STATEMENT OF WORK

Audit of the IAEA Business Continuity Management System

1. Introduction

The International Atomic Energy Agency located in Vienna, Austria (hereinafter referred to as the IAEA) is widely known as the world's 'Atoms for Peace' 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.

The IAEA Secretariat is made up of some 2500 international professional and support staff from scientific, technical, managerial and other professional disciplines.

The IAEA runs most of its operations from a centralized location in Vienna. It also has two regional offices located in Toronto (Canada) and Tokyo (Japan), as well as two liaison offices in New York City (United States of America) and Geneva (Switzerland). The IAEA runs laboratories specializing in nuclear technology in Seibersdorf (Austria) and Monaco.

The Office of Internal Oversight Services' (OIOS) role is to strengthen the IAEA's internal oversight services and its ability to ensure management efficiency and programme effectiveness, and to enhance accountability. OIOS consolidates the functions of internal oversight covering internal audit, programme evaluation, management services and investigations. The Internal Audit function of OIOS provides independent and objective assessments of the adequacy and effectiveness of governance, risk management and control processes.

2. Background

Business Continuity Management (BCM) is a management process that identifies risk, threats and vulnerabilities that could have an impact on an entity's continued operations. It provides a framework for building organizational resilience and the capability for an effective response.

Effective as of December 2014, all entities in the UN System are required to adopt the **UN Organizational Resilience Management System (ORMS)** as an official emergency management framework. The core elements of the ORMS are:

(a) Crisis management decision making and operations coordination framework;
(b) Security support and response;
(c) Crisis Communications;
(d) Mass Casualty Incident Response;
(e) IT Disaster Recovery;
(f) Business Continuity; and

(g) Support to Staff, Survivors and their Families.

The IAEA is working to put in place all components of the Business Continuity Management System that will allow staff to continue operations in crisis situations by identifying priorities, responsibilities, resources and solutions.

3. Scope

OIOS will conduct an audit of the current status of the IAEA Business Continuity Management System[1] and its compliance with the ORMS as a part of the audit plan for 2017/2018. The audit should assess the adequacy of the IAEA's established governance, risk management and control processes to provide reasonable assurance regarding the effectiveness of the Business Continuity Management System.

For the purpose of this audit, OIOS defined the following key components of the BCM system to be assessed by the audit:

(a) The BCM policy;
(b) The establishment of program governance (roles and responsibilities, coordination structure, regular meetings of crisis management structure, etc.);
(c) The Risk Assessment and Business Impact Analysis;
(d) The BCM Planning (Security Plan, Crisis Management Plan, Business Continuity Plan, IT Disaster-Recovery Plan, Crisis Communication Plan, Mass Casualty Incident Response Plan, Staff Support Plan); and
(e) The BCM Plan maintenance, exercise and review.

To conduct the planned audit, OIOS requires the assistance of an external contractor with the expertise to perform such a review efficiently and to provide recommendations for improvement of existing processes, procedures, controls and infrastructure. It is anticipated that such review will be based on:

- Interviews in the relevant organizational units;
- Analysis of existing documentation and job descriptions;
- Surveys with (if applicable);
- Analysis of architecture of the IAEA IT systems and applications supporting critical processes; and
- Analysis of the equipment inventory records and operational practices.

The assessments will encompass all of the programmatic areas of the IAEA:

- Offices Reporting to the Director General (five Offices);
- Department of Management (five Divisions and one Office);

[1] Requirements of an effective Business Continuity Management System are described in the International Standard ISO22301:2012

- Department of Technical Cooperation (six Divisions);
- Department of Nuclear Energy (three Divisions);
- Department of Nuclear Safety and Security (three Divisions and two Offices);
- Department of Nuclear Sciences and Applications (four Divisions and one Office); and
- Department of Safeguards (six Divisions and six Offices).

4. Requirements

The audit shall be performed under the supervision and responsibility of the Director of OIOS and according to International Standards for the Professional Practice of Internal Auditing of the Institute of Internal Auditors. The OIOS IT Auditor will ensure operational coordination with IAEA staff and services. The external Contractor shall complement the role of the assigned IT Auditor within the Internal Audit function of OIOS.

The Contractor shall ensure that all interviews with IAEA staff and services are coordinated through OIOS and shall directly involve the IT Auditor in the execution of the assignment and all meetings.

Before publishing the final report, the Contractor shall, while still on-site, hold debriefing sessions for the relevant management and the technical team to explain and validate findings.

5. Location of Work

The Contractor's services shall be conducted on the IAEA premises in Vienna (Vienna International Centre (VIC), A-1400 Vienna, Austria). The assessment might include a visit to the IAEA facilities in Seibersdorf, which is approximately one hour's drive from Vienna.

The Contractor will be allowed to perform a data analysis of data that is not classified as 'confidential' or 'highly confidential', and to prepare the audit report, off-site. All interviews (up to 30), kick-off and exit meetings shall be organized in the IAEA premises in Vienna, according to the availability of the staff.

The IAEA shall provide, on its premises in the VIC, the infrastructure requested by the Contractor, such as office space, office equipment and internet connectivity, as well as physical access to the VIC.

6. Deliverables

The Contractor shall carry out the activities listed above and provide:

- An assessment of all components of the IAEA BCM system and their compliance with the ORMS, and identify potential weaknesses;
- An assessment of the BCM governance, maintenance, exercise and review;
- A list of IAEA processes critical to implement mandate and programmes and an overview of the current status of the resilience of those processes against disruptive events; and

- An assessment if critical ICT components support expected Recovery Time Objectives[2] (RTO) and Recovery Point Objectives[3] (RPO).

In cooperation with OIOS, discuss and validate outcomes with selected staff/Divisions within the IAEA. The Contractor shall present major findings and recommendations from the report to auditees on an exit conference organized in IAEA premises. In case of a need, OIOS might schedule more than one exit conference, but not more than three exit conferences are foreseen.

Following the exit conference the Contractor shall provide to OIOS the draft assessment report, which shall include the description of the tests performed, audit findings, risk ratings of the findings and the overall Contractor's opinion on the audit results.

OIOS will distribute the draft report to the auditees, collect their responses and send feedback to the contractor. If case of a need, OIOS shall organize additional meetings (up to 5) to facilitate report reconciliation. It is expected that the report reconciliation will last between 10 and 20 working days.

At the end of the reconciliation process, the Contractor shall deliver the final report for review and approval by OIOS in the English language. The report shall be delivered encrypted in softcopy.

Electronic communication of 'confidential' information between the Contractor and the IAEA shall be properly protected by mutually agreed methods.

[2] **Recovery Time Objective (RTO)** defines the time allowed for the recovery of a business function or supporting resources after a disruption/disaster occurs.

[3] **Recovery point objective (RPO)** quantifies the permissible amount of data loss in case of interruption and defines the earliest point in time that is acceptable to recover data.

7. Period of Performance

The audit is expected to take place from December 2017 to March 2018. The exact dates of each audit activity are listed in the table below:

Project Phase (Activity)	Engagement Time Line	Expected effort in person-hours To be completed by the bidder within response	Location
Kick-off meeting	December 2017	x	On-site
Preparation	December 2017	x	Off-site
Interviews, surveys, analysis of documentation and debriefing sessions	December 2017 - February 2018	x	xx% On-site, xx% off-site
Preparation and reconciliation of the draft and final report	March 2018	x	Off-site
Exit conference (1-3 sessions)	March 2018	x	On-site
Total expected effort - xx person-days			

8. Risks and Constraints

The assignment must be completed in March 2018. The main risks and constraints are:

- The possibility of incomplete documentation and late or limited survey responses;
- Failure to organize interviews with all relevant stakeholders;
- The need to manage perceptions and possible conflicts arising during the assignment by carefully involving all key stakeholders in the review process and maintaining objectivity and impartiality throughout the assignment; and
- Failure to fully deliver the expected outputs in a timely manner and with the estimated level of effort.

9. Personnel and Resources

The Contractor shall provide consultants with the following profiles:

- A project lead with a minimum of 10 years of experience in auditing and a proven track of record in performing similar assessments in organizations/companies having more than 2 000 employees;

- A project team comprising experts with a minimum of 10 years of experience in auditing, preferably in the area of Business Continuity Management; and
- At least one team member with a minimum of 10 years of experience in IT Audit with a proven track of record in performing assessments of IT Disaster-Recovery Plans in organizations/companies having more than 2 000 employees.

10. IAEA Support for the Assignment

The Internal Audit function, as the focal point for this assignment, will facilitate the following:

- Access to relevant IAEA documentation;
- Identification of relevant internal stakeholders, preparation and coordination of all stakeholder meetings;
- Support in preparation of surveys;
- Preparation of the OIOS draft and final audit report based on the assessment report provided by the Contractor; and
- Feedback and comments on the draft deliverables throughout the assignment.

11. Other Matters

The Contractor shall be required to sign the IAEA Confidentiality Undertaking for Non-Staff Members. The Contractor shall not remove any data from the premises without prior clearance by OIOS and shall hand over all IAEA data to OIOS at the end of the assignment. In addition, the Contractor shall confirm that no information, in electronic or other form, has been retained beyond the contracted period.

The Contractor shall not share any information related to this assignment with any parties, within or outside the IAEA, without the prior authorization of the Director of OIOS.

12. Quality Control

All work products, intermediate and final deliverables are subject to quality review and formal approval by the IAEA.