Invitation to Quote

RSSB2454– Information Security AdviceProject title

Dear Sir/Madam

RSSB is pleased to invite you to submit a quotation to RSSB for Information Security Advice**.**

The following documents are enclosed which contain all the necessary information you need:

Please read instructions carefully:

1. Instructions
2. The Specification
3. Evaluation Criteria
4. Conditions of Contract

Appendix A: Draft Terms and Conditions

Appendix B: Pricing Schedule

Your Quote should contain all the relevant information and comply with this request.

Quotations must be submitted to the undersigned by the date detailed in section 1.3 below.

Yours faithfully

**Gemma Cuthbert**

**Principal Procurement Business Partner**

<<Enter Name

<<Enter Job Title

1.0 INSTRUCTIONS

1.1 INTRODUCTION TO THE REQUIREMENTS OF THE TENDER:

RSSB is delivering next generation safety reporting technology for the rail industry, making it easier for people to collect information, and extract intelligence.

Modernising safety reporting capability is a key part of the industry's health and safety strategy, and will make it easier for companies to report and track safety incidents and investigations, and so provide the right risk information in the right format to the right people at the right time.

RSSB are creating a completely new cloud-based on-line system exploiting commercial off-the-shelf, state of the art, safety management software, which will replace both the existing Safety Management Information System (SMIS) and Close Call systems.  These currently rely on costly and outmoded technology.

The new system will be called the **Safety Management Intelligence System (SMIS).**

This is a cloud-based system (AWS: Amazon Web Services) and developed by IG (Ideagen Gael). RSSB has agreed to procure SMIS for itself, and on behalf of the rail industry, who shall have access to and use of SMIS (and related data within) once SMIS has gone live.

RSSB placed a contract with IG in March 2016 and the Phase 1 system launch is due in Q1 2017. Prior to launch, a generic (Security-Informed) Safety Case must be prepared by RSSB and presented for signature to the SMIS Programme Board.

The high-level system architecture is defined in Figure 1 and 2.

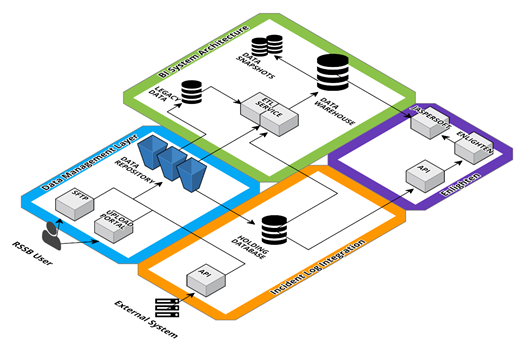
All of the four elements shown in Figure 1are hosted on an Amazon Web Services cloud. Enlighten is a COTS (Commercial Off the Shelf) product, which incorporates the Enlighten Safety Management System (document management and action tracking). The Enlighten module within the Enlighten product is accessed via a web browser (Phase 1) or an Enlighten mobile app (Phase 2). The Enlighten database has been extended to include direct import of some third-party safety-related data (not shown in Figure 1).

The Jaspersoft business intelligence module within the Enlighten product is accessed via a Jaspersoft app. The Enlighten COTS product is being upgraded for RSSB to allow the use of smart forms for event entry.

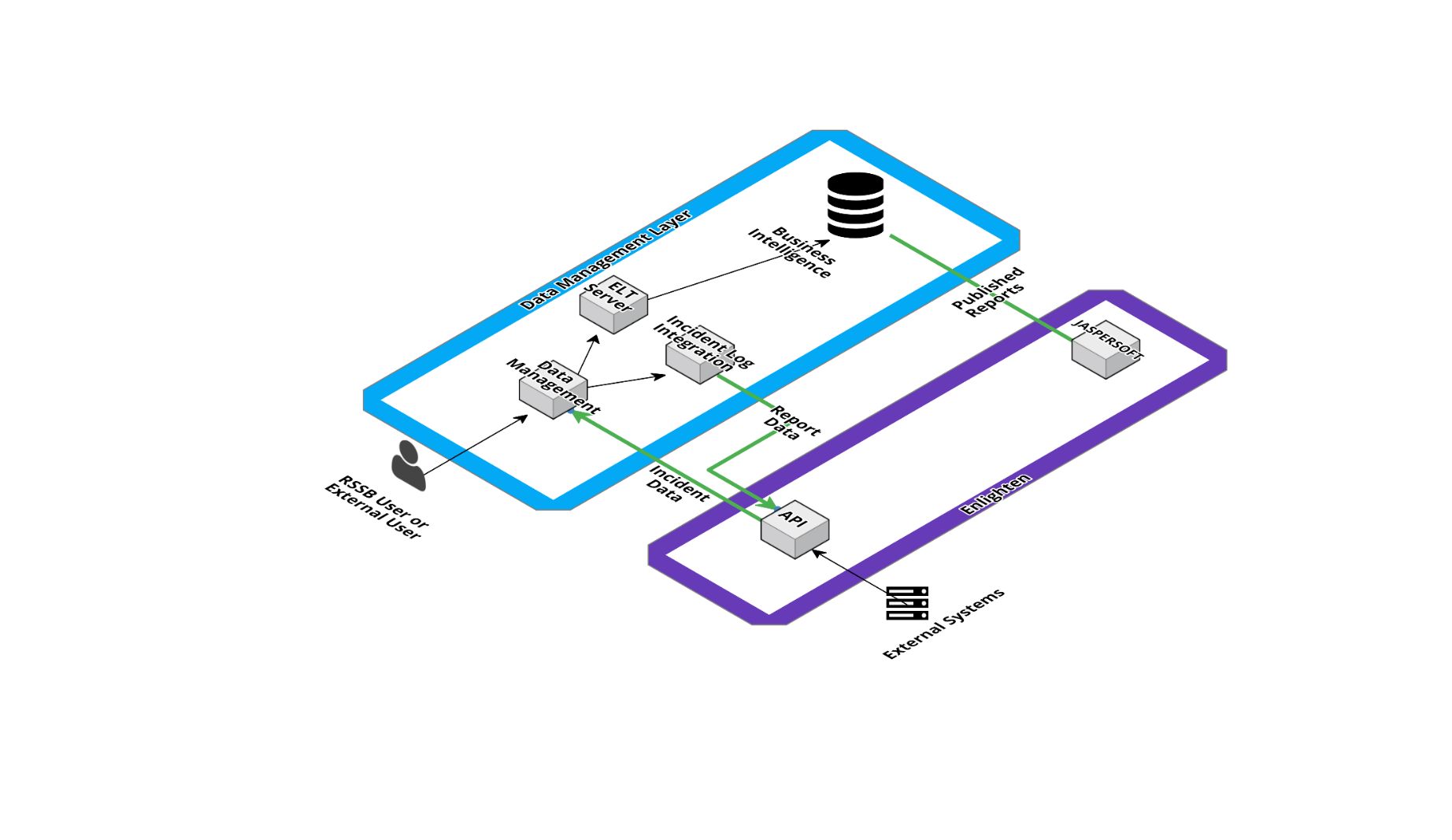
The Enlighten architecture also includes three other areas, based on development and management of databases. These have been custom developed for RSSB, including user interfaces, and are known as the Data Management Layer (DML) They are hosted on a separate AWS account to Enlighten, known as the RSSB DML AWS. The Jaspersoft business intelligence software is hosted within the Enlighten AWS, but managed as part of the DML architecture within SMIS.

Figure 2 presents an updated status on the implementation of third party data import, which is now entering through Enlighten rather than the DML.

Due to the agile software development process being followed, the system architecture and implementation of the SMIS functional specification for Phase 1 launch Q1 2017, and Phase 2 launch, later in 2017, continues to evolve. System architecture updates will be provided at the start of the contract, and prior to the two workshops. Updates on the schedule for development and deployment will be provided as appropriate.

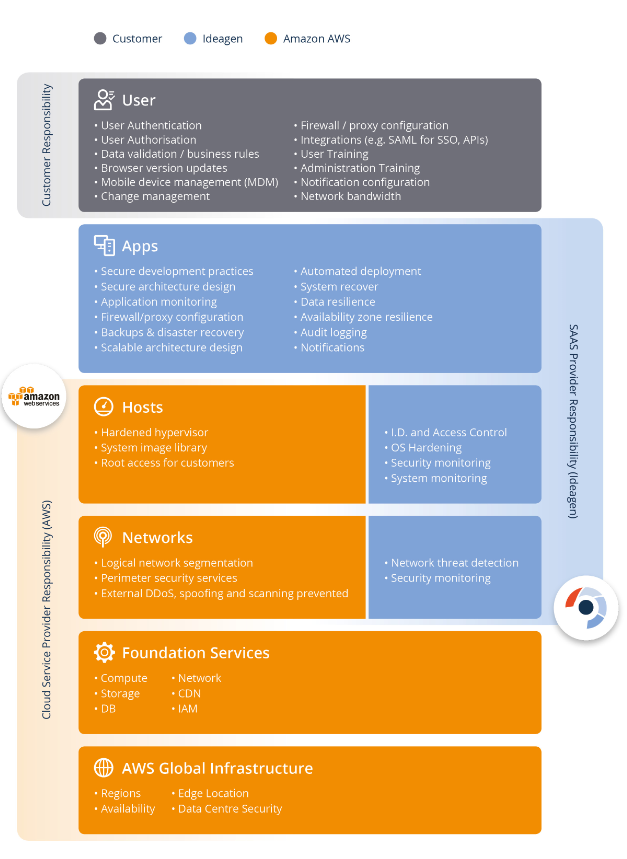


**Figure 1: SMIS+ System Architecture (superseded, awaiting updated drawing)**



**Figure 2: SMIS System Architecture (Data Management Layer) (draft awaiting review and update)**

The (cyber) security responsibilities of the parties involved in the SMIS (for the Enlighten application) are defined in Figure 3. A separate set of security responsibilities for the DML is under development.



**Figure 3: Cyber security responsibilities for Enlighten element of SMIS (draft, under revision)**

1.2 Contact and RSSB Overview

**RSSB REPRESENTATIVE**

Your main point of contact is: **Gemma Cuthbert**

**gemma.cuthbert@rssb.co.uk**

Should you have any queries please email the Representative detailed above.

No approach should be made to any other person in connection with this document unless directed by the above.

1.3 RSSB OVERVIEW

We help the industry understand risk, guide standards, manage research, development and innovation and collaborate to improve.

The rail industry in Britain is made up of many different organisations, but they all form a system and share a common purpose, to move people and freight safely and efficiently by rail. RSSB bring all parts of this system together to support shared decisions, products and services, to help industry drive out unnecessary cost, improve business performance and develop long-term strategy.

Our activities involve:

* **Understanding risk** – Using safety intelligence from across the rail industry and elsewhere with the latest risk modelling to inform members and support safe decision making.
* **Guiding standards** – Creating, reviewing and simplifying GB standards to align with European requirements; managing the Rule Book and making it easier for the railway to deliver efficiently and safely.
* **Managing research, development and innovation** – Undertaking, commissioning and managing research and innovation programmes to address current needs, provide knowledge for decision making now and for the future, and promoting step changes to deliver the Rail Technical Strategy.
* **Collaborating to improve** – As an independent cross-industry body with a critical mass of technical expertise, supporting activities which require collaboration. These range from supplier assurance schemes (RISQS, RISAS) to confidential reporting (CIRAS), from health and wellbeing strategies to sustainability principles.

We are run by the industry, for the industry, with member companies from across the mainline system. The demand for our services comes from the industry itself, and from the involvement of cross-industry groups. For more information go to [www.rssb.co.uk](http://www.rssb.co.uk)

**BEST OVERALL VALUE**

RSSB’s policy is to select suppliers that offer the best overall value for itself and its Members. Price is only one component of overall value. Other factors considered include: the management, strength of the company; ability to control costs; emphasis on providing a quality service; technical capabilities and abilities.

1.4 RESPONSE INSTRUCTIONS

|  |  |
| --- | --- |
| Quotations to be submitted based on the specification: | Detailed in Section 2 |
| Quotation Closing Date: | No later than 09.00hrs  30th January 2017 |
| Response: | Please provide 4 separate files:   * Response to quality question 1 * Response to quality question 2 * Response to quality question 3 * Response to quality question 4 * Appendix B Pricing Schedule |
| Quotations: | To be sent by email to the RSSB Representative. |
| Please ensure you quote the RSSB reference number and title detailed on page 1 | |

* 1. PROCESS AND PREPARATION OF RESPONSES
     1. The Supplier shall not enter in any agreement or arrangement with any third party which would in any way cause RSSB or its members to incur any financial obligations to the Supplier or any third party.
     2. The Supplier shall not approach any RSSB employee, its Representative or its agents to discuss any aspects of the Quote. All communication should be conducted via the RSSB Representative detailed above.
     3. The Supplier shall not canvass support for the award of the contract by approaching any employee of RSSB, its Representative or its agents.
     4. The documents enclosed are to be accepted in their entirety. No alteration will be allowed, unless notified and confirmed in writing by RSSB’s Representative before the date stated for the receipt of quotes. If any alteration is made or these instructions to Suppliers are not fully complied with the quote may be invalidated.
     5. The conditions of contract included in this Invitation to Quote apply. The Suppliers standard terms of business or trade will not be accepted.
     6. Any requested changes to the conditions of contract must be detailed on the Contract Issues Memo document included for consideration. If this is not completed, it is assumed that the Supplier has accepted all terms and conditions detailed and no further changes will be accepted.
     7. The Supplier shall be deemed to have satisfied itself as to the nature, extent and the content of the goods, services or works to be provided, the extent of staff required and all other matters, which may affect the quote.
     8. All prices quoted to be GBP (unless otherwise requested in the Invitation to Quote) exclusive Value Added Tax and firm.
     9. It is the Suppliers responsibility to ensure the Quote is correct at the time of submission. No amendment to the Quote will be allowed after the due date.
     10. Any questions must be emailed to the main point of contact no less than five days before the return date. Note: questions/responses will be circulated anonymously to all Suppliers invited to quote.
     11. Quotes received after the closing date and time will not be considered.
     12. RSSB’s Representative reserves the right to correct any omissions or inaccuracies in the Invitation to Quote and to clarify and/or amend any requirements, up to seven days before the return of quotes.
     13. All information supplied by RSSB must be treated in confidence and not disclosed to third parties except insofar as this is necessary to obtain sureties or quotations required during the preparation of the Quotation. All information provided by Suppliers will be treated in confidence except in stances where references may be sought.

1.6 PRICE QUOTATION

1.6.1 Please complete the Appendix B Pricing Schedule.

1.6.2 The RSSB has a target value of £10,000.00 for the Services. The lowest price shall receive full marks (maximum of 15%) and an offer of the target value shall receive no marks (0%) the rest of the offers shall be evaluated pro rata:

Score = Lowest Tender Price x Available Marks (15%)

Tender Price

1.6.3 Day rates for any further work make up 5% of the scored price. Cell highlighted blue are worth 1.5% and cells highlighted yellow are worth 0.66%. For each rate the lowest price shall receive full marks and the rest of the offers shall be evaluated pro rata:

Score = Lowest Tender Price x Available Marks (1.5% or 0.66%)

Tender Price

1.6.4 All prices quoted are to be in sterling, exclusive of Value Added Tax and must be firm.

1.6.5 A full and comprehensive breakdown of all costs and expenses to provide the goods, services or works requested in this invitation to tender must be provided and all assumptions must be clearly stated.

1.6.6 Failure to provide adequate detail may cause your tender to be judged non-compliant. This shall include for the Services under items 1-7 of the scope:

1. A breakdown by grade and named individual, indicating the number of days to be worked on each task and the daily rate to be charged.
2. A list of sub-contracts with prices and copies of quotations where available (a similar breakdown by grade, named individuals and rates, as above, is required where the sub-contract is for manpower).
3. Details of any other costs, such as hire charges for equipment.
4. Details of travel and subsistence and all expenses to be incurred.
5. The above breakdowns should be further broken down into individual work packages.
   1. PAYMENT SCHEDULE

1.7.1 Payment shall be on completion and acceptance by the RSSB project manager of all deliverables. This is the same for the initial piece of work (items 1-7 of the scope) and any future call off requirements.

2.0 SPECIFICATION

As part of the preparation of the Safety Case, two workshops will be led by RSSB with Ideagen, the suppliers of the SMIS Software as a Service (SaaS) system, in order to review the high-level system architecture, and threats, consequences and controls (as reported in a bowtie format). These workshops will build on the existing security workshops held Q3/Q4 2016 and subsequent changes to the system architecture and documentation (ongoing through to Q1 2017), and the System Safety Case v1.0 (issued 30th November 2016). The high-level system architecture for these workshops will be defined at contract signature, it is anticipated that they will include some aspect of mobile deployment of SMIS, and also the incorporation of new functionality (based on Close Call Reporting) which will incorporate a significant expansion in the user base.

Previous work and documentation will be made available to the successful supplier further to contract award. However, if you feel you need any contextual information prior to providing your tender please contact the procurement lead.

Prior to these two workshops, a Q1 2017 technical review is required of the Phase 1 suite of security documentation (incorporating the ISMS, the Security Management Plan and the supporting documentation, including bowties and summary of risk controls). This technical review will include the results of external pentesting of SMIS, along with the evidence of implementation of remedial actions. The output of the review will be used as input to the SSC, as presented to the SMIS PB for signature. It may include recommendations for further actions to be taken prior to Phase 1 “go live”.

The purpose of the System Safety Case is to demonstrate that the Material Safety Uses (MSU) of SMIS, which is a safety-related system, will be delivered by the SMIS system. An MSU is one where it is plausible that a malfunction in SMIS could, taking account of controls in the surrounding business processes, lead to a safety incident (or to a safety incident not being prevented.

The workshops will not form part of assurance of the ISMS against the ISO27K standards (process and product) nor a review of the software design and implementation against cyber security good industry principles.

|  |  |  |
| --- | --- | --- |
| No. | Requirement | Timescales |
| 1 | Attend a kick off meeting with RSSB who shall brief the supplier on the design, functionality and scope of the SMIS System, and provide the documentation reference pack as input to the technical review (item 2). Documentation includes ISO27001 ISMS, Security Management Plan (SMP), Bowties and supporting documentation), as well as output from Contract no. RSSB 2285 (previous workshops) and answer any clarification questions that the supplier may have at this stage.  This may be held by telephone. | 2nd or 3rd Feb 2017 exact date to be confirmed following contract award |
| 2 | Carry out a technical review on the documentation provided in step 1, the purpose of this is to identify whether the arrangements that have been put in place are fit for purpose and whether any additional arrangements need to be put in place prior to go live.  Provide a report in letter format on the ISO27001 ISMS, Security Management Plan (SMP), Bowties and supporting documentation as prepared, including pentesting results, and actions taken in response to security workshops and pentesting - for presentation to the SMIS PB 10th February, and inclusion in the SSC as approved for Q1 2017 go live.  Be available for telephone consultation on the 10th February, as required | By 9th February 2017 (this is the earliest deadline and the one that we are currently working towards. Dates may change as a result of changes to the programme but in any case, will not be earlier than the 9th) |
| 3 | Prepare the first workshop terms of reference (including reviewing documentation input to the workshop) for Phase 2 and identify topics for discussion. Scope may include:   * Extended business intelligence functionality for Phase 2 deployment * Extended import of third party data into SMIS * Deployment of mobile application (preliminary or finalised) * *(will probably think of others as we talk)* | March 2017, date to be confirmed following contract award |
| 4 | Attend and chair the first workshop (one day duration). A scribe will be provided by RSSB. | March 2017 |
| 5 | Review the workshop outputs. Clarifications shall be sought from RSSB and/or the supplier of SMIS where required. | Workshop undertaken March 2016  Outputs written up and made available to the supplier April 2017 |
| 6 | Provide a report in letter format, commenting on all aspects of:   * inputs to the workshop * process used to undertake the workshop * outputs and clarifications obtained as a result of the workshop   The report shall use expert judgment to assess whether the information and processes were sound, identify key risks and dependencies, and where further clarification or investigation may be required. | By end of April 2017 |
| 7 | A second workshop will be held on outstanding technical items, following steps 3-6.  The scope of the workshop will be clarified as the schedule for development and deployment for SMIS is defined and agreed. | June 2017, date to be confirmed after workshop 1. |
| 8 | Provide third party review on specialist topics including:   * pentest scope, results and implementation of actions (both internal and external) * scope and adequacy of RSSB SSC, updated versions as appropriate * system architecture and supporting documentation * scope and implementation of third party audits, against RSSB’s requirements, including against ISO27001/2, industry guidance and other user requirements as appropriate.   These activities are optional, and further details on scope and timing will be provided as required during the contract duration. | As and when required throughout the contract duration. (initial term 01/02/17 – 31/01/18 with the option to extend for a further year) |
| 9 | Provide third party review and technical guidance on security measures associated with operational software  These activities are optional, and further details on scope and timing will be provided as required during the contract duration. | As and when required throughout the contract duration. (initial term 01/02/17 – 31/01/18 with the option to extend for a further year) The work shall be |

3.0 EVALUATION CRITERIA

Evaluation is based on a split between Quality and Price expressed as 80% Quality and 20% Price

A score below one (1) for any quality question will constitute a failure to evidence suitability (against the requirement of the procurement) and will automatically disqualify the Supplier.

|  |  |  |  |
| --- | --- | --- | --- |
| **Evaluation Criteria - Quality** | | **Maximum Score** | **% Weighting (80%)** |
| **Q1** | Please list your organisation’s certifications (including those linked to ISO9001, ISO27001) and your experience in applying relevant risk assessment standards, including ISO27005, through provision of 2 case studies of a suitably similar nature to RSSB’s requirement.  The response shall give RSSB full confidence in the quality of the supplier’s organisation and assurance in the suitability of their experience.  Max page limit 6 sides A4 | **3** | **15** |
| **Q2** | Please also provide the CV of the individual(s) being proposed to undertake this work. The CV shall demonstrate their experience of providing cyber security services (paid consultancy or informal guidance) with the organisations such as CESG/CPNI, ISO, CIS, ETSI, AWS, BSI, or other suitably similar organisations.  The CV(s) shall give RSSB full confidence in the ability, suitability and experience of the named induvial(s) to deliver the requirements set out in items 1-7 of the scope effectively.  Max page limit 2 sides A4 per CV | **3** | **30** |
| **Q3** | Please provide information on your organisation’s technical competency and experience with the security responsibilities listed in Figure 3, with a focus on cloud-based services. Please provide information for both cloud-based services and client-based applications external to the cloud.  As part of your response, please provide information on up to three recent case studies which highlight your organisation’s technical competency and experience. At least one of the case studies should include your experience with mobile device deployment and significant increases in user deployment numbers.  The response shall give RSSB full confidence in the supplier’s ability to effectively execute these types of services.  Max page limit 6 sides A4 | **3** | **25** |
| **Q4** | Please detail what other technical services outside the scope of items 1-7 that you would be able to provide during the contract should the need arise. The response should demonstrate expertise and capability that would cover the services listed in items 8 & 9 of the scope.  Please support this answer at least one example of your experience in providing these services outside of the rail sector, where your expert judgement is that best practice in those sectors could be usefully deployed by RSSB. Please provide rationale for this assessment.  The response shall demonstrate to RSSB that the supplier has a wide range of skill and technical ability, cross industry knowledge of best practice and can apply these principles effectively and recognise opportunity for improvement.  Max page limit 2 sides A4 | **4** | **10** |
| **Evaluation Criteria – Price** | |  | **% Weighting (20%)** |
| Firm price for essential requirements in 1-7 | |  | 15% |
| Day rates for any additional work | |  | 5% |

Scoring Methodology

|  |  |  |
| --- | --- | --- |
| **Grade label** | **Grade** | **Definition of grade** |
| Unacceptable | 0 | The response has been omitted, or the Tenderer proposal evidences inadequate (or insufficient) capacity or capability to deliver the requirement(s) |
| Weak | 1 | The Tenderer has demonstrated merit, although there is weakness evident in its capacity or capability for the purposes of the procurement. |
| Satisfactory | 2 | The Tenderer has evidenced a level of capacity and capability suitable for the purposes of the procurement. |
| Good | 3 | The Tenderer has evidenced a significant level of capability and capacity for the purposes of the procurement. |

4.0 Conditions of Contract

All goods and services provided by third parties to RSSB are governed under our terms and conditions. See Appendix A.

The initial piece of work shall be undertaken to the timescales set out in section 2. However, the contract shall be for 1 year with the option to extend by a further year giving the supplier 1 months’ notice, to accommodate any ad-hoc work that is identified during this time.

Whilst the initial piece of work (items 1- 7 of the scope) is guaranteed this contract shall not oblige RSSB to commission any further services under the contract if not required and RSSB reserves the right to negotiate or award a contract for any further similar services to any other supplier in any geographical area.

The contract will have a cap of £30,000.00 per year which shall not be exceeded without a written variation approved by RSSB procurement.

Following the initial piece of work should any further work be identified RSSB and the supplier shall follow this commission procedure:

|  |  |  |
| --- | --- | --- |
| 1 | RSSB shall email the supplier a detailed scope of works including timescales and sign off points. |  |
| 2 | The supplier shall respond confirming availability and providing a clearly priced resource schedule in line with the day rates contained in the contract and submitted as part of their tender response.  To ensure that orders over the course of each contract year do not exceed the yearly cap shall include any cumulative spend to date in the email. | Within 2 working days of receiving the order. |
| 3 | To only accept the order as binding when a confirmation email is received attaching a purchase order. |  |