

## Questions and Answers (Q&A)

*in relation to the Request for Information (RFI)  
to identify and evaluate Enterprise Risk Management Software*

| No.  | Question from the Vendor   | Answer from the IAEA Requesting Office/<br>Office of Procurement Services  |
|--|--|--|
| Q&A no. 1. Date of release: 13 November 2019 |  |  |
| 1.   | Can you please confirm if IAEA is looking for an off the shelf readymade product? Or are open to consider a customized solution that can be developed based on the functional requirement?   | The IAEA is looking for off-the-shelf readymade product with some degree of customization and configuration to address the functional needs.   |
| 2.   | Are you able to provide the 3 year budget identified for this project?   | No.  |
| 3.   | Is point A5 mandatory? That is, you want a pre-defined database of all ISO27000 risks and controls?  | Yes, A5 is mandatory and the database shall include a repository/knowledge base of predefined risks as per common information security standards, primarily ISO27000.  |
| 4.   | A7 – what do you wish to integrate with?   | The IAEA will integrate the ERM into the following, not concluding, list: Active Directory, ADFS, WebSSO, AIPS ERP, integration of monitoring environment, etc.  |
| 5.   | A9 – is the need for a system to have API's mandatory?   | Yes, we prefer a system with API functionality.  |
| 6.   | A10 – are you looking to import data from excel or other sources as a one off as part of the implementation or to have this facility available as a general function? This would potentially | We are looking for the feature to import data (e.g. the programmatic structure, organizational structure, etc.) from Excel or other sources whenever necessary (a couple of time per year). Users will not use |

|  |   |  |
|--|---|--|
|  | mean that users are still using excel spreadsheets to collect data which is then uploaded into the ERM?   | excel spreadsheets to collect data, but they are expected to input data directly in ERM.   |
| 7.   | A – a general question – can you confirm that risks and controls are scored individually and that you don’t wish to aggregate or roll up risk/controls and create an average score for that grouping?   | Specific risks are scored individually at each programmatic level. The logic of “average score” is implemented by scoring the risk-subcategories from sub-programme level upward.  |
| 8.   | Is the AIPS code a text field and where does this number come from? The RISK nr field is the unique risk reference?   | The AIPS code is a text field and comes from the programmatic structure (each project/sub-programme/programme/major programme has its own AIPS code). The risk nr field should be linked to the AIPS code of each specific programmatic level, thus the risk nr is a unique risk reference.  |
| 9.   | Section C – The Risk Management Report example - to confirm, you want a system to capture & store all the risk and control data but you want the report generated from this data to be output into Excel in the format given in the RFI?  | This is correct.   |
| Q&A no. 2. Date of release: 19 November 2019 |   |  |
| 10.  | The RFI states that approximately 250 IAEA staff should have access to ERMS, with a maximum of 200 concurrent users (page 6). Can you provide a break down for the 250 users across the different types/functions they will be performing in the system? We provide flexibility in our user licenses to accommodate the requirements of each organization. Not all users will require the same level of functional or system access (i.e. such as reporting only users) nor will be required to use the system as frequently as others. | Out of the 250 concurrent users, approximately 200 will be project/sub-programme managers; the remaining will be Programme/Major Programme managers and staff from coordination offices. The functions are basically the same for all of them but for the staff of the coordination offices (approximately 10-15 people), i.e. they should be able to assess the risks and identify the controls as well as to generate the reports relevant to their programmatic levels. |

|     |  |   |
|-----|--|---|
| 11. | <p>The RFI also requests customer references. Can you provide further detail about the quantities and types of references requested?</p>   | <p>The IAEA is interested in obtaining at least three customer reference, which illustrates your company’s experience in deploying ERMS of a similar size and scope. If available/possible, please include the following information: i) experience implementing ERMS at the sector of international organizations/non-profit and ii) contact details.</p>  |
| 12. | <ul style="list-style-type: none"> <li>• Ref. RFI, page 3, b.2)ii)</li> </ul> <p>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</p> <p>Please could you clarify the meaning of “recalling” and / or provide an example.</p>  | <p>If a specific risk is elevated from a programmatic level to the one above (for e.g. from project to sub-programme level) all the information related to the risk assessment and related controls input at the lower level (project) should be made available to the manager of the upper level (sub-programme manager) for his/her further assessment (including re-scoring). In practice, the manager of a specific programmatic level could decide to elevate a specific risk identified at a lower programmatic level. He/she should be able to retrieve all the information related to this risk input at the lower programmatic level (assessment and controls) and should be able to confirm/re-assess the risk and confirm/identify new controls at his/her programmatic level.</p> |
| 13. | <ul style="list-style-type: none"> <li>• Ref. RFI, page 6, 15 B</li> </ul> <p>Approximately 250 IAEA staff should have access to ERMS of which a maximum of 200 concurrent users.</p> <p>Will all of these users require access as either Project Managers, Sub-Programme Managers, Programme Managers or Major Programme Managers? Or will some of them require access for other purposes, e.g. to only review reports?</p> | <p>All 250 concurrent users but a very small amount (10-15 people) will require the same kind of project/subprogramme/programme/major programme manager access.</p>   |
| 14. | <p>A.3. b.2) ii) - ERMS should allow “recalling” all fields that characterize and assess elevated risks and related controls – what does this mean?</p>  | <p>See answer to Q.12</p>   |

|     |   |  |
|-----|---|--|
| 15. | A.3. b.2) 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; etc. – can you explain further what is needed here? | The logic for assessing specific risk at any programmatic level is always the same and it is described in detail in the FRI at the project level. In a nutshell, we need to link the risk to one or more programmatic outcome and overall outputs (those that could be impacted by the risk) and identify the risk by main/sub-category. And, of course, we should score the risk in terms of likelihood and impact. |
| 16. | A12 - Distribution of the ERMS – what does this mean?   | Please let us know how does your company sales its ERMS? Direct sales or via business partners? Also, does your company directly offers customization, after-sales support or does these activities are available via your business partners?  |