) evidence to the effect that measures taken by the entity concerned are sufficient to demonstrate its reliability despite the existence of a relevant Exclusion Ground; and

(c) in the case of the Tenderer and any subcontractor or other entity on whose capacity or resources the Tenderer or any member or subcontractor of the Tenderer relies, all or any of the supporting documents specified at part 3.2 below.

3.1.4 If a Tenderer does not, upon request by the Contracting Authority, provide evidence which is considered by the Contracting Authority as sufficient to demonstrate:

(1) its fulfilment of any relevant Selection Criterion in accordance with this RFT; and

(2) the absence of Exclusion Grounds (other than those on the basis of which the Contracting Authority has elected, where permitted by Article 57 of the Procurement Regulations, not to exclude the Tenderer) or its reliability despite the existence of a relevant Exclusion Ground,

it shall be excluded from further participation in this Competition.

3.1.5 If a Tenderer does not, upon request by the Contracting Authority, provide evidence which is considered by the Contracting Authority as sufficient to demonstrate:

(1) the fulfilment of any relevant Selection Criterion in accordance with this RFT by any member or subcontractor of the Tenderer or other entity upon whose capacity or resources the Tenderer or member or subcontractor of a Tender is relying; and

(2) the absence of Exclusion Grounds (other than those on the basis of which the Contracting Authority has elected, where permitted by Article 57 of the Procurement Regulations, not to exclude the relevant entity) in respect of any member or subcontractor of the Tenderer or other entity upon whose capacity or resources the Tenderer or member or subcontractor of a Tenderer is relying,

or the reliability of any such entity despite the existence of a relevant Exclusion Ground,

the Tenderer shall be excluded from further participation in this Competition *unless* it replaces the member or subcontractor or other entity upon whose capacity or resources the Tenderer or member or subcontractor is relying with one which meets all relevant requirements of this RFT.

3.1.6 Tenderers are reminded that the Selection Criteria and Exclusion Grounds apply at all times during the Competition (including up to and including the Preferred Tenderer stage).

3.1.7 The Contracting Authority reserves the right, at their sole discretion, to re-assess the eligibility, economic and financial standing and technical and professional capability of any Tenderer (or Tenderer member or subcontractor) at any point(s) throughout this Competition (including at Preferred Tenderer stage).

3.2: Selection Criteria

3.2.1 Not Used.

3.2.2 Tenderers will either pass or fail each of the Selection Criteria as detailed below and in paragraphs 2.21.1 and 2.17. If a Tenderer fails any of the Selection Criteria, the Tenderer will, subject to paragraph 3.1.5, be rejected and excluded from participating in this Competition. The onus is on Tenderers to ensure that their Tenders fully and properly address and respond to the Selection Criteria.

3.2.3 Tenderers, in the first instance, must declare by way of the ESPD and Qualification Response (TRD Document A) that they satisfy the pass / fail Selection Criteria set out below and in paragraphs 2.21.1 and 2.17.

3.2.4 Tenderers must provide the supporting documentation specified below without delay when requested by the Contracting Authority. However, where the Tenderer is unable, for a valid reason, to provide the specified documentation to demonstrate its economic and financial standing, the Tenderer must inform the Contracting Authority of the reason as to why the documentation cannot be supplied and, if the Contracting Authority considers the reason given to be valid, provide such other suitable alternative documentation which the Contracting Authority considers appropriate to prove, to the satisfaction of the Contracting Authority, it satisfies the relevant pass / fail Selection Criterion in respect of its economic and financial standing.

3.2.5 **Economic and Financial Standing Selection Criteria (TRD Document A)**

(a) **Good Financial Standing:**

Pass / Fail Qualifying Threshold: The Tenderer must demonstrate that all accounts held by the Tenderer are in good standing.

Required Evidence: The Self Declaration in Tender Response Document (TRD) Part A must be completed in respect of this criterion.

Tenderers must, when so requested by the Contracting Authority and without delay at any time prior to the award decision being made, provide the following supporting documentation: a letter from the Tenderer's principal bankers or auditors letter or equivalent confirming that all accounts held by the Tenderer are in good standing.

(b) **Financial Capacity - Turnover:**

Pass / Fail Qualifying Threshold: The Tenderer must submit a statement confirming that the company's turnover equalled or exceeded €3 million per annum in any of the last three financial years, or pro-rata if more recently established:

Required Evidence: The Self Declaration in Tender Response Document (TRD) Part A must be completed in respect of this criterion.
Tenderers must, when so requested by the Contracting Authority and without delay at any time prior to the award decision being made, furnish appropriate evidence (e.g., auditor's statement or financial accounts or equivalent) detailing turnover for each of the three previous financial years, confirming that it meets the above required turnover levels).

3.2.6 **Technical and Professional Ability Selection Criteria (TRD Document A)**

(a) **Organisational Resources**

The Tenderer must demonstrate that it has least the following staffing levels who are available to deliver the required Services:

- 10 Service Desk Support Engineers, across L1, L2 & L3 (Incl. at least 1 SOC-Analyst);
- 2 System Architects / Designers;
- 2 Dedicated Managed Services Team Engineers; &
- 1 Project Coordinator / Service Delivery Manager

Required Evidence: The Self Declaration in Tender Response Document (TRD) Part A must be completed in respect of this criterion.
Tenderers must, when so requested by the Contracting Authority and without delay at any time prior to the award decision being made, furnish appropriate evidence of sufficient capacity and resources to properly deliver the required Services as requested above.

(b) **Comparable Contracts:**

The Tenderer must demonstrate that it has successfully delivered three contracts of a similar nature and scale to the Commission for Regulation's requirements under this tender during the previous three (3) years (from the date of this RFT).

Required Evidence: For each such contract, Tenderers must provide evidence of previous experience in this area by completing the tables provided in Tender Response Document (TRD) Part A. These tables may be expanded as necessary.

The entity that performed the Services under the relevant reference contract must be the entity proposed to provide the relevant Services under the Services Framework Agreement.

3.3: Award Criteria

3.3.1 The Services Framework Agreement will be awarded on the basis of the most economically advantageous Tender. The onus is on Tenderers to ensure that their Tenders fully and properly address and respond to the Award Criteria.

3.3.2 A total of 1,000 marks (100%) will be available. The quality/cost ratio is 70:30 as set out below:

Criteria	Max Marks Available	% of Total Marks Available
A: Quality	700	70%
B: Cost	300	30%
Totals	1,000	100%

3.3.3 The Award Criteria, which will be applied in evaluating the quality and cost of the Tenders received, are set out below:

	Award Criteria	Marks Available	Minimum Qualifying Marks*	Tender Response Document
A1.	Service Transition & Mobilisation	**100 marks**	**60 marks (60%)**	TRD Document B Section A1
A2.	Service Management & Governance	**200 marks**	**120 marks (60%)**	TRD Document B Section A2
A3.	Service Levels & Performance Management	**150 marks**	**90 marks (60%)**	TRD Document B Section A3
A4.	Resourcing Model & Key Personnel	**200 marks**	**120 marks (60%)**	TRD Document B Section A4
A5.	Proposals for Sustainability & Social Value	**50 marks**	**30 marks (60%)**	TRD Document B Section A5
A6.	Cost	**300 marks**	**N/A**	TRD Document C
	Total	**1,000 Marks**		

* Tenderers must achieve the minimum marks set out in the table above. Failure to achieve the minimum marks will result in rejection of the Tender and elimination from the Competition (in which case the price of the Tender concerned will not be used in determining the marks under the Cost criterion).

3.3.4 The lowest price Tender will receive the maximum score achievable under the relevant Award Criterion. The scores of all other valid Tenders will be calculated using the following formula:

Cost Score =	(L) Lowest Cost Tender / (N) Tendered Cost under evaluation	x	(T) Maximum Number of Marks Available under the Award Criterion

The "Total Cost of Tender" submitted in response to Appendix 2 is the price of Tenderers for this purpose.

3.3.5 The following scoring methodology will be applied in respect of any sub-criteria for award criteria A1 to A5. The score awarded within a range will depend on the extent to which the relevant description under the "Meaning" column below is satisfied.

Weighting	Meaning
91%- 100%	An excellent response, with very few or no weaknesses, that demonstrates a complete understanding of requirements and provides comprehensive and convincing assurance that the Tenderer will deliver to an excellent standard.
80% - 90%	A very good response that demonstrates real understanding and fully meets the requirements and assurance that the Tenderer will deliver to high standard.
60% - 79%	A satisfactory response which demonstrates a reasonable understanding of requirements and gives reasonable assurance of delivery to an adequate standard but does not provide sufficiently convincing assurance to award a higher mark.
30% - 59%	A response where reservations exist. Lacks full credibility/convincing detail, and there is a significant risk that the response will not be successful.
1% - 29%	A response where serious reservations exist. This may be because, for example, insufficient detail is provided, and the response has fundamental flaws, or is seriously inadequate or seriously lacks credibility with a high risk of non-delivery.
0%	Response completely fails to address the criterion under consideration

3.3.6 If the evaluation results in a tie break between two or more Tenders, then the Tender with the highest overall "qualitative" score under award criteria 1, 2 and 3 shall be deemed the most economically advantageous Tender.

3.3.7 The award of the Services Framework Agreement to the highest ranked Tenderer will be conditional upon, in particular, the Tenderer submitting to the Contracting Authority, to the extent not already provided, within seven (7) days (or such other period specified by the Contracting Authority) of request by the Contracting Authority, the following evidence in respect of the Tenderer (and any members, subcontractors or other entities which are being relied upon by the Tenderer or its members or subcontractors, as applicable, in accordance with part 3.1 above):

(i) a declaration in the form attached at Appendix 4;

(ii) where applicable, evidence to the effect that measures taken by the entity concerned are sufficient to demonstrate its reliability despite the existence of a relevant Exclusion Ground; and

(iii) all or any of the supporting documents and evidence specified at part 3.2.

3.4: Presentation of Proposals

3.4.1 Tenderers may be required to make a presentation and/or attend meetings and/or attend interviews in respect of the proposal contained in their Tender. The Contracting Authority will not be responsible for the cost of such presentations.

3.4.2 The presentation will be used for verification and understanding purposes only. Any scores provisionally allocated against the Award Criteria in advance of the presentation can either remain the same or be adjusted downwards as a result of the presentation. They will not be adjusted upwards as a result of the presentation.

3.4.3 If a clarification or supplementary information in respect of the content of a Tender which is given during the presentation may impact upon a Tenderer's provisional score, the Tenderer will be asked to confirm the clarification and/or supplementary information in writing in the interest of transparency and good administration.

3.5: Standstill Period

3.5.1 If the Procurement Regulations apply to this Competition, no contract will be executed until at least fourteen (14) calendar days after the day on which the Tenderers have been sent a notice informing them of the result of this Competition ("**Standstill Period**") if such notice is sent by electronic means. The Standstill Period shall be sixteen (16) calendar days if such notice is sent by other means. The Preferred Tenderer will be notified of the decision of the Contracting Authority and of the expiry date of the Standstill Period.

3.5.2 Tenderers should note that the Contracting Authority may, when notifying Tenderers of the results of this Competition, include the scores obtained by the Tenderer concerned and the scores obtained by the Preferred Tenderer in respect of each award criterion assessed by the Contracting Authority, including cost / price.

3.6: Return Signed Contracts

3.6.1 The successful Tenderer must sign and return the Services Framework Agreement and the confidentiality agreement, both in duplicate, to the Contracting Authority no later than 21 calendar days from the date of expiry of the Standstill Period unless notified otherwise in writing by the Contracting Authority. A signed Services Framework Agreement returned by the successful Tenderer is not binding on the Contracting Authority until the Contracting Authority has signed the Services Framework Agreement .

3.6.2 Where the signed Services Framework Agreement has not been received by the Contracting Authority within the period as specified at paragraph 3.6.1 then the Contracting Authority may (but is not obliged to) proceed to award the Services Framework Agreement to the next highest ranked Tenderer in accordance with paragraph 3.6.1 above.

3.7: Evaluation Committee

3.7.1 The Evaluation Committee appointed by the Contracting Authority will conduct the evaluations. Each member of the Evaluation Committee will undertake such functions and tasks as each may agree to be allocated to a member or members.

3.7.2 The Contracting Authority reserves the right, at its discretion, at any time to remove, substitute, appoint, decrease or increase the members of the Evaluation Committee without notice to Tenderers.

3.7.3 The Evaluation Committee may nominate one or more persons, including third parties, to conduct certain meetings or discussions or to evaluate or consider certain matters on its behalf during the process.

3.7.5 The Evaluation Committee is entitled to carry out investigations and undertake such other matters in respect of any matter arising out of or incidental to the Competition and/or its evaluations where, in the opinion of the Evaluation Committee, this is necessary, appropriate or helpful. The Evaluation Committee may, in particular, seek independent financial and market advice to validate information declared, or to assist in the evaluation.

3.7.6 The Contracting Authority reserves the right to make independent trade, credit and security inquiries on Tenderers before appointing any Contractor or awarding any contract pursuant to this Tender process.

Appendix 1: Requirements and Specifications

Tenderers must address each of the issues and requirements in this part of the RFT and submit a detailed description in each case which demonstrates how these issues and requirements will be dealt with / met and their approach to the proposed delivery of the Services. A mere affirmative statement by the Tenderer that it can/will do so or a reiteration of the tender requirements is NOT sufficient in this regard.

The CRU intends to appoint a single Managed Service Provider (MSP) through this Services Framework Agreement to deliver comprehensive ICT Managed Services. This will encompass the ICT Service Desk, Managed Security Operations Centre (SOC) as a Service, the provision of optional dedicated support resources, and ad-hoc professional service resources to assist with a range of ICT projects and some operational activities. The appointed Service Provider will be responsible for delivering all necessary technical support and expertise to manage the CRU's ICT needs, covering infrastructure, cloud services, both physical and virtual systems, as well as applications and services across Levels 1, 2, and 3. The framework agreement will initially run for two years, with the possibility of two further 12-month extensions, up to a total maximum duration of four years.

The ICT Managed Services and SOC Services provided under this Services Framework Agreement will be needed continuously for the entire duration of the contract. Optional dedicated resources and ad-hoc project work will be engaged as required, with such assignments awarded through agreed Statements of Work (SoWs) at the sole discretion of the CRU.

The Commission aims to secure the best possible value for money, while ensuring that the selected provider delivers a high standard of service tailored to the organisation's needs.

The CRU's requirements can be broadly split into the following requirements:

A. **ICT & SOC Managed Services** – these are described in more detail in section 2.0 below.
B. **Optional Dedicated Support Resource(s)** – this is described in more detail in section 3.0 below.
C. **Ad hoc Project Work / Professional Service Days** – this is described in more detail in section 4.0 below; &
D. **Software Licensing Renewals** – this is described in more detail in section 5.0 below.

Upon conclusion of the Services Framework Agreement with the successful tenderer, an SOW will be concluded immediately for ICT & SOC Managed Services. CRU will generally award separate SoWs for optional dedicated support resource requirements and for individual project work as needs arise. However, it may also include such projects within the scope of the ICT Managed Service SOW, by application of the Change Control procedure in that contract, where it considers this more appropriate, in a given case.

The estimated value (exclusive of VAT) of the Services Framework Agreement (including the value of all SOWs) is in or around EUR 3,500,000 (excl. VAT) over the maximum four-year duration. This estimate is provided for information purposes only and is not binding. There is no guarantee of any particular volume, value, scope or frequency of work or SOWs.

It is possible that the actual value may be significantly higher or lower than estimated and this estimate does not in any way limit the scope, volume or quantity of services that may be drawn down under the Services Framework Agreement.

Whilst the technical information set out in this RFT has been prepared in good faith, it does not purport to be a comprehensive statement of all matters relevant to the requirements of

CRU. The Commission will not accept any liability or responsibility for its adequacy, accuracy or completeness, nor does it make any representation or warranty, expressed or implied, with respect to the information contained within the RFT. The successful tenderer is responsible for assuring its own technical due diligence is done to its satisfaction as part of any initial phase of work.

The CRU will have the right under the Services Framework Agreement and relevant SOWs to increase or decrease the scope of the ICT Managed Services or Managed SOC Services in line with its fluctuating requirements, and subject to the requirements of applicable law.

1. Introduction

The Commission for Regulation of Utilities ("CRU") is Ireland's independent energy and water regulator. The CRU was originally established as the Commission for Energy Regulation ("CER") in 1999. The CRU's mission is to protect the public interest in Water, Energy and Energy Safety. The work of the CRU impacts every Irish home and business. The sectors we regulate underpin Irish economic competitiveness, investment and growth, while also contribute to our international obligations to address climate change.

CRU has recently launched a new Strategic Plan 2025-2027. This strategic plan underpins our role in regulating Ireland's evolving energy and water sectors, and ensures that essential services are delivered efficiently, safely, and in line with national policy objectives.

This strategic plan will allow CRU to:

- Protect and empower customers, with an increased focus on the energy sector as it grows in scale and complexity;
- Maintain resilience of electricity, gas and water in partnership with relevant Departments and key stakeholders;
- Drive competitiveness to support choice and affordability;
- Enable customers to become more active in the energy market
- Provide dispute resolution services for customers to ensure they receive a high level of service;
- Enhance our oversight and monitoring of investment in the regulated network sectors;
- Build the organisation's capacity to focus on long-term sectoral developments so that it can provide economic analysis and advice for national and EU-level policy stakeholders;
- Drive the decarbonisation of all regulated sectors to benefit society and the economy; &
- Ensure public safety across the expanded sectors which CRU regulates, as new electrification technologies reach consumers and as biomethane and hydrogen are introduced into the gas network.

The CRU is guided by eight strategic priorities that sit alongside the core activities we undertake to deliver on the public interest. These are:

Further information on the CRU's role and relevant legislation can be found on the CRU's website at www.cru.ie. The CRU privacy notice is also available at https://www.cru.ie

2. Specification of Requirements

CRU seeks an experienced ICT Managed Services Provider (MSP) who can support the organisation with all end-to-end ICT Managed Services and Technical Support, Security Managed Services Support (SOC-As-A-Service), and to manage the CRU's ICT infrastructure, including the production site, DR site and Azure hosted systems, applications (both on-premise and cloud), networks, services, etc. The Service Provider will also be required to provide optional dedicated support resources and provide ad-hoc professional services to support various projects, as and when required.

2.1 Scope of Requirements

The ICT Managed Service involves the provision of ICT Support to ensure that CRU ICT infrastructure, systems, applications, networks and services are adequately supported, maintained, secured and developed in line with organisational needs.

The ICT infrastructure, systems and services include, but are not limited to, the following:

(i) ICT Infrastructure:

Item	Quantity
Dell PowerStore SAN	2 (Prod & DR)
Dell ESXi VMWare Hosts	4 (Prod & DR)
Servers (Virtual)	45 (Prod); & 63 (DR) with 11 live 52 offline in DR Azure 8 VMs
Servers (Physical)	6 (Including hosts & Backup Servers)
Laptops (Mixed Manufacturers Incl. HP, Dell, Lenovo)	270+ (Likely to increase to 380+ over the contracted term)
Printers MFPs (Under 3rd Party Contract)	5
Video Conferencing Rooms (Primarily Logitech Equipment)	17
Cisco Meraki Switches	12
Cisco Meraki Access Points	10
Firewalls (FortiNet) Production & DR	5 (4 Physical Fortinet FortiGate 100F's & 1 Azure VM Appliance)

*All hardware figures set out above are estimates and are subject to change. The ICT Managed Service must cover all existing and future ICT Infrastructure requirements.

(ii) ICT Systems and Services: M365, various client-server applications (under 3rd Party Support Agreements – but will require 1st level support), back-ups solution (Veeam backup & replication), desktop software, file printing & scanning, email, web browsing, remote access (including site to site & client VPNs), SFTP (secure FTP), Wi-Fi, meeting room software, audio

visual software, disaster recovery & back-up services, asset management software, AI SIEM Solution, etc.

The Commission currently employs approximately 197 staff members who will require ICT Support and Managed SOC Services. Over the course of the contract, the total number of staff is projected to increase. The anticipated annual headcount growth is as follows: by the end of Year 1 – an additional 71 staff, by the end of Year 2 – a further 70, and by the end of Year 3 – a further increase of 49, resulting in a total headcount of 387 by the end of the initial three-year period. However, staff numbers may fluctuate during the four-year term, and any such changes will remain within the scope of the fixed charge for ICT Managed Services and SOC Managed Services.

Staff will require support from multiple locations, including but not limited to, the CRU main office, located at Exchange Hall, Belgard Square North, Tallaght, Dublin 24, D24 PXW0, and from various home locations. CRU has a hybrid working arrangement where staff can work approx. 60% of time from home. All of the above are in scope of the fixed fee for the managed services requirement (including Managed SOC). Any changes to staff numbers will be notified to the service provider, 30 days in advance. Technical support will also be required at the CRU DR Site located at the Revenue Datacentre, Johns Rd. Dublin 8, to ensure the DR solution and its associated infrastructure is fully maintained.

Staff primarily use laptop computers however some tablet devices are also used. Approx. 40% of staff also use CRU smartphones. The ICT environment is virtualised using VMWare and virtual servers are spread across multiple sites, including the on-premise environment (approx. 45+ VMs), Microsoft Azure (approx. 8 VMs) and the DR environment, (approx. 11 VMs [online], and with full replica of all VMs from Production site [offline]) located at the Revenue Datacentre, John's Rd. Dublin 8. All CRU ICT systems will be required to be available to staff from 07:30 – 18:30 Monday to Friday. The Service Provider will be required to perform certain services outside of the hours stated above (e.g. server reboots), and these services will form part of the general ICT Managed Services. An out of hours service must be available with the number provided to the CRU ICT Manager and/or their representative.

An overview of the CRU's current ICT environment is included in Annexes A - H for information.

It is envisaged that all in-scope Commission hardware and software will continue to be owned by the Commission and will be based across two physical sites, 1) main site in Belgard Square North, Tallaght, D24 PXW0, and 2) the Disaster Recovery Site, Revenue Datacentre, Johns Rd. Dublin 8. CRU also uses hosted services from Microsoft Azure for a small number of virtual servers (VMs). During the lifetime of this Services Framework Agreement, some CRU applications, services, and / or VMs will move/ migrate to cloud-based services/ solutions and the MSP will be responsible for the delivery and / or support of these initiatives. The CRU Digital Strategy 2025 – 2030 includes continued adoption of cloud migration over the next 4 Years. Cloud based migrations will be subject to professional services drawdown days under ad-hoc projects via SoWs. The MSP must have personnel who are trained and competent to deliver Azure based migration support and implementation services.

The ICT managed support services will include the provision of an ITIL (Information Technology Infrastructure Library) based central Service Desk which will manage (log, co-ordinate, resolve) the lifecycle of all ICT support tickets and incidents, including the recording of solutions/ fixes in the CRU IT Glue Software Solution / Knowledge Base. The MSP must log all service requests and will be responsible for communicating with all end users to resolve technical issues and/ or to advise of any workarounds available. The MSP will be responsible for resolving all ICT service requests, and must escalate where

necessary, either internally within the MSP or externally to 3rd Parties, to ensure that all service requests are promptly resolved.

In circumstances where service requests and/ or incidents cannot be resolved remotely, the MSP must provide onsite technical support, within the SLA timeframe, with detailed knowledge and experience of CRU ICT infrastructure, systems and services. This onsite resource must be available, as required, to visit either the CRU Production Site or CRU DR Site. On-site visits are within scope of the general ICT Managed Services. Where 3rd Party Vendors are required, the MSP must also co-ordinate and manage these resources for onsite visits, i.e. where hardware warranty call-outs / swap-outs are scheduled, etc.

The MSP must monitor the performance and availability of CRU ICT assets through an asset management service/ agent and must track the current status and characteristics of each ICT asset, including patching levels, performance, compute resources, etc. The agent deployed must have remote access capabilities. The monitoring information must also be readily available to the CRU's ICT Manager and their associated Team members. Patching status of ICT assets must be provided to the CRU ICT Manager on a monthly basis.

This Service Desk must ensure that they adhere to strict configuration and change management procedures, as set out by the CRU ICT Manager. All changes must be documented and recorded for future reference. This is essential to minimise any service disruptions to CRU business users and services, and to be able to roll back if necessary. Changes must only be made, once approved by the CRU ICT Manager, in order to maximise service efficiencies/ benefits and/ or to avoid any service disruptions.

The successful tenderer will contribute positively towards the delivery of the CRU's Digital Strategy. This will involve, identifying opportunities and/ or new technologies that could add value and measurable benefits to CRU. The MSP will provide advice and support to assist in the alignment of ICT applications, services, infrastructure and solutions, and to ensure that all technologies deployed/ adopted meet the organisations business needs.

The MSP will manage the demand and performance of the CRU's ICT infrastructure, systems and services. This will include monitoring and reviewing service level agreements (SLA's) and performances of other ICT Service Providers to ensure that optimum targets are set and met. The MSP must plan and manage the activities for rationalisation, migration and integration of CRU's ICT assets.

See Annex B for a current list of CRU ICT assets.

The CRU shall make available its ICT Manager and their team to work with the selected tenderer during the establishment of the ICT Managed Services. The CRU ICT Manager shall be responsible for overseeing the ongoing management of the Service Provider (and ICT Managed Services) for CRU. The tenderer shall be responsible for the management of the ICT Managed Services and associated services.

The following sub-sections outline further details relating to the service requirements, including service levels, service management and the service desk. Delivery and performance of the following services will be reviewed every quarter at a Service Review Meeting. The MSP must appoint a dedicated Service Delivery Manager who will be responsible for attending quarterly meetings. The CRU ICT Manager may request the attendance of other MSP Personnel, as and when required.

The service provider will, in particular (and without prejudice to the more general description in other parts of this section), be required to provide the following specific services as a part of the ICT Managed Service:

i. Provision of a fully managed service desk based on best practice ITIL managed services framework. This will include a multi-channel helpdesk with a dedicated email address and contact number as well as a portal for end users to log tickets. The helpdesk must allow for the recording, categorisation, prioritisation, escalation and reporting of all incidents and service requests**.**

ii. Proactive 24/7 monitoring of key servers and network devices to enable rapid identification and resolution of potential issues. The Tenderer will be required to provide regular reports giving an executive summary of such monitoring, highlighting any key issues and resolution actions.

iii. The Service Provider must be able to fully support the CRU core ICT environment based upon, VMWare, Microsoft Operating Systems including MS 2016 Server onwards and end user devices based on MS Windows 11 and any future operating system, all versions of M365 including Business Premium, F3, E3 and E5, Co-pilot, PowerBI, Visio & Project.

iv. The Set-up, configuration and maintenance, including relevant software installation, of new or existing Servers (including deploying new VMs), PCs, smart phone devices, laptops, tablets or network hardware (including Wi-Fi systems), as required. As well as the decommissioning of hardware that is no longer required, and the updating of the CRU ICT Asset Register, as required. CRU currently has a policy of refreshing hardware on a regular basis. It is expected that approx. 400 new PCs (laptops, tablets and/ or desktops) will be replaced during the next 4 years and configuration, setup and deployment of these new devices is within scope of the standard MSP services and the fixed annual price. CRU will retain ownership of all hardware, unless otherwise agreed in a given case. CRU will remain responsible for the proper disposal of its ICT assets in accordance with its internal policies, however the Managed Services Provider will be required to assist the CRU ICT Manager and ICT Team, by providing support, and any required information, during the disposal process, and by readying hardware for disposal (i.e. wiping clean any data etc.).

v. Set-up and maintenance of all user profiles, including access rights to in-scope ICT systems and services. This will include setting user permissions for on-premise and cloud-based solutions, including but not limited to, Active Directory/ Azure Entra ID, MS Dynamics, MS Business Central, and other CRU Business Applications, etc.

vi. Set-up of users on security systems for accessing the CRU network, e.g. DUO MFA System, Fortinet VPN, Microsoft Authenticator, Cisco Umbrella, Sophos, etc.

vii. Monitoring email and internet usage solutions, i.e. Mimecast, Lookout for Work, Sophos Intercept X, Cisco Umbrella, etc. The Service Provider will be required to provide detailed reports, to the CRU's ICT Manager, as and when required, on the effectiveness of these services/ solutions. These reports may be subject to review at the quarterly service review meeting.

viii. Supporting the CRU ICT Dept. in the implementation of various CRU ICT User Policies. The Service Provider will be required to provide quarterly reports of the effectiveness

of this service to the CRU ICT Manager, as and when required. All existing and new ICT Policies will be made available to the successful tenderer.

ix. The MSP must manage the CRU Software Licence Portfolio and associated support arrangements. This will involve working with the CRU ICT Manager / ICT Dept. to ensure that all required licences are in place for the software packages, solutions and services in use. Where appropriate, the service provider will also ensure that sufficient third-party support arrangements are in place and will manage those arrangements on behalf of the Commission. This may involve the transfer of existing software license agreements to the MSP. The MSP will help maintain the Commission's compliance with all software licensing during the contracted period, including support with the renewal process of such arrangements, as required. The service provider will also be responsible for managing any Microsoft Audits, or similar audits, should any arise during the contract period.

x. The service provider will be responsible for managing the software/SaaS renewals portfolio for all solutions used by CRU. CRU currently has a number of SaaS solutions and other ad-hoc solutions that require annual renewal, and the service provider must ensure this inventory is maintained and kept up to date. The service provider will be required to provide the CRU ICT Manager with a minimum of 60 days' notice of any renewal. A full inventory of current SaaS solutions will be made available to the successful tenderer. CRU will utilise OGP Frameworks where possible for software renewals, however the MSP may be asked to submit a quotation, or multiple quotations, to the CRU ICT Manager / ICT Dept., if required, for products that cannot be renewed via the OGP Frameworks. Renewals will be at the discretion of the CRU ICT Manager and must only be renewed once a Purchase Order (PO) has been issued and confirmation of the order has been provided by CRU. The MSP will be required to demonstrate value for money and to provide any and all discounts where available. They must also provide written assurance on competitive pricing. The cost of the software renewals must not exceed any list price or recommend retail price.

xi. Patch & firmware management – the service provider must deploy all stable software patches and firmware updates as they become available for all software/ hardware systems, solutions and services employed by the Commission. The MSP will also be responsible for upgrading Operating Systems of in-scope user devices, as requested, i.e. from W11 to the next Operating System and W2016 Server to next Server Operating System. The service provider will be required to provide monthly / quarterly reports outlining the software versions and patch levels for all key services and systems on the Production Site, DR Site and Azure Site. Patch management includes, but is not limited to, all ICT assets, both physical and virtual, and specifically all Microsoft updates / patches, VMware updates, and manufacturer updates for hardware in use within the CRU. All patch and firmware updates are within the scope on the general ICT Managed Services contract and the associated annual fixed price.

xii. The MSP will be responsible for all Firewall and VPN support & maintenance. This includes the existing physical Fortinet 100F firewalls (4) and any future replacement devices. This involves supporting the 2 Production firewalls (100F's), the 2 DR firewalls (100F's) and the Azure virtual firewall. The MSP will be responsible for resolving all

faults and/or issues and making required changes as needed. The MSP must manage all firewall service tickets and record all changes in the CMDB.

xiii. Support and deliver core business software upgrades. The service provider will be required to work with all third-party suppliers, in line with relevant support arrangements, as appropriate, to apply and test key software upgrades. The responsibility for ensuring the successful upgrade of the various software packages employed by the Commission will lie with the MSP service provider and the third-party suppliers, working in conjunction with each other to achieve the successful upgrade of the various solutions. This support will include, but is not limited to, deploying new Server VMs for 3rd Parties, provisioning remote access for them and assisting in the configuration of the environment.

xiv. Manage hardware warranties and support arrangements – the service provider will be required to work with CRU to ensure that the required hardware warranties and support arrangements are in place, and kept up to date, including supporting the renewal of such arrangements if required. The MSP will also be required to manage the replacement of faulty hardware, under warranty agreements, and to co-ordinate the deployment and commissioning of same.

xv. Management of all daily back-ups and replications. The service provider will be responsible for monitoring and maintaining a comprehensive backup and replication of all data and systems for CRU. This will involve ensuring the current, and future backup / replication solutions are monitored daily on both the production and DR sites. The current solutions that are in place are Veeam Backup and Replication, and Wasabi Cloud Storage. The service provider will be required to provide detailed reports for review at the quarterly service review meetings. The backup and replication solution must be closely monitored, and all issues must be resolved as quickly as possible.

xvi. As part of the day-to-day management, the service provider may be asked by the CRU ICT Manager, or another appointed individual, to provide a restore of the full system or individual VMs or files to the end of previous business day. This will form part of the general ICT Managed Services and is essential for Business Continuity / Disaster Recovery.

xvii. Proactive monitoring of key servers and network devices to enable rapid identification of potential issues and steps taken / required to resolve them. The service provider will be required to provide quarterly reports providing a detailed Executive Summary of such monitoring, highlighting any key issues and resolution of actions.

xviii. Monthly reporting on agreed Key Performance Indicators (KPIs) to the CRU ICT Manager. The purpose of these reports will be to assist the CRU ICT Manager to ascertain the quality of service being provided, to ensure that the agreed Service Level Agreement (SLA) targets are being met, and to identify any trends that may need to be dealt with. Incident reports will need to be provided at the request of the CRU ICT Manager for any Priority 1 tickets.

xix. The Service Provider will be responsible for ensuring a smooth transition from the current support arrangements (if necessary) to any new support arrangements at the end of the contracted period. Each tenderer should include within their tender response how they propose to manage that transition and the expected time required to migrate to the new structure.

xx. Service providers must be in a position to fully support, develop and integrate with the Commission's existing business systems / applications.

xxi. The Service Provider will be required to work with the CRU ICT Dept. in the continuous improvement and ongoing development of the existing Business Continuity Plan (BCP) and Disaster Recovery (DR) Plan. This will involve quarterly testing of the BCP/ DR solution to ensure that the solution is functioning correctly and remains fit-for-purpose. Reports of all testing will be required and will be reviewed at the quarterly service review meeting. Any issues identified must be resolved immediately and is within scope of the ICT Managed Services Contract.

xxii. CRU conducts annual cybersecurity penetration testing of all in-scope systems, networks and applications, and the Service Provider will be responsible for implementing recommendations, as required, for remediation of any technical misconfigurations or other technical issues identified.

xxiii. The service provider will be required to provide out of hours cover in the event of emergencies and should provide the CRU ICT Manager and / or other recommended authorised individuals with an out of hours number and ensure service engineers are available to respond to such events. This service is part of the general ICT Managed Services and must be included within the annual reoccurring charges.

xxiv. The Service Provider will be required to familiarise themselves with all CRU business applications and provide 1st level troubleshooting support prior to invoking any external third-party support. The MSP must ensure that all environmental issues, for example; networking issues, security issues and any other minor issues are eliminated before escalation to the 3rd Party Support Providers. The CRU ICT Dept. will provide general information to the successful MSP on all business applications used within CRU. This information will be provided via the CRU knowledgebase.

xxv. The CRU telephony system is a mix of a legacy NEC IP phone system and Microsoft Teams. The physical NEC solution and its associated PBX is expected to be removed from the production during the initial contract term, and the MSP will be required to provide support services for the NEC system until it is decommissioned. The MSP must provide ongoing support & maintenance for the MS Teams solution throughout the full contract term.

xxvi. If CRU instructs the Service Provider to obtain a domain name for CRU, the Service Provider shall act as an agent for CRU when doing so, including in dealing with the relevant domain name registration authority.

xxvii. The CRU may instruct the Service Provider to procure certain goods or services on behalf of CRU from time to time, including but not limited to: (i) new software licences; (ii) software licence renewals (both of licences originally procured by the Service Provider and licences procured by other service providers); (iii) hardware; (iv) any other goods or services, (together, "Third Party Services"). Where CRU instructs Service Provider to procure Third Party Services on its behalf, Service Provider shall procure such Third-Party Services in accordance with the conditions set out in Appendix 5 – Services Framework Agreement.

The service provider will, in particular (and without prejudice to the more general description in other parts of this section), be required to provide the following specific services to all staff as a part of the ICT Security Managed Service (SOC-As-A-Service):

- The Service Provider must provide CRU with a 24/7 365 day per year Managed Security Operations Centre (SOC) Service. SOC monitoring tools and/ or agents, as required, must be deployed to all devices and assets within the CRU ICT environment. The MSP must have at least 1 SOC-Analyst available to CRU at all times, to respond to any critical incidents in real-time.

- The Service Provider must ensure that they have a holistic view of all CRU ICT infrastructure and assets and must ensure that all security threats and vulnerabilities are monitored.

- The SOC Service must perform continuous vulnerability checks across the CRU ICT environment and technology. This service must cover, but is not limited to, endpoints, network, cloud resources, web and proxy, VMs, system and application data, network shares, end user behaviour analytics, etc. The Service Provider must use the existing solution, ConnectSecure, and any future solutions to remediate vulnerabilities.

- The SOC Service must be able to identify risks and qualify threats, and provide an automated response, if necessary, to ensure CRU systems and data is protected from cybersecurity attacks.

- The SOC Service must include threat investigation and triage. This will involve, but is not limited to, isolation of identified threat(s), incident analysis, real-time threat hunting, impact analysis, incident response and escalation, as required.

- The service provider must be familiar with AI based SIEM solutions and use the existing solution, Darktrace, for monitoring threats.

- The Service Provider will be responsible for liaising with any 3rd Party vendors, if required, to restore CRU ICT Assets and Infrastructure to optimum performance.

- The service provider will be required to maintain a proactive approach throughout the lifetime of the MSP Services Framework Agreement. This will involve keeping up to date with all new and emerging cyber security threats and ensure that all recommended preventative action is taken to protect the CRU ICT systems and networks.

- The Service Provider must provide the CRU ICT Manager with regular reports on the SOC Service, the frequency of these reports will be agreed at the outset of the Services Framework Agreement. The SOC Service will be reviewed on a quarterly basis, at the regular Service Review Meeting with the CRU ICT Manager and their Team. Any deficiencies identified with the service must be rectified immediately. Failure to rectify any deficiencies in the SOC Service may result in the termination of the service(s).

- The Service Provider SOC Resources will be required to meet with CRU resources once a month to discuss open items, ongoing threats, vulnerability reports and remediation steps and actions that are in progress, planned and/or scheduled.

- The Service Provider must ensure that the SOC Service is continuously reviewed and improved and must implement any identified efficiency gains that enhance the overall delivery of the service. All changes to the SOC Service must be fully agreed with the CRU ICT Manager, prior to implementation.

- The Service Provider must also act on any instructions provided to them by the CRU ICT Manager in respect of any cybersecurity alerts raised via 3rd Parties or national agencies, i.e. recommendations issued by the National Cyber Security Centre (NCSC) or via An Garda Siochána.

- The Service Provider must also act on any instructions provided to them by the CRU ICT Manager in respect of recommendations required from Cybersecurity Audit Reports, i.e. where deficiencies or configuration / mis-configuration issues have been identified and pose a risk to CRU ICT Assets or users.

- The Service Provider must deliver the services required as per the SLA set out in Section 2.5 below.

- The service provider will be responsible for ensuring a smooth transition from their SOC Service to any new future support arrangements, if required, at the end of the Services Framework Agreement. This will involve liaising and supporting the transition process with any future MSP.

General Requirements – Third Party Solutions

The Managed Service Provider (MSP) must be able to provide 1st Level Support on all CRU Business Applications, i.e. initial troubleshooting to identify any user or environmental issues like networking issues, user issues, OS issues etc. 2nd level / 3rd level support for some specific business applications can be provided by third party suppliers under existing agreements / contracts / purchase orders. The MSP must however manage the support ticket / incident to completion and ensure that the 3rd Party providing all 2nd level / 3rd level support for business applications rectifies the issue and that the fix is recorded within the CRU IT Glue Solution / knowledgebase/ CMDB.

The MSP must familarise themselves with the CRU applications portfolio and must work with the relevant third parties to ensure that they have a good general understanding of the products and business applications in use.

Below is a list of the current suite of business applications deployed in CRU. This list is not exhaustive and is subject to change. The MSP will be required to support this list of business applications, and any future additions. Future additions must be considered to be within scope

and there will be no entitlement to a variation to the ICT Managed Service fixed fee in the case of such an increase. Changes will be notified in writing to the successful bidder through a change control process, 30 days prior to any such change.

- OpenText Content Manager v24.5 and above
- Microsoft Dynamics & Business Central
- Plexos Energy Modelling Software
- Pisys ATMS (Action Tracking Management System)
- Keyhouse Legal Case Management
- Decision Time
- Strandum HR

2.2 Other ICT Services

The 2nd level and above, ICT support and maintenance for the following front and back-office systems is provided under separate framework agreements / contracts / purchase orders, some of which have been developed to provide economies of scale for public sector bodies. The MSP will be required / responsible for liaising and coordinating on service tickets / issues with these service providers and must engage with them directly, if required:

a) Managed Print Services (MPS) - the CRU's printing requirements are provided under an existing Managed Print Services (MPS) framework agreement with a third party provider. CRU operate 5 Multi-Function Devices (MFDs) within the main office. The MSP will however be required to handle any printer networking and or driver related requests / issues / problems and must liaise with the MPS provider to ensure resolution of any related service tickets. The MSP will be responsible for closing out all printer support tickets.

b) Desktop, laptops & associated computer consumables – the physical devices are provided by third party suppliers under existing OGP framework agreements. However, the successful tenderer will be required to track key details of such assets, advise the CRU ICT Manager regarding replacement / upgrade requirements, and liaise with the third-party provider(s) regarding any hardware related issues. The MSP will also be responsible for arranging and scheduling any hardware call-outs or replacements under existing warranty arrangements.

c) Website hosting – all of the CRU Websites (i.e. CRU.ie, Safeelectric.ie, RGI.ie & semcommittee.com) are hosted offsite and supported by third party service providers. This will continue to be the case for the foreseeable future. The MSP will be required, as part of the general ICT Managed Services, to work with the CRU ICT Manager on any domain related issues, i.e. DNS record changes and/ or additions, DMARC changes, DKIM, SPF changes, etc.

d) Internet connectivity – this is provided by third party providers. (Virgin Media, Eir & Government Networks) The MSP will be required to work with these 3rd Party Providers to resolve any connectivity issues and will be responsible for closing out all service-related support tickets and / or incident tickets.

e) DR Hosting – this is provided by the Revenue Commissioners. The CRU DR equipment is located in the Revenue Data Centre in Johns Rd, Dublin 8. Hosting services are not currently required as part of this Services Framework Agreement, however, the management and maintenance of the DR site, including the patching of VMs and VMware hosts, is within scope of the ICT Managed Services & SOC - Services

Framework Agreement. The MSP will be responsible for all patching of the DR environment and must provide a comprehensive report to the CRU ICT Manager, on a regular basis to ensure that the environment is kept fully up-to-date and secure. Regular DR testing is within scope of the ICT Managed Services and must be provided on a quarterly basis.

The successful tenderer will be required to cultivate positive working relationships with other ICT Suppliers / Providers of CRU. This will be essential to ensure that the overall ICT requirements of the CRU are satisfied.

The service provider will need to demonstrate the capability to understand the nature of the services outlined above, and work with CRU on any future developments and / or changes to the CRU's ICT infrastructure, systems and services.

2.3 Variance to Scope

Some CRU ICT systems / infrastructure / applications etc. might move in or out of scope of the ICT Managed Services due to the dynamic nature of business requirements and emergent technologies. In this context the CRU reserves the right to add or remove systems / infrastructure / applications etc. from the ICT Managed Services. This would be done in accordance with the Change Control procedure set out in the Services Framework Agreement.

2.4 Service Management

The ICT Managed Services must be delivered in-line with industry recognised best practises (such as ISO 20000 IT Service Management Standard or equivalent) and aligned with the ITIL (Information Technology Infrastructure Library) services framework, whilst also being supported through a Service Desk as a Single Point of Contact for all in-scope users. The Service Desk requirement and service levels for the resolution of reported incidents or support requests are covered in further detail below under *Service Desk and Service Levels*.

The Service Provider must resolve as many reported incidents as possible at first contact, including through the use of a Knowledge Base of known problems and utilisation of remote support technologies to help diagnose and resolve such incidents to limit the need for on-site support where appropriate. However, should it not be possible to resolve issues remotely, the MSP must have resources locally, i.e. in the greater Dublin area, who can be mobilised at short notice and sent onsite to resolve issues at the CRU offices.

The ICT Managed Services must incorporate proactive monitoring and preventative maintenance of all in-scope systems and services to identify potential performance, capacity and security issues, with the aim of resolving them before they impact on services to users.

The Service Provider must proactively make recommendations to CRU Management where changes are identified that could improve the performance or security of in-scope systems and services – including the regular assessment of incidents to identify any underlying problems and, subsequently on approval from CRU and where appropriate, the Service Provider should be able to provide support to implement any agreed changes – these may qualify to be treated as 'Project Work', subject to the evaluation on a case by case basis by the CRU ICT Manager.

The service provider must meet with the CRU ICT Manager on a quarterly basis to review quality of service and performance against service levels. Appropriate reports, that enable proactive ICT management by highlighting recurring issues & trends, must be provided a week in advance of these meetings. Tenderers should provide sample reporting packs as appendices to their responses.

The detail of the reporting format and arrangements will be agreed with the Service Provider at the initial meetings based on actual data. It should be noted that the reports under the ICT Managed Services must, unless otherwise required by the CRU, report against all services provided under all call-off contracts awarded under the framework agreement. This is so that there is a single reporting system.

The following are some sample reports that the CRU ICT Manager may wish to access:

- Number issues logged;
- Number of issues exceeding agreed SLA targets;
- Number of issues that met agreed SLA targets;
- Breakdown of issues assigned to third parties;
- Number of issues that exceeded third party SLA;
- Number of issues that met third party SLA;
- The number of Issues resolved by the Service Desk at first level;
- The percentage of overall Issues fulfilled by the Service Desk;
- Number of issues logged per hour each day;
- Number of issues that were escalated;
- Number of issues escalated to third parties outside the Service Desk;
- Number of customer complaints received broken down by category;
- The number of issues logged per priority;
- The number of issues logged per category;
- The number of issues logged per department/business area;
- The top 5 users reporting issues; and
- The trending in respect of the above data over time

Tenderers should identify within their tenders whether or not it will be possible to provide these reports.

The Service Provider must also ensure that their Service Desk Manager is available to meet with dedicated CRU ICT resources, on a weekly basis, to review any open and ongoing support tickets. This meeting with be agreed between the relevant parties and reports must be provided at least 1 day in advance, to allow the CRU ICT resources to consult with ICT Management.

2.5 Service Desk and Service Levels

Single Point of Contact

The Service Provider must provide a ‘Single Point of Contact’ through a Service Desk for all CRU user support tickets / incidents on all in-scope systems, applications and services. The Service Desk will be responsible for finding and delivering fixes / solutions to issues raised and must manage all tickets escalated to 3rd Parties. The Service Desk engineers must follow-up on all issues until they are fully resolved and issues must not be passed

back to the CRU ICT Dept. for resolution. The CRU ICT Dept. is responsible for the delivery of the CRU Digital Strategy, Contract & Budget Management, ICT Procurement. ICT Training, Project Management, cybersecurity training, hardware provisioning, etc. and does not provide end user technical / desktop support.

The Service Desk

The Service Provider must have at least, the following resources available across Levels 1, 2 & 3. These resources must be readily available to deliver the core service. This is a pass / fail requirement. The following resources must be available;

- 10 X Service Desk Support Engineers (Incl. at least 1 SOC-Analyst)
- 2 X System Architects / Designers;
- 2 X Dedicated Managed Services Team Engineers;
- 2 X Backup & Replication Engineers; &
- 1 X Project Coordinator / Service Delivery Manager

The service provider must also have a call/service ticket tracking facility which can be accessed by CRU ICT personnel. This solution must be ITIL compliant.

All incidents and support requests, whether identified through the Service Desk or as a result of monitoring and maintenance, must be recorded and tracked within a Service Desk System / Solution. At a minimum, the information recorded in the Service Desk System / Solution must include:

- Unique incident reference number;
- Category and Description of incident;
- Source – user support call or another;
- Allocated priority;
- Time and date incident raised;
- Time and date of first contact;
- Resolved at first contact or escalated;
- Time and date incident escalated;
- Details of escalation;
- Classification and Description of how resolution achieved;
- Time and date of incident being resolved; and
- Time and date of incident being closed.

The Service Desk must provide regular updates to users as to progress of their service tickets/ incident resolution commensurate with priority level and also allow ICT staff, and in particular, the CRU ICT Manager to check the status of incidents and service tickets online by way of a portal.

The Service Desk system must allow the CRU ICT Manager, or any nominated ICT resource, to access up to date management information on incidents raised and the performance of the service provider in resolving incidents. Ideally, this management information should be available in real-time.

Service Desk Hours

The Service Desk core hours must be Monday to Friday 7.30am – 6.30pm, with the option for the CRU to extend service outside of these hours on request from CRU. Any extension beyond the core hours will be dealt with in accordance with the Change Control procedure in the call-off contract concerned.

Tenderers must outline what arrangements they would propose to put in place for emergency / unplanned cover outside of these core hours. The CRU will require emergency / out of hours support for system outages and / or system critical updates. This may include, but is not limited to, software / firmware updates to the CRU SAN devices and / or virtual hosts, essential security updates and / or resolving server outages / issues etc. This service will form part of the general ICT Managed Services and must be included in the annual fee.

Service Desk Contact

The Service Desk must support contact by telephone and email or a secure online application.

Support Request Answer Service Levels

Telephone calls must be answered within 60 seconds – excluding any automated keypad or voice activated routing, which itself should be no more than 3 levels.

If the phone cannot be answered within 60 seconds, the option to have a recorded message must be offered.

The Service Desk must respond to email and/or voice messages within 30 minutes where Priority is unknown to acknowledge support request and confirm priority classification - this is a service level. Otherwise, Initial Response must be in line with appropriate service level as set out in the table below.

Response and Resolution Service Levels

Response and resolution of support calls must be provided to the service levels set out in the following table. The level of failure to meet the stated service levels must not be greater than 10% for non-Critical calls and no greater than 5% for Critical calls in any of the agreed quarterly reporting periods:

Priority Level	**Priority Description**	***Initial Response***	***Solution Identified and / or Third Party Invoked***	***Problem Resolved***
1	**Critical**. System, application or service unavailable to all users of that system, application or service and it is seriously impacting CRU's ability to do business.	30 mins	1 hour	4 hours
2	**High**. System, application or service is not fully available to over 50% of users of that system, application	1 hour	2 hours	12 hours

	or service and it is impacting CRU's ability to do business.			
3	**High**. System, application or service available but service is degraded and is adversely affecting users. Work around or short-term fix exists but is unsustainable.	2 hours	4 hours	24 hours
4	**Medium**. System, application or service available with satisfactory work around in place for affected users.	4 hours	8 hours	50 hours
5	**Low**. Minor problem with limited or no impact to users or business.	8 hours	24 hours	100 hours

All service response times are hours within the core operating hours stated above (or, where applicable, any extended operating hours agreed with the CRU).

"**Initial Response**" is defined as:

- Support request logged, along with time of request, name of supported user, agreed priority, details of support required and a unique reference number; and
- Receipt and acknowledgement by email of the support request raised by a supported user – to include incident details.

The second level response (which is a service level) depends on whether the system, application or service is covered by a CRU third party support contract or warranty:

1 Where the support of the system, application or service is covered entirely by the ICT managed service, then the second level response time is for a solution to be identified and agreed with CRU, along with the required resources allocated to achieve resolution.

2 Where the system, application or service is covered by a CRU third party support contract or warranty, then the second level response time is for third party to have been contacted, and their service level triggered.

"**Resolution**" is defined as the restoration of the system, application and / or service to the satisfactory of the user requesting support; or the implementation of an acceptable (to the user) temporary work-around which will enable the system, application and/or service to be

used – the work-around must be signed-off by the user together with an agreement to a plan for a permanent solution to the problem.

Where a CRU third party support contract or warranty is involved, then the target time for resolution will not be less than the relevant service level within that CRU third party support contract or warranty. In such cases, the service provider must work with the relevant third party in the resolution of issues and manage the third-party service level agreement / contract / warranty on behalf of CRU.

It will be responsibility of the service provider to ensure that all issues, including those with third parties, are resolved to the satisfaction of the CRU and within the contracted service levels under the Service Framework Agreement. In the event that a third party vendor is not cooperating or fails to meet its obligations under their service level agreement / contract / warranty with the Commission, the issue should be brought to the attention of the CRU ICT Manager who will escalate it with the appropriate Account Manager. However, the Service Provider will still be responsible for ensuring a successful resolution is found to the issue / incident.

An incident can only be closed by agreement with the reporting user, the user's Manager or the CRU ICT Manager.

2.6 Dedicated Account Manager

The service provider must have a dedicated Account Manager as a single point of contact.

The Account Manager will be responsible as a single point of contact for all services provided under the Services Framework Agreement, whether as a part of the ICT Managed Services, SOC Services or ad hoc projects.

2.7 Quality Requirements

The Service Provider is required to be self-monitoring, and as such is required to put in place a set of procedures which will ensure the quality and delivery of service. This must ensure that the CRU's ICT infrastructure, systems, applications and services are readily available and that the CRU's data is protected to the best possible standard.

Two months after the handover from the existing supplier / establishment of the Services Framework Agreement, the Service Provider shall establish a Quality Plan compliant with the requirements of the CRU. The Quality Plan shall apply to all relevant ICT infrastructure, systems, applications and services that the Service Provider is responsible for (under any or all call-off contracts under the Services Framework Agreement) including but not limited to:

- **Systems Monitoring and Fault Rectification** - The Service Provider shall establish procedures to remotely monitor the operation of the CRU's ICT infrastructure, systems, applications and services so that faults occurring are identified as early as possible. These procedures should define the set of actions to be undertaken in the event of system, application or service failure.
- **Data Build and Data Checking –** The Service Provider shall identify the check points involved in any data manipulation processes and shall identify any automatic or manual tests which are carried out on the data whether partially built or complete in order to ensure its accuracy and completeness.
- **Systems and Data Updates –** The Service Provider shall put in place procedures which describe how updates to the systems, applications and its data are undertaken in a way that does not adversely affect the operation of the CRU's business services and the lines of reporting and liaison that are required in order to effect this. Data update procedures shall describe how any data is

released in a controlled way so that all delivery systems are updated with the same data and the checks that are made to ensure that the data update at each delivery system is successful.

- **Version Control** – The Service Provider shall put in place procedures to control and monitor changes to the systems, applications and data. Procedures shall describe the methods by which data, applications and systems are version and configuration controlled including documentation requirements and sign off processes. Procedures shall also identify how the systems, applications or data can be "rolled back" to a previous version in case of unforeseen problems with the update.
- **Change Management Procedures** The Service Provider shall comply with the change management procedures outlined in the appended Services Framework Agreement.
- **Security Procedures –** The Service Provider shall maintain a secure computing environment to the standard defined by CRU ICT Security Policies and conform to all the requirements of the Data Protection Acts 1988 to 2018 including GDPR (and as amended from to time to time). The Service Provider shall work with the CRU ICT Manager to determine various ways to enforce ICT Security Policies including, but not limited to:
    - minimise the risk of a computer virus, malware or ransomware being introduced into the CRU's computer network;
    - minimise the possibility of any unlawful electronic access into the CRU's computer network or data;
    - provide for the secure storage of the software, hardware, documentation, equipment under the control of the service provider; and
    - comply with security instructions issued by the CRU.

2.8 Price

Tenderers must include a fixed fee for the provision of ICT Managed Services and SOC Services (combined) for each year in the Tender Response Document – TRD Part C. Any costs associated with the transition / setup phase should be included in the fixed fee for YR 1.

3.0 Optional Dedicated Support Resource(s)

3.1 Overview

The CRU will have the right under this Services Framework Agreement to drawdown additional ICT Dedicated Support Resource(s), as it may require, from time to time. The following list, in section 3.2 below, is an indicative list of the types of resources, that CRU may require over the lifetime of this Services Framework Agreement. There is no guarantee of any particular volume of work, value, scope or frequency of appointments that may be made under this requirement. CRU reserves the right to drawdown and appoint, as and when required, and also reserves the right to cancel any such agreement, as required. The Service Provider must provide a daily rate, in TRD Part C, for each of the resources set out in the below list.

3.2 List of Dedicated Support Resource(s)

- Web Applications Developer / Programmer
- Applications Developer Architect
- Applications Developer Manager
- Mobile Developer Architect
- Mobile Applications Developer
- SharePoint Developer
- Test Manager
- Test Analyst
- Programme Manager
- Junior Project Manager
- Senior Project Manager
- Business Analyst
- Technical/Infrastructure Architect
- Database Systems Architect
- Database Systems Manager
- Database Systems Designer
- Database / Data Warehouse Consultant
- Data Architect
- Data Scientist
- Business Intelligence Architect
- Business Intelligence Analyst
- Business Intelligence Developer
- CRM Architect (MS Dynamics)
- CRM Developer (MS Dynamics)
- ICT Change Management Specialist
- SharePoint Support / Administrator
- Active Directory System Architect
- Storage (SAN) Architect
- Network Design Engineer
- Network Administrator
- Systems Administrator
- Virtualisation Specialist
- Information Security Architect
- Information Security Analyst
- Penetration Tester
- Cyber Security Specialist
- Cyber Security Engineer
- ICT Manager

4.0 Ad-hoc Project Work

4.1 Overview

The CRU will have the right under the Services Framework Agreement to drawdown additional ICT Consultancy Services, under Statements of Work (SoWs) as it may require from time to time. This will include, in particular:

- The design, implementation and deployment of a number of ICT Projects as summarised below. These projects will be awarded by the CRU ICT Manager to the Service Provider on a case-by-case basis as budgets allow. An indicative list of such projects is outlined below.

- Support for a number of priority tasks that the Service Provider may be required to deliver and / or input into under the direction of the CRU ICT Manager. These tasks are listed in the table in Annex G. The CRU ICT Manager will agree a plan for delivery of these tasks with the Service Provider at the outset of the Services Framework Agreement.

Tenderers should include a skills profile of proposed resource(s) to fulfil the above.

4.2 Identified ICT Projects

Under the CRU's recently developed Digital Strategy 2025 – 2030, a number of projects have been identified to improve the CRU ICT infrastructure, services, applications and solutions. There is a strong focus on value for money with the aim of reducing costs and aiding greater efficiency, effectiveness and productivity. Cost is a primary driver, and CRU will only be in a position to significantly alter or improve its ICT infrastructure if an economic return on investment can be demonstrated within a 3-4 year period.

Below is an indicative list of projects, that the CRU ICT Dept. will be focusing on over the next 4 years (this list is not exhaustive and does not limit the scope or type of projects that may be drawn down pursuant to this Services Framework Agreement under SoWs). CRU does not guarantee that all or any of the below projects will be delivered through the provision of professional services via the MSP under SoWs, and reserves the right to issue individual tenders, on a per project basis, if there is a possibility of achieving better value for money, through open competition.

- **Cyber Awareness Training** – specialised cybersecurity training to all staff as required. The MSP may be required to provide suitably qualified resources, to deliver this training, as per section 3.2 above.
- **CRU Intranet & Staff Portal** – centralised communication portal, integrated with the central document management solution, with collaboration functionality. The solution would integrate with existing and future business applications, support hybrid working, ensure accessibility to key data feeds like calendars and tasks, and be highly secure. The portal would be scalable and support CRU's strategic goals. It is likely that this software will be procured via an OGP Framework / open competition however the MSP may be required to provide suitably qualified resources, to support this project, as per section 3.2 above.
- **Finance System** – support, maintain and develop the existing Microsoft Business Central solution. This project will involve delivering various enhancements to the existing solution and implementing upgrades as and when required. The MSP may be

required to provide suitably qualified resources, to support this project, as per section 3.2 above.

- **Case Management & Workflow** – delivery of case management and workflow solutions. This may include, but is not limited to, Microsoft Dynamics, Salesforce or other similar solutions. This also includes supporting the existing Customer Care Team Microsoft Dynamics Platform and/or other internal solutions. The MSP may be required to provide suitably qualified resources, to support this project, as per section 3.2 above.
- **Integration Platform** – This Platform will connect CRU's business applications and data sources, enabling seamless, secure, and scalable data exchange and workflow automation. The solution would be designed to reduce complexity, improves data consistency, and support digital transformation by centralising integration management and aligning with CRU's strategic objectives. It is likely that this software will be procured via an OGP Framework / open competition however the MSP may be required to provide suitably qualified resources, to support this project, as per section 3.2 above.
- **Enterprise Architecture Solution** – Enterprise architecture solution to standardise, organise and develop roadmaps for the CRU ICT infrastructure and applications to align with, and facilitate, the achievement of organisational goals and objectives. It is likely that this software will be procured via an OGP Framework / open competition however the MSP may be required to provide suitably qualified resources, to support this project, as per section 3.2 above.
- **Various AI Solutions** – support AI initiatives that add value to CRU, this may include AI enabled search solutions, cybersecurity solutions, chatbots and/or other related technologies, etc. It is likely that these software solutions/ platforms will be procured via an OGP Framework / open competition however the MSP may be required to provide suitably qualified resources, to support this project, as per section 3.2 above.
- **Data & Reporting** – Business Intelligence reporting tools, enabling greater access to CRU datasets. It is likely that this software will be procured via an OGP Framework / open competition however the MSP may be required to provide suitably qualified resources, to support this project, as per section 3.2 above.
- **Cloud Migration** – Review of existing VMs / business applications with the potential of moving some / all to cloud-based solutions. The MSP will be required to assist the CRU in determining a suitable migration path / strategy and assist in conducting a Cost Benefit Analysis (CBA) for any future move to cloud-based solution(s). The MSP may be required to provide suitably qualified resources, to support this project, as per section 3.2 above.
- **Firewall(s)** – this project will involve a review and potential replacement of the existing physical firewalls on the Production and DR site(s) when they reach EOL. This review is not expected to take place until 2027. It is likely that hardware will be procured via an OGP Framework however the MSP may be required to provide suitably qualified resources, to support this project, as per section 3.2 above.
- **Software licencing** – Conduct comprehensive review / audit to ensure compliance and identify any licences required and / or no longer required. The MSP may be required to provide suitably qualified resources, to support this project, as per section 3.2 above.
- **Industry Portal** – this project will involve the implementation of multiple collaboration applications between CRU and industry participants, i.e. for licensing, consultations, secure file transfer and data entry. The solution would streamline interaction with industry stakeholders and would introduce automation where possible. It is likely that this software will be procured via an OGP Framework / open competition however the MSP may be required to provide suitably qualified resources, to support this project, as per section 3.2 above.

- **Records/ Document Management Solution** – this project may involve the upgrade of the existing solution or the wholesale replacement of it with an alternative solution if deemed to be more fit-for-purpose and aligned with CRU requirements. It is likely that this software will be procured via an OGP Framework / open competition however the MSP may be required to provide suitably qualified resources, to support this project, as per section 3.2 above.
- **Phone Solution** – this project will involve reviewing the current and future telephony requirements and developing and implementing a new telephony solution that meets the future hybrid working requirements of CRU and its stakeholders. It is likely that this software / platform will be procured via an OGP Framework / open competition however the MSP may be required to provide suitably qualified resources, to support this project, as per section 3.2 above.
- **LAN Upgrade –** this project will involve reviewing and replacing existing switches in the CRU main office and DR site. This review is not expected until 2027. It is likely that hardware will be procured via an OGP Framework however the MSP may be required to provide suitably qualified resources, to support this project, as per section 3.2 above.
- **ISO27001/ Cyfun Project –** this project will involve assisting the CRU in preparing for ISO27001/ Cyber Fundamentals certification. This work includes aligning CRU to the NIST Framework, and other similar frameworks, and implementing various technical initiatives as necessary. The MSP may be required to provide suitably qualified resources, to support this project, as per section 3.2 above.
- **Pen Testing –** this project would involve various pen testing initiatives, including physical testing, social engineering, phishing, vishing, smishing, etc. The MSP may be required to provide suitably qualified resources, to support this project, as per section 3.2 above.

The Service Provider may also be required to provide project specific support to CRU outside of the remit of the indicative list of projects specified above. The above list includes various initiatives set out in the CRU Digital Strategy 2025 – 2030 and also includes other general initiatives. CRU will engage in a detailed analysis in respect of each proposed project, with the successful tenderer, following award of the Services Framework Agreement. As stated, CRU may choose to procure any or all of the listed projects through separate competitive tenders if this approach is likely to deliver better value, and there is no obligation to assign these projects to the MSP under Statements of Work.

4.3 Price

Tenderers must include the maximum hourly / daily rates (assume 7.5 hrs per day) that will apply for any projects awarded SoWs (or, at the Commission's option, variations under the Change Control procedure for the ICT Managed Service) in the Pricing Schedule included, TRD Part C.

These maximum daily / hourly rates will apply for the duration of the Services Framework Agreement without any increase.

4.4 List of Resource(s) for Ad-hoc Projects

The below list sets out the typical resources used in the delivery of ad-hoc projects. This list is an indicative list and will be used for evaluation purposes. It does not limited CRU in respect of the resources that may be used for project related activities. CRU may decide to use a mix of ad-hoc resources and optional dedicated resources to deliver projects.

- ICT Solutions Architect
- Systems Engineer
- Information Security Engineer
- Cyber Security Specialist
- ICT Project Manager (Intermediate)

5.0 Software licensing renewals

Where available, the CRU will utilise Office of Government Procurement (OGP) Frameworks to renew existing software licences and/or purchase new software solutions. This approach ensures compliance with public sector procurement guidelines and leverages the benefits of aggregated purchasing power, supporting the objective of achieving best value for money in all software renewals. The Service Provider will be expected to work with the CRU to identify opportunities to use OGP Frameworks and to facilitate renewals and/or purchases through these channels whenever possible.

Where suitable OGP Frameworks are not available, the Service Provider may be required to renew and/or purchase some software licences on behalf of CRU, as part of its ICT operations. CRU expects the appointed Service Provider to secure the best possible value for money in all such transactions. Where appropriate, the Service Provider should utilise the request for supplemental tender process to ensure competitive pricing and transparency. The objective is to achieve software renewals at recommended retail prices or better, thereby maximising cost efficiency for the organisation while maintaining compliance and continuity of service. This approach supports the CRU's commitment to prudent financial management and high standards of service delivery throughout the duration of the Services Framework Agreement.

The appointed MSP must provide clear and ongoing assurances that all services, renewals, and procurements deliver best value for money for CRU. This requirement is fundamental to public sector procurement and is reinforced by both internal policy and national guidelines.

The MSP will be expected to:

- Demonstrate that all licence renewals / purchases, are competitively priced and benchmarked against market standards. This may involve providing CRU with multiple quotes, if available.
- Provide transparent reporting and justification for all costs, including evidence of competitive processes or market testing where frameworks are not available.
- Support the CRU in regular reviews of procurement strategy to ensure ongoing value for money, futureproofing, and alignment with the organisation's digital strategy.

These assurances must be embedded in the MSP's approach from contract award and throughout the contract lifecycle, with regular reviews and reporting to the CRU ICT Manager and Procurement Team.

The current list of software licences is provided at Annex H

6.0 Specification of Common Requirements

6.1 Introduction

The Service Provider is required to address the following requirements in the provision of all and any services under the Services Framework Agreement.

6.2 Transition Plan and Implementation

Tenders will be expected to outline in their responses a clear, concise plan for how they will manage and implement transition from the current arrangements in scope of this Services Framework Agreement to their proposed ICT Managed Services.

Where appropriate, the Service Provider will be responsible for transition of documentation from incumbents (in conjunction with the CRU ICT Manager), consolidation of this documentation and the maintenance of this documentation to reflect the current systems at all times.

The new Services Framework Agreement must be in place by **Monday, 4th April 2026**.

It will be the Service Providers responsibility to familiarise themselves with the infrastructure and support requirements before this date.

The CRU shall endeavour, where appropriate and possible, to make available its ICT Manager to the Service Provider during the transition period to provide reasonable input and information.[1] After this time the tenderer must assume full responsibility for the delivery of all services, as set out in the Services Framework Agreement.

6.3 Accessibility Requirements

All services provided under the Services Framework Agreement must be delivered in a manner consistent and compliant with the ICT accessibility guidelines prescribed by the National Disability Authority so that those with hearing, visual and learning difficulties in particular are all catered for in appropriate ways when using the ICT support services. The guidelines can be found at the website http://www.nda.ie.

7.4 Security

The Service Provider will be responsible for data protection and security of data to a standard of ISO27001 guidelines, or equivalent. The service provider must be familiar with the requirements of GDPR, FOI and any other relevant legislation.

7.5 Co-ordination with other 3rd Party ICT Suppliers

The CRU has contracts with other specialist ICT Providers including provision of Business Applications and associated support and maintenance.

It is a key requirement for the service provider to cultivate positive working relationships with all other ICT Providers (whilst doing so in accordance with any directions of the CRU ICT manager) in order to provide the underlying ICT infrastructure support and maintenance necessary to support the functions of each of those third parties and so that the overall ICT requirements of the CRU are satisfied.

An integrative approach that employs ICT as both an enabler and solution provider to the CRU and that uses best practice and industry standards, working within the boundaries of governance and compliance that apply to the CRU is necessary, and is required.

Where a CRU third party support contract or warranty is involved in order to resolve an ICT issue, the Service Provider must work with the relevant third party in the resolution of issues

[1] The availability or not of the CRU's ICT Manager within the transition period, or any information or input provided or not provided by them, will not impact on or dilute the Service Provider's obligations or responsibility or entitle it to any extension of time

and manage the third-party service level agreement / contract / warranty on behalf of CRU. It will be the responsibility of the Service Provider to ensure that all issues, including those with third parties, are resolved to the satisfaction of CRU and within the contracted service levels. In the event that a third-party vendor is not cooperating or should fail to meet its obligations under their service level agreement / contract / warranty with the Commission, the issue should be brought to the CRU ICT Manager who will escalate it with the appropriate Account Manager. However, the service provider will still be responsible for ensuring a successful resolution is found to the issue.

7.6 IP

All bespoke works, including software and documentation, and intellectual property delivered under the Services Framework Agreement are delivered for and on behalf of CRU, and as such are property of CRU exclusively. The Services Framework Agreement contains relevant provisions in this regard.

7.7 Exit

On completion of the Services Framework Agreement awarded under this procedure, the Service Provider will be responsible for the smooth and efficient transition of all up to date documentation / data to any new Service Provider(s) of the service and for assisting in the smooth and effective transition of the service. This includes an inventory of all software, licenses, assets, SaaS renewals, IaaS renewals, etc.

7.8 Proposals for Sustainability & Social Value

In addition to obligations in the field of environmental, social and labour law that apply at the place where the services are provided, that have been established by law listed in Schedule 7 of the European Union (Award of Public Authority Contracts) Regulations 2016, tenderers are required to demonstrate that adequate measures are in place to decarbonise their service delivery.

Tenderers must describe their approach to the sustainability and improving social value of business operations as it applies to the delivery of the services required under this contract. Such approaches may include:

- Specific proposals to address the environmental impact of the services being delivered which result in measurable reductions in emissions, energy, resource use or equivalent.
- Focus on contract specific measures to reduce environmental impact (e.g., device power policies, cloud carbon optimisation, device circularity, certified disposal/WEEE, travel minimisation), and / or social measures (e.g., apprenticeships, upskilling, local SME participation in the service supply chain) linked to delivery.
- Quantify expected impacts/ how measured; e.g. a 12–24 month improvement roadmap with KPIs and quantified benefits.

Annex A: Overview of CRU's Current ICT Environment

Existing ICT Environment

The Commission currently employs approximately 197 staff members who will require ICT Support and Managed SOC Services. Over the course of the contract, the total number of staff is projected to increase. The anticipated annual headcount growth is as follows: by the end of Year 1 – an additional 71 staff, by the end of Year 2 – a further 70, and by the end of Year 3 – a further increase of 49 staff, resulting in a total headcount of 387 employees by the end of the initial three-year period. CRU may also employ various contractors and/or consultancy staff during the lifetime of the contract who should be considered to be within scope for ICT support services. Staff numbers may however fluctuate during the four-year term, and any such changes will remain within the scope of the fixed charge for ICT Managed Services and SOC Managed Services.

The current ICT systems are provided to staff by way of a combination of on-premise and SaaS based solutions. The majority of systems are accessed via laptops and tablets from multiple locations, i.e. home and office environments, and a small number of desktop PCs are used for office-based activities. The key software solutions / systems deployed are set out in Annex D. This list is not exhaustive and is subject to change. All changes are within scope of this contract.

The CRU ICT Department currently consists of 10 staff, which includes 1 full time ICT Manager, 4 full time ICT Senior Technical Analysts, 1 full time Technical Analyst, 1 full time ICT Technical Assistant, 1 full time ICT Administrative Executive, 1 ICT & Facilities Officer and 1 part time records administrator. The CRU ICT Team is primarily focused on the delivery of the CRU Digital Strategy, ICT Project Management, Contract & Budget Management, ICT Procurement, ICT Training and other strategic priorities. The internal ICT Team will not be responsible or involved in the delivery of ICT Desktop Support. The Service Provider will be responsible for delivering full end to end desktop support to the CRU users and should not assume that the ICT Team will be available to assist with the delivery of same. The Service Provider will also be responsible for liaising with all 3rd Parties when external application and system support is required, and must oversee and resolve all service, support and incident tickets.

The current provision of ICT Services to the Commission is made up as follows;

External partnerships

- One primary external ICT Managed Service Provider (MSP) who is responsible for first, second and third level support for desktop, network and server related issues. The current provider also provides Managed SOC and DR Support Services. Additional work is provided on a separate project basis as and when required under SOWs. (This Contract)
- The main business applications used by all users are M365 & OpenText Content Manager. M365 issues are supported by the primary MSP, as needed. The OpenText Content Manager application is supported and maintained by a separate third-party company however 1st level support for Content Manager is within scope of this contract.

- The CRU Customer Care Team (CCT) use Microsoft Dynamics for the management of all Customer Care Cases. This solution is a SaaS based solution and is supported by a third-party provider however the new contract should have a provision to provide these services, if needed.
- The CRU HR Department use Strandum for the HRM. This solution is supported by a third-party provider.
- The Finance Department use Microsoft Business Central. Support for this solution is provided by a third party, however the new contract should have a provision to provide these services, if needed.
- The Commission has a number of Internet Service Providers who provide Internet connectivity to the Commission. These services are currently provided by Virgin Media, Eir and Government Networks.
- The Commission use FortiGate Firewalls on all sites. These devices are within scope for the new MSP Contract.
- The Commission has a number of audio-visual devices, such as large LCD screens, various video conferencing Logitech devices. Support for these devices is currently provided by a third-party provider, however the new contract should have a provision to provide these services, if needed.
- The Commission has a Disaster Recovery system which is in the Revenue Data Centre. Hosting is provided by the Revenue. (Management and maintenance of this system is within scope of this MSP contract)
- A Managed Print Service (MPS) is in place with a third-party provider via an OGP framework agreement. 1st level support is within scope for this MSP contract.
- A number of smart phones (iPhones & Android) are provided to a subset of staff, and these devices are supported by a third party. 1st level support is within scope for this MSP contract.
- The purchase of laptops, tablets, PCs and associated consumables is via 3rd Party provider(s) under an existing OGP framework agreement. Support of these devices is within scope of this MSP Contract.
- The Commission uses Keyhouse as a case management system within the Legal Dept. This product is supported by a third-party provider.
- The Commission uses ATMS for tracking safety actions within the Energy Safety Division. This solution is supported by a third-party provider.
- The Commission uses Plexos Modelling software within the Energy Markets Division. This solution is supported by a third-party provider.

All solutions supported by 3rd parties must be supported at Level 1 prior to any escalation. The MSP will be required to gain a general understanding of all products used.

Core ICT Systems

The Commission employs a Microsoft Windows Server Domain architecture with Active Directory/ Entra ID. The main Production & DR servers are built upon VMWare with full virtualisation aside from two separate Veeam servers which are used for backup and replication purposes. The physical hardware on the production site is a Dell PowerStore SAN and two Dell Hosts with identical equipment on the DR site.

The network protocol in use is TCP/IP with the possible intention to adopt IPv6 in the future.

The Commission's email is based on the Microsoft Exchange Online.

Remote access for users is provided via FortiGate VPN. Some users connect to the CRU system using VDI. Remote access solutions are protected by MFA with number matching. Various conditional access policies are in place.

The following is an overview of the Commission's Core environment.

8 Attached at ***Annex B*** is a diagram that provides a high-level view of the Commission's network. All equipment and network connections shown on the diagram are in scope for this requirement. The ICT Managed Services Provider will be expected to work with the Commission to help manage all external ICT related agreements.

9 Attached at ***Annex C*** is a list of all hardware currently in use at the Commission; all of this hardware is in scope for this requirement; appropriate third-party support arrangements are, or should be assumed, to be in place for all currently active hardware.

10 Attached at ***Annex D*** is a list of all software currently in use at the Commission – including number of users of each and version installed; all this software is in scope for this requirement; appropriate third-party support arrangements are or should be assumed to be in place for all currently active software.

Desktop Environment

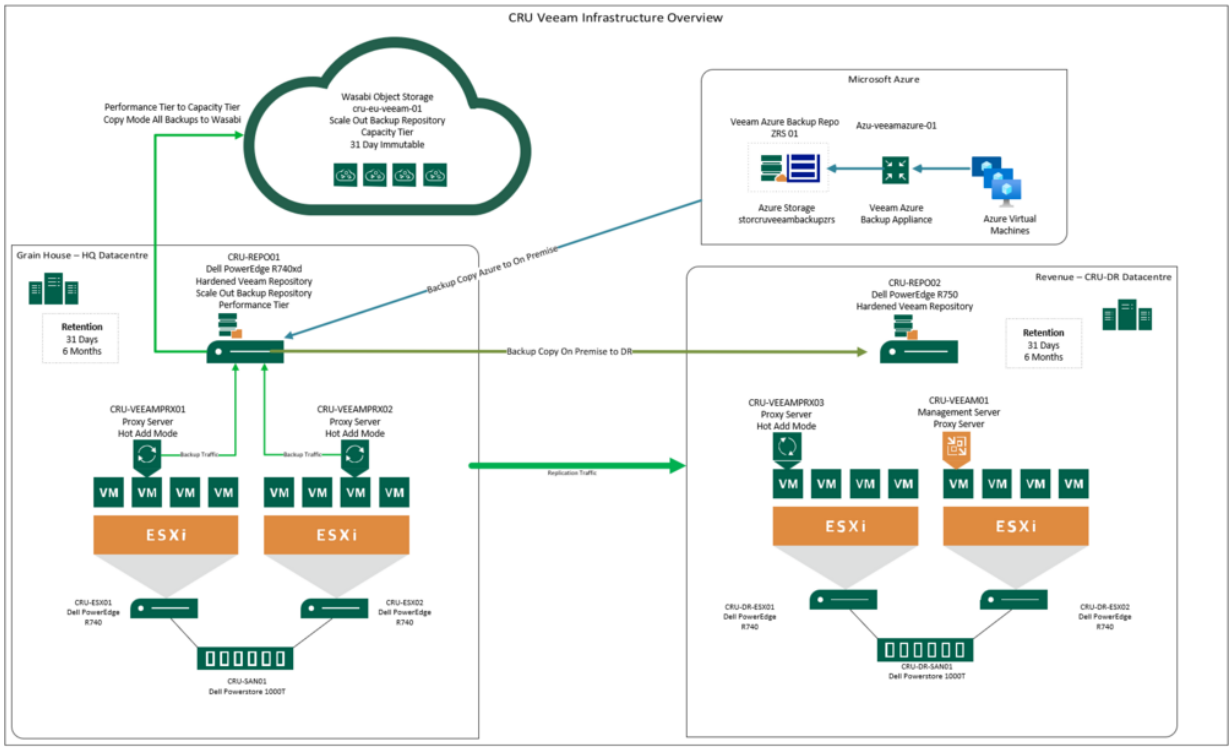
The current desktop environment for all users is as follows:

- The majority of laptops and Tablets currently used by the Commission are using the Microsoft Windows 11 operating System. An upgrade to future versions of Microsoft Operating Systems for all devices is within scope of this contract.
- The office productivity suite used by the majority of staff is Microsoft 365 Business Premium, and in a small number of cases F3, E3 and E5. All are within scope for support.
- OpenText Content Manager is installed on all devices, and 1st level support is within scope for support.
- Each device has the following security software installed, Bitlocker, Sophos Intercept X, Cisco Umbrella and remote monitoring tools.

Annex B: High Level View of the CRU's Network

The diagram below depicts an overview of the CRU Environment.

1. The CRU currently have approx. 45 (Prod), 63 (DR) with 11 live 52 offline & 8 VMs in Azure.
2. The system is based upon a VMWare environment on a Dell SAN with two hosts on each site
3. The LAN infrastructure is based on Cisco Meraki Switches & wireless APs. These access points have multiple Wi-Fi Networks which broadcast in the CRU main office.
4. There are two physical Veeam Servers for onsite backup and replication.
5. There are two Fortinet Firewalls in Production, and 2 in DR. There is 1 virtual Firewall VM in Azure.
6. There is a cloud Wasabi Repository for cloud backup storage.
7. The LAN infrastructure is based on Cisco Meraki Switches & wireless APs.
8. The DR site has a replica SAN and two Dell Hosts, also due to be replaced shortly (Figure 2)



Annex C: List of Current Hardware

In-scope Infrastructure

Device	Quantity	Role/ Function	Status
Dell PowerStore 1000T	2	Main Storage Area Network Device	Under warranty & will be retained.
Dell R740	6	Two Veeam Servers & four VMWare Hosts (Split across 2 sites)	Under warranty & will be retained.
Cisco Meraki Switches & Aps	12 Switches 10 Access Points	LAN & Wireless	Under warranty & will be retained for now. Subject to change during the next contract period.
Laptops (Mixed Manufacturers Incl. HP, Dell, Lenovo)	225+	Primary Staff Devices	All Under warranty & will be replaced as needed.
Printers MFPs (Under 3rd Party Contract)	5	Primary printing devices	All Under warranty & will be replaced as needed.
Video Conferencing (Primarily Logitech Equipment)	17	Primary VC solutions in all meeting rooms	All Under warranty & will be replaced as needed.
Firewalls (Fortinet 100F) Production & DR	4 Physical 1 Virtual (Azure)	Primary Firewalls	All Under warranty & will be replaced as needed.
NEC SV9100 PBX	1	Legacy Phone System	In the process of being decommissioned

Client devices

Laptops and tablets are sourced via an OGP Framework Agreement. All devices are within warranty and will be replaced on an ongoing basis via the OGP drawdown agreement.

Network

The network within the CRU is based upon Cisco Meraki devices deployed across all floors and connected via fibreoptic cabling.

Wireless Network

Various access points are also installed across all floors.

Annex D: List of Current Software

The following is the software deployed on a standard users device (Some users will require additional specific software installed depending on their role, i.e. Finance, HR, Energy Modelling etc. see Annex A above for a full list of additional applications);

a) M365 Business Premium incl. Teams, Outlook, Word, Excel, PowerPoint, etc.
b) OpenText Content Manager v24.5
c) Sophos AV & Intercept X
d) MS Project (On some devices)
e) MS Visio (On some devices)
f) Adobe Acrobat Reader
g) Edge / Chrome
h) Cisco Umbrella
i) Monitoring Tools
j) Bitlocker

All Client devices are currently running MS Windows 11 OS. Future upgrades to newer versions of Microsoft operating systems for all end user devices is within scope of the standard MSP Services Framework Agreement.

The following list sets out the software currently used within the ICT environment. This list is not exhaustive and is subject to change. Software solutions will move in and out of scope of the managed services contract throughout the contract term.

Software Solution	MSP 1st Level Support Required	MSP 2nd & 3rd Level Support Required	3rd Party Vendor Support Available
Microsoft 365 Business Premium, F3, E3 & E5 (Including future M365 Products)	Yes	Yes	Yes (CSP)
Microsoft Windows server 2016, 2019, 2022 & 2025 (Including future Microsoft Server OS Products)	Yes	Yes	Yes (CSP)
Microsoft Windows 11 (Client Devices) and future Microsoft Client Operating Systems	Yes	Yes	Yes (CSP)
VMware 8.0 (Including future versions)	Yes	Yes	Yes
Cisco Meraki	Yes	Yes	Yes
Cisco Umbrella	Yes	Yes	Yes
SafeCom Managed Print	Yes	No	Yes
OpenText Content Manager for Records Management	Yes	No	Yes
Microsoft Dynamics for Customer Care (SaaS)	Yes	No	Yes
Microsoft PowerBI, SQL, Visio, Project, SharePoint	Yes	Yes	Yes (CSP)

Microsoft Business Central	Yes	No	Yes
Strandum HR	Yes	No	Yes
Pisys ATMS (Action Tracking Management System)	Yes	No	Yes
Plexos Integrated Energy Model Software	Yes	No	Yes
Keyhouse Legal Case Management	Yes	No	Yes
MS Teams & Zoom	Yes	Yes	Yes
Decision Time (OneAdvanced);	Yes	No	Yes
SAP Concur (SaaS)	Yes	No	Yes
Veeam Backup & Replication	Yes	Yes	Yes
Darktrace	Yes	Yes	Yes
Connect Secure	Yes	Yes	Yes
Sophos Intercept X	Yes	Yes	Yes
Wasabi	Yes	Yes	Yes
Mimecast	Yes	Yes	Yes
Lookout Enterprise Security (Mobile Devices)	Yes	Yes	Yes
Rocket Cyber	Yes	Yes	Yes
Active Directory/ Entra ID/ IAM/ PIM/ Conditional Access/ MFA/ SSO/ Azure	Yes	Yes	Yes
IT Glue/ My Glue/ Fresh Service (CMDB)	Yes	No	Yes
Citric/ Progress ShareFile	Yes	No	Yes
uSecure	Yes	No	Yes
DUO	Yes	Yes	Yes
Nerdio	Yes	Yes	Yes
Logitech Room Booking Solution	Yes	No	Yes
OneSpan eSignature	Yes	No	Yes
RedHat Linux	Yes	Yes	Yes
Fortinet VPN Software	Yes	Yes	Yes

Annex E: Audio Visual Requirements

Below is a list of the audio-visual equipment currently installed in the CRU meeting rooms that is required to be covered for L1 Support as part of the new ICT Managed Services Framework Agreement.

- Logitech Rally Pro PTZ Camera with Logitech Tap Touch Controller X 1
- Logitech Meetup advanced conference video bar X 16

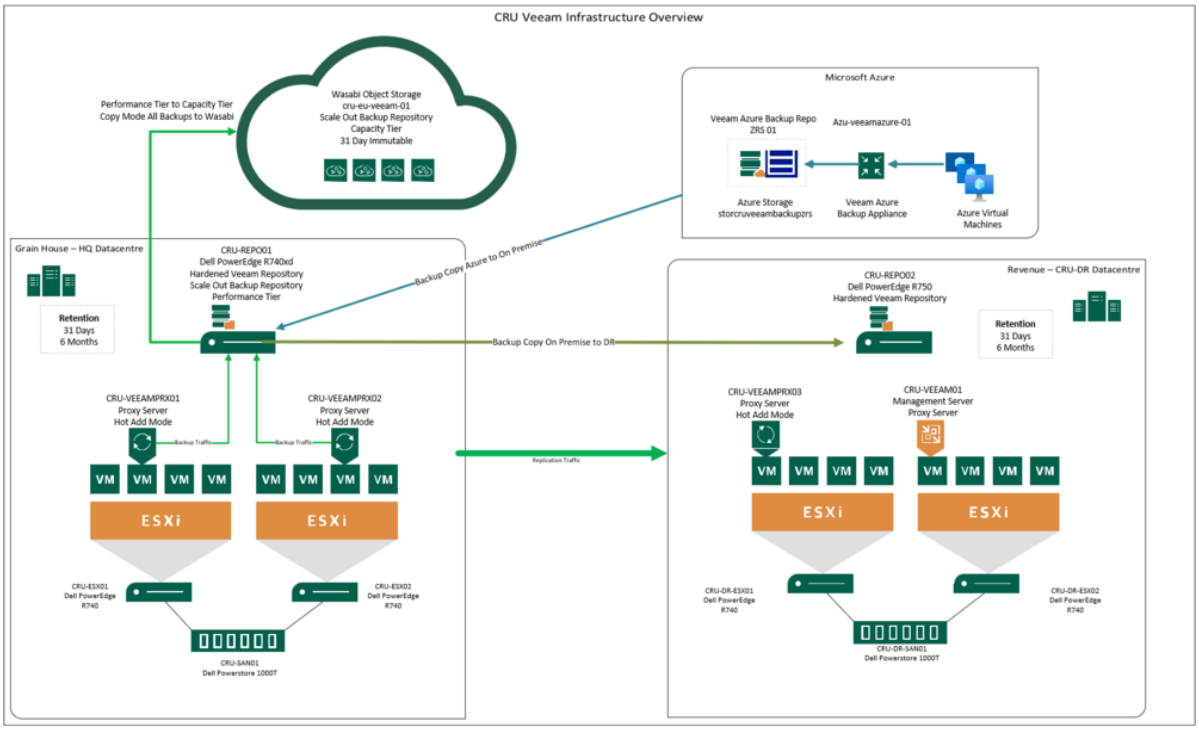
Each meeting room has an audio-visual display consisting of either a small or large screen LCD display. All hardware is within scope for L1 Support which can be escalated to L2 Support with various external providers, if necessary.

Annex F: Disaster Recovery – Current Set-up

The current Disaster Recovery (DR) solution in place for CRU is based on Veeam backup and replication to an offsite data centre located in the Revenue Datacentre. Wasabi Cloud backup storage is also used. CRU propose to continue to use the current solution(s) for the medium to long term, subject to further discussions with the new MSP. The Service Provider must maintain, support and potentially enhance this current solution. The MSP will be required to perform regular DR Tests, as agreed with the CRU ICT Manager. These tests must be conducted on a quarterly basis, at a minimum.

The Service Provider will be required to monitor, maintain and support the existing backup and replication solution. Monthly reports will be required and will be assessed at the quarterly service review meeting. The Service Provider will be required to install monitoring agents on the DR systems and ensure all alerts and issues are resolved. Monthly patching of the DR site will be required at both OS level and VMware host level. Firmware updates to hardware is also within scope. The Service Provider will be required to monitor the VPN to the DR site to ensure it remains stable and also secure from any external threats.

The MSP will also be required to review the existing solution and recommend improvements and / or enhancements that will provide overall benefits for CRU.



Annex G: Priority Tasks

There are a number of priority tasks that the service provider must deliver and / or input into under the direction of the CRU ICT Manager. The tasks are listed in the table below in no particular order. The CRU ICT Manager will agree a plan for delivery of these onboarding tasks with the successful tenderer at the outset of the Services Framework Agreement.

#	Task
1	Review, enhance and develop the BCP and DR Plans to ensure they are relevant for the new Managed Services Contract.
2	Review all CRU ICT Policies
3	Review, enhance and develop the CRU ICT knowledgebase for desktop support engineers to ensure they are familiar with all CRU ICT Systems, applications and services.
4	Implement a formal Patch Management Process for both the production and DR sites and submit to the CRU ICT Manager for approval.
5	Implement a formal Change Management & Approval Process.
6	The MSP shall routinely review and optimise the company's request and ticket types, including troubleshooting categories and process flows, to ensure clarity and efficiency. The MSP will design and maintain customized templates, workflows, and approval paths within the ticketing system to streamline internal requests. All improvements must enhance request visibility, approval accuracy, and overall process consistency.
7	Develop & Implement Formal Incident Response Process (CSIRT) in accordance with the CRU Security Management Framework.
8	Implement Formal Monitoring of Audit Trails and Security Logging
9	Review and revise current CRU Security solutions, as required.
10	Implement a portal for the CRU ICT Team to monitor the progress of all desktop support tickets and managed service tickets
11	Deploy agents on CRU assets and ensure all are actively monitoring for faults and incidents
12	Train desktop support engineers on any CRU bespoke applications that require 1st level support
13	Implement a reporting mechanism for the CRU ICT Manager to access key information. E.g. Monthly Service Reports, Patch Management Reports etc.

14	Establish a formal service review process, to ensure all reports, for consideration, are available to the CRU ICT Manager 5 days prior to any such meeting. Reports will include an up-to-date service ticket review noting SLA conformance, security reports, project updates and any other material that the CRU ICT Manager deems necessary. The frequency of the meetings will be agreed with the CRU ICT Manager at the commencement of the Services Framework Agreement and may be subject to change by agreement during the contracted term.
15	The MSP shall perform regular audits of all user accounts, including guest, staff, and service accounts across all on-premise, cloud, server, and application environments. Following each audit, the MSP must produce a report detailing findings, actions taken, and required remediation. The MSP is responsible for cleaning up, correcting, and securing any identified issues to maintain a compliant and secure environment.
16	The MSP shall provide structured audit reports that include both a detailed technical analysis with recommendations and a simplified high-level overview suitable for management review. Reports may cover SOC activities, account cleanup, security findings, and operational performance. This dual-format reporting is intended to improve clarity, reduce review time, and increase overall efficiency and productivity.

Annex H: Software Renewals

CRU operates a diverse suite of software and systems, each requiring timely licence renewals to ensure compliance and seamless service delivery. Under the new ICT Managed Services Framework Agreement, it is critical to proactively manage and renew licences for all core applications, security solutions, and productivity tools. This includes, but is not limited to, essential solutions as set out in Annex D above.

Wherever possible, CRU will utilise Office of Government Procurement (OGP) Frameworks to renew existing software licences. This approach ensures compliance with public sector procurement guidelines and leverages the benefits of aggregated purchasing power, supporting the objective of achieving best value for money in all software renewals. The appointed Service Provider is expected to work with the CRU to identify and facilitate renewals through OGP Frameworks. Where suitable frameworks are not available, the Service Provider may be required to renew licences on behalf of CRU, always aiming to secure the best possible value and maintain compliance.

The appointed MSP must provide clear and ongoing assurances that all services, renewals, and procurements deliver best value for money to CRU. This requirement is fundamental to public sector procurement and is reinforced by both internal policy and national guidelines. The MSP will be expected to:

- Demonstrate that all licence renewals, are competitively priced and benchmarked against market standards.
- Provide transparent reporting and justification for all costs, including evidence of competitive processes or market testing where frameworks are not available.
- Support the CRU in regular reviews of procurement strategy to ensure ongoing value for money, futureproofing, and alignment with the organisation’s digital strategy.

These assurances must be embedded in the MSP’s approach from contract award and throughout the contract lifecycle, with regular reviews and reporting to the CRU ICT Manager and Procurement Team.

The following list of licenses may fall within scope for renewal under the ICT MSP Contract.

Product/ License	Quantity	Renewal Type
Wasibi Backup & Recovery	50TBs	MSP
Red Hat Enterprise Linux Server	2	MSP
ATMS	30 Users	MSP
Cisco Umbrella	200 Users	OGP
Citrix/ Progress ShareFile	30 Users	MSP
DMARC Essentials	N/A	MSP
Fresh Service	10 Users	MSP
Meraki	12 Devices	OGP
Lookout Enterprise Security	50 Devices	MSP
Microsoft Teams Phone System	200 Users	MSP
Mimecast	220 Users	MSP
Nerdio	10	MSP
uSecure	200 Users	MSP
Veeam Backup & Replication	2	OGP
VMWare/ Broadcom	2	OGP
Fortinet Firewalls	5	OGP
Microsoft Azure Consumption	Monthly Storage & Compute Power	MSP/OGP
Darktrace	200 Users	MSP

*__NB:__ This list is subject to change, and any additions should be considered within scope.

Appendix 2: Pricing Schedule

Tenderers are required to complete **Tender Response Document (TRD) Document C: Cost Award Criteria** noting the following**:**

Instructions	
Tender Response Document (TRD) – Document C applies to **011-03-609: Single Member Framework Agreement for the Provision of ICT Managed Services 2026-30**	
	**Instructions for completion of Document C Cost Award Criteria (300 Marks)** • Tenderers who wish to be considered for this competition must fully complete **all sections** of this document. • Tenderers are not permitted to include any additional Price Assumptions in their response. Any such information provided WILL NOT BE CONSIDERED.

Tenderers are required to confirm that the tender holds good for the period set out in paragraph 2.23.2 after the closing date for receipt of tenders. This period may be extended where the Tender validity period is extended pursuant to paragraph 2.23.3.

Appendix 3: Tenderers' Statement (See TRD A)

Tenderers shall complete and return the following form of Tenderers' Statement

TENDERERS' STATEMENT

TO: Commission for Regulation of Utilities

RE: Request for Tenders for the Single Member Framework Agreement for the Provision of ICT Managed Services 2026-30 [011-03-609]

Having examined your Request for Tenders (the "RFT") including the Instructions to Tenderers, the Selection and Award Criteria, the Requirements and Specifications, and the terms and conditions of the Services Framework Agreement, we hereby agree and declare the following:

1. We understand the nature and extent of the Services required to be delivered as described in the Requirements and Specifications at Appendix 1 to the RFT.
2. We accept all of the terms and conditions of the RFT, the Services Framework Agreement and the Confidentiality Agreement and agree, if awarded a Services Framework Agreement, to execute the Services Framework Agreement at Appendix 5 to the RFT and the Confidentiality Agreement at Appendix 6 to the RFT.
3. We accept all the Selection Criteria and Award Criteria as set out in Part 3 of the RFT.
4. We agree to provide the Contracting Authority with the Services in accordance with the Services Framework Agreement and our Tender.
5. We agree that, if awarded any Services Framework Agreement, we shall, in the performance of such contract, comply with all applicable obligations in the field of environmental, social and labour law.
6. We confirm that we have complied with all requirements as set out at Part 2 of the RFT.
7. We confirm that all prices quoted in our Tender will remain valid for the period of time commencing from the Tender Deadline, as specified at paragraph 2.10.3 of the RFT.
8. We shall, if awarded any Services Framework Agreement under the RFT, have in place on the Effective Date of the Services Framework Agreement all insurances (if any) as required by paragraph 2.21.1 and paragraph 2.21.2 of the RFT.

Signed: (Authorised Signatory)	
Print Name	Click here and insert details
Position:	Click here and insert details
Company:	Click here and insert details
Address	Click here and insert details
	Click here and insert details
Date:	Click here and insert details

Appendix 4: Declaration as to Personal Circumstances of Tenderer (See TRD A)

Re: Request for Tenders for the Single Member Framework Agreement for the Provision of ICT Managed Services 2026-30 [011-03-609]

Name of Tenderer:	Click here and insert name
Registered Office:	Click here and insert address
	Click here and insert address
	Click here and insert address

I, _____, *[insert name of Declarant]* having been duly authorised by _____ *[insert name of entity]*, sincerely declare that _____ *[insert name of entity]* itself or any person who has is a member of the administrative, management or supervisory body of _____ *[insert name of entity]* or has powers of representation, decision or control in _____ *[insert name of entity]*:

(a) Has never been the subject of a conviction for participation in a criminal organisation, as defined in Article 2 of Council Framework Decision 2008/841/JHA.

(b) Has never been the subject of a conviction for corruption, as defined in Article 3 of the Convention on the fight against corruption involving officials of the European Communities or officials of Member States of the European Union and Article 2(1) of Council Framework Decision 2003/568/JHA as well as corruption as defined in the national law of the Contracting Authority or _____ *[insert name of entity].*

(c) Has never been the subject of a conviction for fraud within the meaning of Article 1 of the Convention on the protection of the European Communities' financial interests.

(d) Has never been the subject of a conviction for terrorist offences or offences linked to terrorist activities, as defined in Articles 1 and 3 of Council Framework Decision 2002/475/JHA respectively, or for inciting or aiding or abetting or attempting to commit an offence, as referred to in Article 4 of that Framework Decision.

(e) Has never been the subject of a conviction for money laundering or terrorist financing, as defined in Article 1 of Directive 2005/60/EC of the European Parliament and of the Council.

(f) Has never been the subject of a conviction for child labour and other forms of trafficking in human beings as defined in Article 2 of Directive 2011/36/EU of the European Parliament and of the Council.

(g) Is not in breach of its obligations relating to the payment of taxes or social security contributions.

(h) Has, in the performance of all public contracts, complied with applicable obligations in the field of environmental, social and labour law that apply at the place where the works are carried out or the Services provided, that have been

established by EU law, national law, collective agreements or by international, environmental, social and labour law listed in Schedule 7 of the European Union (Award of Public Authority Contracts) Regulations 2016.

(i) Is not bankrupt or the subject of insolvency or winding-up proceedings, its assets are not being administered by a liquidator or by the court, it is not in an arrangement with creditors, its business activities are not suspended nor is it in any analogous situation arising from a similar procedure under national laws and regulations.

(j) Is not guilty of grave professional misconduct.

(k) Has not entered into agreements with other economic operators aimed at distorting competition.

(l) Is not aware of any conflict of interest due to its participation in the Competition.

(m) Has not had any prior involvement in the preparation of the Competition.

(n) Is not guilty of significant or persistent deficiencies in the performance of a substantive requirement under a prior public contract, a prior contract with a contracting entity, or a prior concession contract, which led to early termination of that prior contract, damages or other comparable sanctions.

(o) Is not guilty of serious misrepresentation in supplying the information required for the verification of the absence of grounds for exclusion or the fulfilment of the Selection Criteria for this Competition and did not withhold such information and did not fail or is not able to submit supporting documents in respect of this Competition as required under Regulation 59 of the European Union (Award of Public Authority Contracts) Regulations 2016.

(p) Has not undertaken to unduly influence the decision-making process of the Contracting Authority in respect of the Competition, or obtain confidential information that may confer upon it undue advantages in respect of the Competition; or negligently provided misleading information that may have a material influence on decisions concerning exclusion, selection or award.

except to the extent expressly stated otherwise here:

[Please identify, if relevant, which of the above statements is applicable in the box provided above.]

I understand and acknowledge that the provision of inaccurate or misleading information in this declaration may lead to my business/firm/company/partnership being excluded from participation in this or future tenders, and I make this solemn declaration conscientiously believing the same to be true and by virtue of the Statutory Declarations Act, 1938. This declaration is made for the benefit of the Contracting Authority.

Signature of Declarant	**Name of Declarant in print or block capitals**

Declared before me by _____ who is personally known to me

(or who is identified to me by _____ who is personally known to me)

at _____ this _____ day of 2026

_____

(signed) Practicing Solicitor / Commissioner for the Oaths

Appendix 5: Services Framework Agreement

Please refer to separate document – Appendix 5

RFT Appendix 6: (Additional Schedule to Services Framework Agreement) Confidentiality Agreement

THIS AGREEMENT is made on the [date] day of [month] 2025 BETWEEN:

[Insert name of Contracting Authority] of [insert Address] (hereinafter "the Contracting Authority") of the one part; and

[Contractor's legal name: to be completed on signing.], of [Contractor's address: to be completed on signing.] (hereinafter called "the Contractor") of the other part.

WHEREAS

A. By Request for Tenders dated [insert date] entitled [insert title] (the "RFT") the Contracting Authority invited tenders ("Tenders") for the provision of the services described in Appendix 1 to the RFT (the "Services") ("the Competition"). The Contractor submitted a response to the RFT dated the [Insert Date of Tender].

The Contractor has been identified as the preferred bidder in the Competition.

B. For the purposes of the Competition and any subsequent contract awarded thereunder (if any) ("the Contract") certain confidential information (the "Confidential Information") as defined at clause 2 of this Agreement, will be furnished to the Contractor. The Confidential Information is confidential to the Client.

NOW IT IS HEREBY AGREED in consideration of the sum of €2.00 (the receipt of which is hereby acknowledged by the Contractor) as follows:

1. The Contractor acknowledges that Confidential Information may be provided to him by the Contracting Authority and that each item of Confidential Information shall be governed by the terms of this Agreement.

2. For the purposes of this Agreement "Confidential Information" means:

2.1 unless specified in writing to the contrary by the Contracting Authority all and any information (whether in documentary form, oral, electronic, audio-visual, audiorecorded or otherwise including any copy or copies thereof and whether scientific, commercial, financial, technical, operational or otherwise) relating to the Contracting Authority, the provision of services under the Contract and all and any information supplied or made available to the Contractor (to include agents, Subcontractors, customers and suppliers) for the purposes of the Contract (s); and

2.2 any and all information which has been derived or obtained from information described in sub-paragraph 2.1

3. Save as may be required by law, the Contractor agrees in respect of the Confidential Information:

3.1 to treat such Confidential Information as confidential and to take all necessary steps to ensure that such confidentiality is maintained;

3.2 not, without the prior written consent of the Contracting Authority, to communicate or disclose any part of such Confidential Information to any person except

i to those employees, agents, Subcontractors and other suppliers on a need to know basis; and/or

ii to the Contractor's auditors, professional advisers and any other persons or bodies having a legal right or duty to have access to or knowledge of the Confidential Information in connection with the business of the Contractor

PROVIDED ALWAYS that the Contractor shall ensure that all such persons and bodies are made aware, prior to disclosure, of the confidential nature of the Confidential Information and that they owe a duty of confidence to the Contracting Authority, and shall use all reasonable endeavours to ensure that such persons and bodies comply with the provisions of this Agreement.

4. The obligations in this Agreement will not apply to any Confidential Information:

i in the Contractor's possession (with full right to disclose) before receiving it from the

Contracting Authority; or

ii which is or becomes public knowledge other than by breach of this clause; or

iii is independently developed by the Contractor without access to or use of the
Confidential Information; or

iv is lawfully received from a third party (with full right to disclose).

5. The Contractor undertakes:

5.1 to comply with all directions of the Contracting Authority with regard to the use and application of all and any Confidential Information or data (including personal data as defined in Data Protection law);

5.2 to comply with all directions as to local security arrangements deemed reasonably necessary by the Contracting Authority including, if required, completion of documentation under the Official Secrets Act, 1963 and comply with any vetting requirements of the Contracting Authority including by police authorities;

5.3 upon termination of the Competition (or the Contract) for whatever reason to furnish to the Contracting Authority, all Confidential Information or at the written direction of the Contracting Authority to destroy in a secure manner all (or such part or parts thereof as may be identified by the Contracting Authority) Confidential Information in its possession and shall erase any Confidential Information held by the Contractor in electronic form. The Contractor will upon request furnish a certificate to that effect should the Contracting Authority so request in writing. For the avoidance of doubt

"document" includes documents stored on a computer storage medium and data in digital form whether legible or not; and

5.4 to comply with the requirements of Data Protection law

5.5 for the purposes of this Agreement "Data Protection law" means all applicable national and EU data protection laws, regulations and guidelines, including but not limited to the Data Protection Acts 1988 to 2018; Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (the General Data Protection Regulation), and any guidelines and codes of practice issued by the Data Protection Commission or other supervisory authority for data protection in Ireland from time to time.

6. The Contractor shall not obtain any proprietary interest or any other interest whatsoever in the Confidential Information furnished to him by the Contracting Authority and the Contractor so acknowledges and confirms.

7. The Contractor shall, in the performance of the Contract, access only such hardware, software, infrastructure, or any part of the databases, data or ICT system(s) of the Contracting Authority as may be necessary for the purposes of the Competition (and obligations thereunder or arising therefrom) and only as directed by the Contracting Authority and in the manner agreed in writing between the Parties.

8. The Contractor agrees that this Agreement will continue in force notwithstanding any court order relating to the Competition or termination of the Contract (if awarded) for any reason.

9. The Contractor agrees that this Agreement shall in all aspects be governed by and construed in accordance with the laws of Ireland and the Contractor hereby further agrees that the courts of Ireland have exclusive jurisdiction to hear and determine any disputes arising out of or in connection with this Agreement.

SIGNED for and on behalf of the Contracting Authority (being a duly authorised officer)	SIGNED for and on behalf of the Contractor
Witness	Witness