Annex A - Requirements

This document accompanies the Invitation to Tender (ITT) for a Safeguards Information Management and Reporting System (SIMRS). The SIMRS will store, manage and report information relating to the support of UK and international nuclear material accountancy and safeguards obligations. The SIMRS will be required to receive reports from locations around the UK and then perform validation and verification activities on these reports to ensure their correctness and completeness. The information held in the reports will then be stored to allow the quantities of different categories of nuclear material held within UK accountancy areas to be determined at any time. SIMRS will also be required to translate reports received from within the UK into a different defined format for submission to the International Atomic Energy Agency (IAEA) in order for the UK to meet its international nuclear material accountancy and safeguards commitments. While the accountancy and reporting aspects of the SIMRS are mandatory, it is desirable for the SIMRS to also be able to support Safeguards inspectors in undertaking inspections/verifications and as an asset registry. This ITT relates to the design and delivery of a SIMRS achieving all mandatory requirements, as well as an initial 2 year maintenance and support period, during which time ongoing development can take place in order to achieve any remaining desirable requirements.

This Annex details non-functional and functional requirements for the system, along with associated priorities. While much effort was spent to make this requirements list as accurate as possible, it should be considered as a draft that would be developed further with the selected Tenderer, and as such, the Office for Nuclear Regulation (ONR) reserve the right to amend or make changes to the requirements currently listed. Equally should Tender applicants have any questions regarding these, please send them to the Tender Response Contact as outlined in the ITT.

The non-functional requirements of SIMRS are captured in Table 1. The functional Requirements are in Table 2. In these tables the first column contains the requirement and its unique reference number. The second column contains explanatory text and notes to aid in understanding what the requirement means. The third column contains a priority, utilising the following code:

M – Mandatory requirement. This function, feature or capability is essential to the success of the system. These requirements represent the Minimum Viable Product (MVP) and are identified with the term “must”. The SIMRS must have achieve these by the end of December 2018.

D – Desirable requirement. This function, feature or capability should be built into the system unless extenuating circumstances are agreed upon with the ONR as to why it cannot be. These are a lower priority than M and are identified with the term “should”. It is possible that the SIMRS does not need to meet these requirements by the end of December 2018, however these must be achieved within the initial 2 year maintenance and support period.

As mentioned in the ITT, tender responses are encouraged to submit two prices as follows:

1. The cost to implement a SIMRS that meets all Mandatory requirements by the end of December 2018 and all Desirable requirements within the following 2 year period.
2. The cost to implement a SIMRS that meets all Mandatory and Desirable requirements by the end of December 2018.

Table 1. Non-Functional Requirements for the SIMRS

#	Requirement	Explanatory Text	Priority
NF1	The system source code must be submitted to an Escrow agreement.	This agreement will ensure ONR access to any developed source code.	M
NF2	The solution proposed must include an initial 2 year maintenance and support programme, with the option to extend for 2 years in single year increments.	This maintenance and support programme should be sufficient to meet requirements NF25-NF27. Also for solutions where the Desirable requirements are not to be met before December 2018, this should include achieving those requirements within those 2 years.	M
NF3	The system must be provided along with training capable of educating users on how to use the system.	Training will be required for selected members of ONR, estimates being approximately 20 users. It is expected that staff should be able to use the majority of SIMRS functions having undergone the training.	M
NF4	The system must be provided along with user training guide documentation.	The SIMRS must have included within it user training guide documentation. It is expected that sufficient information be included in these that new users could establish a basic understanding of how to use the SIMRS.	M
NF5	The system must be provided along with system documentation.	This system documentation should detail to a sufficient level how the SIMRS is coded/operates.	M
NF6	During development, the successful applicant must design and build the SIMRS using their own IT hardware (eg. Laptop or server).	Development should take place on developer hardware. During the discovery phase of the project dates for movement to the final platform will be discussed.	M
NF7	Individuals working on this SIMRS project must have SC clearance.	It is believed the SIMRS will hold up to UK OFFICIAL-SENSITIVE information. During the discovery phase of the project the maximum classification will be confirmed.	M
NF8	The system must be able to support 50 concurrent users.	Including ONR staff, inspectors and potentially duty holders.	M
NF9	The system must be accessible through standard IT equipment and infrastructure.	Depending on the proposed solution, any SIMRS that will be accessed from IT hardware should be accessible from computers/laptops using standard software such as internet explorer, firefox, chrome etc.	M
NF10	The system must have ONR branding/colour scheme.	The SIMRS interface must have ONR branding and colour scheme.	M

NF11	The system must be based on currently supported underlying technology, and this must be maintained for the life of the contract.	It is expected that the SIMRS should operate for a number of years, and the hardware/software used should be supported.	M
NF12	The system should align with existing ONR and Safeguards software/processes.	In the Discovery phase of the project a list of ONR and Safeguards existing software will be provided that the SIMRS should ideally align with. Also in the discovery phase the level of interaction/integration will be identified. This could include packages like TRIM, for example.	D
NF13	The system must have capacity to store historic data and the data expected over the next 30 years.	The system is expected to receive (pending Brexit negotiations) an initial bulk transfer of accountancy data from Euratom. Following this data will then be added as the system is used. Estimates of the quantities are as follows: 1) Bulk transfer data from Euratom of approximately 30 Gb, 2) Yearly addition of data to SIMRS of approximately 1 Gb. The SIMRS must therefore be able to store an estimated 60 Gb of data. In the Discovery phase of the project these estimates will be refined and suppliers are encouraged to investigate methods to ensure performance whilst retaining this quantity of data.	M
NF14	The system must be able to store data for a time period in excess of 30 years.	The SIMRS must be able to store the identified data for 30+ years. The type of storage media and storage arrangements must be selected appropriately.	M
NF15	The system must adhere to Government standards for storage of SNI up to OFFICIAL-SENSITIVE.	The data within the SIMRS will include Special Nuclear Information (SNI) up to UK OFFICIAL-SENSITIVE and must be protected as such. Further details can be found in Annex C. This includes government classification markings.	M
NF16	The system must hold all of its data within the UK.	Cloud based solutions, server based solutions and any back-up solutions must ensure that the data is stored within the UK. The only exception to this is when reports are transmitted to the IAEA or other states outside of the UK.	M
NF17	The system must have functionality to control access to authorised users only.	The SIMRS itself, and therefore the data within it, must only be accessible by authorised users.	M
NF18	The system must only allow permitted functionality to authorised users.	Additionally to access, functionality must be limited to authorised users.	M

NF19	The system should maintain a security log.	The SIMRS should identify wherever possible repeat attempts to subvert any security features in place. This includes repeated failures to “log-in”, attempts to perform functionality not permitted for that user etc. Changes made to authorised users lists, levels of access and levels of functionality should also be captured.	D
NF20	The system should include features to aid in resilience to cyber threats.	Security functions should be included where practicable to increase resilience to cyber threats. The supplier is expected to be ISO 27001 certified, or able to demonstrate previous delivery of systems that are secure. https://www.itgovernance.co.uk/iso27001	D
NF21	The system must have functionality for at least 3 ONR Safeguards administrator users.	In the Discovery phase of the project a list of administrators, authorised users, likely to be grouped into user groups, will be discussed and levels of access/functionality to be specified.	M
NF22	The system must have functionality for administrators to amend approved users and identified user lists.	These administrator users would be ONR personnel and have functionality such as that in NF17. Also see Requirement NF21.	M
NF23	The system must be capable of regularly backing up all of its data.	The regularity of the back-ups will depend on the technology solution, however estimates indicate that the SIMRS will have information added/edited at least once a day. Therefore performing back-ups daily is likely.	M
NF24	The system should be capable of backing-up data to two appropriately maintained geographically separate locations in the UK.	If physical servers/storage are to be used for the backups rather than a cloud-based solution, then the ONR would require two geographically separate back-ups facilities within the UK. It is a possibility that these can be at existing ONR sites, although alternatives to this are encouraged. The back-up sites would require UPS/air conditioning/security etc as appropriate. If a cloud-based solution is proposed the back-up needs can be discussed.	D
NF25	The system must be designed such that any foreseeable failure would not cause irretrievable loss of data.	The project will identify, based upon the solution proposed, a set of foreseeable failure mechanisms. The SIMRS should be designed to mitigate these risks to the point where no foreseeable outcome would be result in irretrievable loss of data.	M

NF26	The system must be operational to end users during standard operation for no less than 95% in a year.	Taking into account standard maintenance it is required that the SIMRS be operational to users 95% of them time. This relates to approximately 8 hours a week, or over a year approximately 18 days of unavailability. This time could be used for required maintenance, processing of data etc. In the discovery phase of the project availability during report submission periods will be discussed in detail.	M
NF27	The system must have functionality to be returned to an operational state within 48 hours of a failure, and should lose no more than 24 hours worth of received data.	Should a fault or failure occur, the system (and subsequent support and maintenance plan) must permit the system to be operational within 48 hours. Addition of data to the SIMRS could potentially occur daily, thus a system that would not lose more than 24 hours worth of submitted data is required.	M
NF28	The system should minimise the use of licensed or proprietary software.	The SIMRS solution should limit the use of proprietary software where possible. This is to avoid additional licensing costs, intellectual property issues or ongoing maintenance concerns. Open-source and free licence solutions are preferred.	D
NF29	The system should require a minimal amount of maintenance.	Any maintenance required by the system should be minimal, ideally with any maintenance required to be undertaken at “quiet hours” for the system so as to not interfere with ongoing operations.	D
NF30	The system must be capable of being hosted on cloud-based or local server-based platforms.	At present the ONR are undertaking a large-scale IT infrastructure project that will likely result in replacement of the existing system. The details of the technology to be used in this replacement have not yet been specified. Therefore the SIMRS should ideally be flexible enough to work on a cloud-based system, a server-based system etc.	M
NF31	The system must be capable of being migrated to alternative data centres or platforms.	As NF30, the system must be capable of being migrated between data centres or platforms.	M
NF32	The system must meet international obligations by the end of December 2018, for parallel running starting on the 1st January.	Parallel running against the existing Euratom system will commence on 1st January. In the Discovery phase of the project the exact details for how this parallel running will work will be identified.	M

NF33	The system must be able to support FOI requests and adhere to Data Protection laws and policy.	These will be clarified in the discovery phase.	M
NF34	The development of the system should follow the Government Digital Service (GDS) process and meet the Digital Service Standard.	It is desirable that the delivery of the SIMRS follows the GDS guidelines and standards. More information on these can be found here: https://www.gov.uk/service-manual	D

Table 2. Functional Requirements for the SIMRS

#	Requirement	Explanatory Text	Priority
F1	The system must be accessible by personnel at all three of the ONR office locations.	The ONR office locations are: Bootle (Redgrave Court, Merton Road, Bootle, L20 7HS), London (Rose Court, 2 Southwark Bridge, London, SE1 9HS) and Cheltenham (St James House, St James Square, Cheltenham, Gloucestershire, GL50 3PR).	M
F2	The system should be accessible by personnel at other locations within the UK.	Such as at duty holder locations.	D
F3	The system must have functionality to import/read-in duty holder submitted data.	Currently duty holders send submitted data to Euratom by means of an encrypted e-mail. When ONR takes over this function the SIMRS must be able to import/read-in this submitted data once it has been decrypted by ONR staff. See requirement F5 regarding the SIMRS performing this decryption process.	M
F4	The system should have functionality for duty holders to submit information into the SIMRS.	In future it is desirable for duty holders to potentially have access to the SIMRS directly and be able to submit data directly.	D
F5	The system should include functionality to streamline the input of duty holder submitted data into the SIMRS.	The current arrangements regarding duty holder submissions focuses on encrypted e-mails to a Euratom account. Whereas Requirement 3 specifies the SIMRS must be able to import/read-in this information once decrypted – this relies on a manual decryption process to be performed by an ONR inspector. It is desirable in future for the SIMRS to streamline this process and be capable of receiving the encrypted e-mail, de-crypting it and importing the data directly. The current encryption method used by all-but-one duty holder, the ONR safeguards team and Euratom is Zed. https://www.zedencrypt.com/encryption-data-protection One duty holder uses PGP encryption.	D

F6	The system must enable approved users to input accountancy information.	Some users must have the ability to input accountancy information. All inputs must be captured in the change log. While users must never be able to edit duty holder submitted information, it is likely that the records holding duty holder submission information might have “notes” or “comments” fields that ONR may wish to input text into, for example.	M
F7	The system must enable approved users to add/update report templates.	Some users must have the ability to input/edit reporting templates. Additions and changes to templates must be captured in the change log.	M
F8	The system must include functionality to perform completeness checks on user submitted data.	These completeness checks will be identified in the discovery phase of the project. They focus on ensuring that duty holders have included all required fields when submitting information to the SIMRS/ONR, that the information has the correct syntax and any other mistakes/oversights that could be identified upon data submission. The discovery phase of the project will identify a set list of checks to be performed.	M
F9	The system must include functionality to perform validation checks on submitted and stored information.	These validation checks will be identified in the discovery phase of the project. They focus on ensuring that the information submitted by duty holders and information held within the SIMRS is accurate, identifying any inconsistencies or anomalies. An example validation test on submitted information would be that a material balance area only allowed to hold Uranium has received a shipment of Plutonium. An example validation test on stored information would be a check to show that the same amount and type of material that has left one material balance area has arrived in another with the same information. The discovery phase of the project will identify a set list of checks to be performed and expected values for duty holders/specific material balance areas.	M
F10	The system should include functionality to undertake completeness and validation checks automatically.	As many checks as possible should be automated, to reduce the amount of inspector time taken.	D
F11	The system should enable approved users to add/edit equipment, timetable and other stored information.	Approved users should be able to edit this information, with changes being tracked in the change log (req 3.1).	D

F12	The system must have functionality to produce reports meeting the IAEA Code 10 reporting.	Code 10 compliant reports are an essential output of the SIMRS. Information submitted by duty holders must be translated into an IAEA code 10 format and a report generated. Examples of reporting templates and associated .XML schemas will be provided during the discovery phase of the project. It should be noted that currently XML format is used by Euratom to submit to IAEA. Further reading is available here: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32006H0040 https://www.iaea.org/sites/default/files/sg-fm-1170-subsidiary-arrangement-code-10-fixed.pdf	M
F13	The system should have functionality to send reports to the IAEA.	At present reports are sent by Euratom to the IAEA by encrypted e-mails (using PGP). In the discovery phase of the project agreement will be sought with the IAEA to determine whether the ONR shall continue by this means or whether submissions by another means are desired.	D
F14	The system must have functionality to produce custom reports.	An option to produce additional report templates or to create reports containing user-selected data is required.	M
F15	The system must use consistent nomenclature to that used by EURATOM/IAEA.	In the discovery phase of the project the nomenclature to be used will be established and the SIMRS must align with this.	M
F16	The system must be able to translate information received in Euratom 302/2005 format/nomenclature into IAEA Code 10 format/nomenclature.	Euratom and IAEA use variants of nomenclature. In the Discovery phase of the project the translation between the two will be established and the SIMRS must be able to implement this. In particular in taking stored information and translating it into IAEA nomenclature prior to Code 10 reports being generated.	M
F17	The system must allow for human-checking and approval of reports prior to them being submitted to the IAEA.	While it may be beneficial for the SIMRS to submit code 10 compliant reports automatically on these dates, there must be a robust human-check and approval process in place.	M
F18	The system should be able to produce reports in a variety of formats (eg. PDF, XML etc.)	It is desirable that the SIMRS can produce reports in a variety of formats, such as XML, PDF and potentially others. These will be identified in the discovery phase of the project.	D

F19	The system must be able to submit data to the IAEA by aligning with their new State Declaration Portal.	In the discovery phase of the project it will be agreed with the IAEA whether future alignment to the SDP is required. If it is, then it is essential that the SIMRS includes functionality to submit reports via that route. Otherwise, this may become a desirable requirement.	M
F20	The system should store information about UK material balance areas, including basic technical characteristics, particular safeguards provisions and facility attachments.	There are approximately 180 material balance areas at sites within the UK. Each has basic technical characteristics (BTC) as well as other information. It is desirable to store this information within SIMRS. In the Discovery phase of the project this information will be identified and collated, ready for entry into SIMRS.	D
F21	The system must store nuclear material accountancy information for the UK material balance areas.	The primary purpose of the SIMRS is to store nuclear material accountancy information. This includes up-to-date quantities of the different categories of nuclear materials in all material balance areas within the UK as well as records for changes/transfers to inventories. This information will be provided via the duty holder submissions, therefore the SIMRS should receive, process and store that information to form accurate accounting. This includes a readily accessible current book balance per material category for each material balance area and the UK as a whole.	M
F22	The system must store a protected copy of all duty holder submissions.	It is essential that original copies of duty holder submissions are retained.	M
F23	The system must include a change log for all added/stored information.	A change log must be kept in order to record addition, processing and amendment of all information within the SIMRS. This must include information such as date, time, author and other relevant metadata to be realised in the discovery stages of the project.	M
F24	The system must include a robust change control process, ensuring no information is ever lost/deleted.	A change control process must be in place to ensure that no “original” information is ever lost/deleted. Whenever changes would be made, the previous version must be kept. Changes must be added to the change log. See Requirement 23.	M

F25	The system must be able to import duty holder data in currently used formats.	The majority of duty holder submitted information is in XML format, however in the Discovery phase of the project the existing formats, current transmission mechanisms and types of submissions from duty holders will be identified and the SIMRS must be able to import from these.	M
F26	The system should be able to store general safeguards files.	It is desirable that the SIMRS should link to the ONR document management system. Since this is currently under review, and potentially to be replaced, the SIMRS should provide a suitable document storage area that can be linked to.	D
F27	The system should be able to store timetable/calendar/planning information.	It is desirable that the SIMRS should store timetabling/calendar information regarding safeguards commitments, such as inspection dates, report due dates and any other information useful to on-site inspections. In the Discovery phase of the project this information shall be defined.	D
F28	The system should be able to store details and information collected as part of undertaken inspections.	It is desirable that SIMRS hold information/reports collected/written during and after inspections. These will again be PDFs, Word files and Excel spreadsheets.	D
F29	The system should be searchable by a variety of means.	Users should be able to search the SIMRS to locate information they need. Such search criteria might be keywords, report numbers, date, author, duty holder, material balance areas etc. In the Discovery phase of the project a list of criteria will be identified.	D
F30	The system should be able to receive, store and submit reports in support of third party Nuclear Cooperation Agreements.	Currently duty holders submit nuclear cooperation agreement information and reports are generated then sent to respective States. It is desirable that in future the SIMRS could be used for this purpose. During the discovery phase of the project the extent of desired nuclear cooperation agreement capability will be identified.	D

F31	The system must have functionality to import migrated existing and historic accounting data provided by Euratom.	Since 1973 (45 years), Euratom have been storing/maintaining the nuclear material accountancy information for the UK and passing reports to the IAEA. As ONR look to take this over, we are seeking to receive a bulk transfer of all historic data from Euratom. Discussions are ongoing regarding the format and quantity of this data, however it is expected this will be known by May 2018. It is possible that the data will be in a variety of formats. The SIMRS must have functionality to accept this bulk data. It should be noted that this data only concerns nuclear material accountancy (ie. No equipment information, schedule information, general safeguards information).	M
F32	The system must store protected copies of all submitted reports to the IAEA.	As reports are generated and sent to the IAEA, protected (cannot be deleted or edited) copies must be kept.	M
F33	The system should store records of notifications sent to identified users.	The SIMRS should be able to store information such as date, time, recipients etc. of notifications.	D
F34	The system should have the functionality to send notifications to personnel.	Similarly to authorised users (See NF23), in the Discovery phase of the project lists of “identified users” and groups of these will be identified. The SIMRS should be able to send notifications to these users/groups.	D
F35	The system should notify identified users when duty holders have submitted information.	As above.	D
F36	The system should notify identified users when IAEA reports are generated/submitted.	As above.	D
F37	The system should notify identified users of relevant deadlines in the timetables.	As above.	D
F38	The system should notify identified users of the results of the completeness checks when they are performed.	As above.	D
F39	The system should notify identified users of the results of the verification checks when they are performed.	As above.	D
F40	The system should have functionality to encrypt data/reports being sent externally of the SIMRS.	In particular encryption may be needed when sending data/reports to the IAEA. In the Discovery phase of the project the encryption needs and methods will be identified.	D