

## Request for Information

### Enterprise Risk Management Software

#### Background

The International Atomic Energy Agency located in Vienna, Austria (hereinafter referred to as the “IAEA” or the “Agency”) is widely known as the world’s “Atoms for Peace and Development” organization within the United Nations (UN) family.

Established in 1957 as the world’s centre for cooperation in the nuclear field, the IAEA works together with its Member States and multiple partners worldwide to promote the safe, secure and peaceful use of nuclear technologies.

Detailed information about the work of the IAEA is available at [www.iaea.org](http://www.iaea.org)

#### 1. Risk Management at the IAEA

The IAEA provides support to its Member States through the implementation of programmatic activities structured in hierarchical levels starting from the delivery level, named “Projects” through “Sub-Programmes” (i.e. a set of Projects within the same subject area), “Programmes” (i.e. a set of Sub-Programmes within the same broader subject areas) up to “Major Programmes” (i.e. a set of Programmes contributing to the achievement of specific high level objectives). The IAEA programmatic structure is revised every two years and is reflected in the IAEA Programme and Budget biennial publications.

#### 2. Identification of a Business Need

Currently, there is no specialised IT system for the management of risks at the IAEA. Risks are managed manually using Microsoft Excel spreadsheets. Tracking all details and modifications in these spreadsheets is complex, time-consuming, and error-prone.

The IAEA is considering deploying an Enterprise Risk Management Software (hereinafter referred as “ERMS”) that would allow users with different programmatic roles and responsibilities (Project Managers, Sub-Programme Managers, Programme Managers and Major Programme Managers) of the IAEA to identify, characterize and assess the impact and likelihood of specific “risks” and identify and assess effectiveness of associated “internal controls”, intended as risk mitigation measures.

Any specific risks logged in the ERMS shall be associated with one of the six (6) main risk categories and one of the forty (40) sub-categories which make up the new Agency-wide risk catalogue. Project managers are expected to log the majority of specific risks. At the level of Sub-Programme and above (Programme and Major Programme), managers are mainly expected to rate risk “sub-categories” as a whole,

based on the project-level specific risks; nonetheless, they may selectively log further specific risks which can only be articulated at their level as well as elevate project-level specific risks to their programmatic level.

This Request for Information (RFI) is targeted towards companies offering on-premises (hereinafter referred to as "on-prem") solutions and/or Software-as-a-Service (SaaS) solutions.

### 3. Request for Information

This Request for Information (RFI) consists of the following parts:

- A. Requested Technical and Functional Information;
- B. Requested Commercial Information (*for budget purposes only*);
- C. Supplementary Information; and
- D. Request for Information Guidelines.

#### A. Requested Technical and Functional Information

The IAEA is interested in receiving the feedback on the following technical and functional requirements:

- 1. Company's/ERMS name;
- 2. Implementation method: on-prem or SaaS;
- 3. Functional capabilities including:
  - a) ERMS should allow the progressive "roll-up" of risk and control assessments in line with the programmatic "layers" adopted by the IAEA – i.e. Projects, Sub-Programmes, Programmes and Major Programmes;
  - b) ERMS should allow to log information based on the following "bottom-up" logic:
    - b.1) Project managers (lowest programmatic layer):
      - i) Identify specific Project risks, link them to a Project outcome and overall output, associate them to a main category and a sub-category of risk and assess the

“inherent” level of risk likelihood/impact (i.e. without considering controls);

- ERMS should allow a drop-down selection of Programme and Budget outcomes and overall outputs at Project level (and at higher programmatic levels);
  - ERMS should allow a drop-down selection of “main” and “sub-categories” of risk (taken from the risk catalogue); if a sub-category is selected the ERMS should identify the related main category automatically.
- ii) Identify all relevant internal controls which are aimed to mitigate each logged risk, characterize them (e.g. ownership, implementation, frequency) and assess their effectiveness and possible need for improvements;
- ERMS should allow a drop-down selection of “control types” based on a standard inventory.
- iii) Considering the overall effectiveness of the internal controls and other risk response measures in reducing the inherent level of risk, assess the “residual” likelihood and impact of the risk on the underlying Project outcome.

#### b.2) Sub-Programme managers

- i) Take stock of the Project-level risk assessment for their Sub-Programme by reviewing, for each risk sub-category, all Project specific risks and related controls logged in by Project managers;
- ERMS should allow a visually user-friendly summary view (map) by risk sub-category of a specified group of Project specific risks and controls.
- ii) Elevate selected Project level risks which create impacts at Sub-Programme level – the ERMS should allow “recalling” all fields that characterize and assess elevated risks and related controls;
- iii) Identify any further Sub-Programme specific risk, link it to (one or multiple) Sub-Programme outcome and overall

output; associate it to a main/sub-category of risk and assess the inherent risk likelihood/impact; identify and characterize internal controls related to each Sub-Programme specific risk; assess residual impact and likelihood of risk (similar system requirements as for b.1);

- iv) Characterize each relevant risk sub-category in the context of their Sub-Programme (e.g., narrative description of recurrent/significant risks, description of response approach adopted) and express an overall assessment of residual likelihood and impact.

### b.3) Programme managers

This level of management performs a similar type of risk and control assessment tasks of the Sub-Programme managers. Programme managers base their assessment on sub-categories of risks and only selectively log further specific risks or elevate specific risks identified at lower programmatic layer.

- ERMS should allow a simple and effective visualization of “heat maps” configurable by Programme managers, e.g. – impact/likelihood positioning of each risk sub-category by various Sub-Programmes.

### b.4) Major Programme managers (highest programmatic layer)

This level of management performs a similar type of risk and control assessment tasks of the Programme managers. Major Programme managers base their assessment on sub-categories of risks and only selectively log further specific risks or elevate specific risks identified at lower programmatic layer.

The final output of the risk identification and assessment process is:

- A list of Major Programme specific risks, including those elevated from the lower programmatic layers;
- An overall assessment (e.g., narrative description of recurrent/significant risks, description of response

approach adopted) of the risk sub-categories relevant at Major Programme level (including residual likelihood and impact);

- A consolidated risk heat map at Major Programme level highlighting the top risk sub-categories for further IAEA-wide consolidation (corporate risk).
4. Feasibility to operate the system in multiple “environments” - likely two at the time- corresponding to the consecutive Programme and Budget cycles normally handled by managers at the same time. For example, during the 2020-21 biennium managers will periodically monitor the risk situation and continuously update and assess controls, while at the same time they will need to be able to forecast risks, and related controls, based on the programmatic activities planned for the future biennium 2022-23;
  5. Required content frameworks: ERMS shall include a repository/knowledge base of predefined risks as per common information security standards, primarily ISO 27000 series, to facilitate registration and management of Information Security Management System (ISMS) related risks;
  6. Technical requirements in case of on-prem installation (e.g. hardware, operating system, database, software, etc.);
  7. Technical requirements in case of SaaS installation (e.g. integration of Active Directory, Single Sign-On, integration of monitoring environment, general Application Programming Interface (API) requirements, etc.);
  8. Data exchange (integration) possibilities with Oracle Enterprise Resource Planning;
  9. API functionalities;
  10. Export and import of data from external sources (e.g. Microsoft Excel, Microsoft Structured Query Language (SQL));
  11. Demo access;
  12. Distribution of the ERMS: directly by your company or via business partners?
  13. Implementation of the ERMS: is it performed directly by your company, including customization and configuration, or do your business partners or subcontractors carry out such tasks?
  14. Confirmation that all communication, documentation, software, training, and support is available in the English language; and

## 15. Customer References.

### **B. Requested Commercial Information**

The IAEA is interested in receiving cost estimations for budgeting purposes. In preparing such cost estimations, please consider the following information:

- Approximately 250 IAEA staff should have access to ERMS of which a maximum of 200 concurrent users.

Please provide commercial information in EURO. No figures quoted in this RFI will be carried forward to any potential future solicitations.

Kindly provide the following information:

- a) Licensing structure;
- b) ERMS one-time implementation costs;
- c) ERMS ongoing operational costs (annual);
- d) ERMS one-time implementation and ongoing operational costs for five (5) years;
- e) Availability and scope of technical support function, including a detailed description and related cost. If initial support is provided for free, please specify the timeframe; and
- f) Additional (optional) services (e.g. consultancy fees for on-site or remote assistance).

### **C. Supplementary Information**

The draft of the IAEA Risk Management Reporting is available in the **Annex 1**.

## D. Request for Information Guidelines

### RFI closing Date and Time

Please submit your company's response to this RFI by **22 November 2019 17:00HRS CET, Vienna (Austria)**. Kindly submit your company's response to this RFI by using the provided template (please see **RFI Response Form**).

### IAEA Point of Contact

All correspondence and questions relating to this RFI should be addressed to the following point of contact by email:

Yury Golovkov (Mr)

IAEA Procurement Officer

Email: [y.golovkov@iaea.org](mailto:y.golovkov@iaea.org)

### Company and Product Presentations

Companies participating in this Request for Information may be requested to arrange a general presentation of their company and arrange for a demonstration of their product to the IAEA (e.g. via teleconference, WebEx or on-site) or give the IAEA the opportunity of a trial use of the product. Any company presentations, demonstrations or trials shall be at the company's expense.

### Non-Binding

This is a Request for Information only. This RFI does not constitute a solicitation. At no point shall any exchange of communication be understood to be contractually binding. The IAEA reserves the right to change or cancel the requirement at any time during the RFI.

Submitting a reply to this RFI does not automatically guarantee that your company will be considered for receipt of the solicitation when issued. Any final solicitation for this requirement may not be restricted to suppliers that respond to this RFI.