Tender Scope for Cyber Risk Assessment and Business Continuity Planning

1. Introduction

The **Civil Aviation Authority of Fiji (CAAF)**, hereinafter referred to as "the Authority," is seeking proposals from qualified and experienced vendors to conduct a comprehensive **Cyber Risk Assessment** and develop a robust **Business Continuity Plan (BCP)**. The objective is to enhance our cybersecurity posture, prioritize assets based on criticality, and ensure the resilience of our business operations against potential cyber threats and disruptions.

2. Objectives

- **Cyber Risk Assessment**
    - Identify and evaluate cyber risks across all areas of the Authority's operations.
    - Develop a detailed risk register documenting identified risks, their potential impacts, and recommended mitigation strategies.
    - Categorize assets based on priority and criticality to the business.
    - Create a strategic roadmap for risk mitigation and cybersecurity enhancements.
- **Business Continuity Planning**
    - Conduct a thorough Business Impact Analysis (BIA).
    - Develop a comprehensive Business Continuity Plan that ensures the continuity of critical business functions during and after a disruption.
    - Establish procedures for regular testing, maintenance, and updating of the BCP.

3. Scope of Work

The selected vendor will be responsible for delivering the following services:

A. Cyber Risk Assessment

1. **Asset Identification and Categorization**
    - Inventory all information assets, including hardware, software, data, and network components.
    - Categorize assets based on their importance to business operations, confidentiality, integrity, and availability requirements.
2. **Threat and Vulnerability Assessment**
    - Identify potential internal and external threats to the Authority's assets.
    - Assess vulnerabilities within the current IT infrastructure and processes.
    - Evaluate the likelihood and potential impact of identified threats exploiting vulnerabilities.
3. **Risk Analysis and Evaluation**
    - Quantify and prioritize risks based on their potential impact and likelihood.

    - Map risks to specific assets and business processes.
4. **Risk Treatment Planning**
    - Recommend appropriate risk mitigation strategies (avoidance, reduction, sharing, or acceptance).
    - Develop action plans for implementing recommended controls and measures.
5. **Development of Risk Register**
    - Document all identified risks, assessments, and mitigation plans in a comprehensive risk register.
    - Include risk owners, review dates, and status updates.
6. **Roadmap Creation**
    - Develop a strategic roadmap outlining steps to enhance cybersecurity measures over a defined timeline.
    - Include short-term, medium-term, and long-term initiatives with clear milestones.

B. Business Continuity Planning

1. **Business Impact Analysis (BIA)**
    - Identify critical business functions and processes.
    - Determine the effects of disruptions on these functions.
    - Establish Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).
2. **Strategy Development**
    - Identify and evaluate recovery strategies for critical operations.
    - Recommend solutions for resource requirements, including personnel, technology, and facilities.
3. **Plan Development**
    - Draft a comprehensive Business Continuity Plan tailored to the Authority's needs.
    - Outline roles and responsibilities, communication plans, and step-by-step recovery procedures.
4. **Training and Awareness**
    - Develop and deliver training programs to ensure staff are aware of the BCP and their specific roles.
    - Provide materials for ongoing awareness and education.
5. **Testing and Maintenance**
    - Design and conduct BCP testing exercises (e.g., tabletop exercises, simulations).
    - Establish procedures for regular review and updates of the BCP to reflect changes in the business environment.

4. Deliverables

The vendor is expected to provide the following deliverables:

- **Risk Register**: A detailed document listing all identified risks, assessments, and mitigation strategies.
- **Asset Categorization Report**: Classification of assets based on priority and criticality.

- **Cybersecurity Roadmap**: Strategic plan outlining initiatives for risk mitigation and cybersecurity enhancement.
- **Business Impact Analysis Report**: Findings and analysis from the BIA process.
- **Business Continuity Plan**: A comprehensive plan covering policies, procedures, and recovery strategies.
- **Training Materials**: Documentation and resources for staff training and awareness programs.
- **Testing Reports**: Results and analysis from BCP testing exercises.
- **Executive Summary**: High-level overview of key findings and recommendations suitable for senior management.

5. Vendor Qualifications

Prospective vendors must demonstrate the following qualifications:

- Proven experience in conducting cyber risk assessments and developing business continuity plans for organizations of similar size and complexity.
- Expertise in relevant standards and frameworks (e.g., ISO 27001, ISO 22301, NIST Cybersecurity Framework).
- Certified professionals (e.g., CISSP, CISM, CISA, CBCP) as part of the project team.
- Strong project management capabilities and the ability to deliver on time and within budget.
- Excellent communication skills and the ability to work collaboratively with internal stakeholders.

6. Proposal Requirements

Vendors should include the following information in their proposals:

- **Executive Summary**: Brief overview of the proposal and its alignment with the Authority's objectives.
- **Company Profile**: Background information, including years in business, areas of expertise, and organizational structure.
- **Relevant Experience**: Examples of similar projects completed, including client references.
- **Project Team**: Bios and qualifications of key personnel assigned to the project.
- **Methodology and Approach**: Detailed description of the proposed approach for the risk assessment and BCP development.
- **Project Plan**: Timeline with key milestones, deliverables, and resource allocation.
- **Cost Proposal**: Breakdown of all costs, including fees, expenses, and any additional charges.
- **Compliance Statement**: Confirmation of the ability to meet all requirements outlined in this tender.
- **Additional Information**: Any other relevant information that supports the proposal.

7. Evaluation Criteria

Proposals will be evaluated based on the following criteria:

- **Understanding of Requirements** (20%)
  - Demonstrated comprehension of the project scope and objectives.
- **Experience and Expertise** (30%)
  - Relevant experience and qualifications of the vendor and project team.
- **Methodology and Approach** (25%)
  - Soundness and effectiveness of the proposed methodology.
- **Cost Effectiveness** (15%)
  - Value for money and transparency of the cost proposal.
- **References and Past Performance** (10%)
  - Feedback from provided references and track record of delivering similar projects.

8. Compliance Matrix and Evaluation Criteria

To ensure a transparent and objective selection process, the Authority will use the following compliance matrix to evaluate vendor proposals. Vendors are required to complete the matrix by indicating their level of compliance and providing comments or references to their proposal where appropriate.

Compliance Matrix

Instructions for Vendors

- **Vendor Response**: Indicate your level of compliance with each criterion by selecting **Yes**, **Partial**, or **No**.
- **Comments/Reference**: Provide brief comments or references to sections in your proposal that address the criterion.
- **Points Awarded**: This column will be filled out by the evaluation committee based on the quality of your response.

Scoring Guidelines

- **Yes**: Full compliance; the vendor meets or exceeds the requirement. Eligible for full points.
- **Partial**: Partial compliance; the vendor meets some aspects of the requirement. Eligible for partial points.
- **No**: Non-compliance; the vendor does not meet the requirement. Zero points awarded.

Evaluation Criteria and Point Allocations

No.	Criteria	Description	Maximum Points	Vendor Response (Yes/Partial/No)	Comments/Reference	Points Awarded (Filled by Authority)
1	**Understanding of Requirements**		**20**			
1.1	Comprehension of Project Scope	Demonstrated understanding of the tender's objectives and requirements	10			
1.2	Alignment with Authority's Goals	Proposal aligns with the Authority's strategic goals and needs	10			
2	**Experience and Expertise**		**30**			
2.1	Relevant Project Experience	Experience in similar projects (cyber risk assessment and BCP development)	15			
2.2	Qualifications of Project Team	Expertise and certifications of team members (e.g., CISSP, CISM, CISA, CBCP)	10			
2.3	Knowledge of Standards and Frameworks	Familiarity with ISO 27001, ISO 22301, NIST CSF, etc.	5			
3	**Methodology and Approach**		**25**			
3.1	Proposed Methodology	Clarity and soundness of	15			

		the proposed approach				
3.2	Project Plan and Timeline	Realistic and detailed plan with key milestones	10			
4	**Cost Effectiveness**		**15**			
4.1	Cost Transparency	Clear breakdown of costs, fees, and expenses	5			
4.2	Value for Money	Competitive pricing relative to the services offered	10			
5	**References and Past Performance**		**10**			
5.1	Client References	Positive feedback from previous clients	5			
5.2	Track Record	Demonstrated ability to deliver projects on time and within budget	5			
	Total Points		**100**			

Minimum Qualification Threshold

Vendors must achieve a minimum score of **70 out of 100 points** to be considered for final selection.

Detailed Criteria Description

1. Understanding of Requirements (20 Points)

- **1.1 Comprehension of Project Scope (10 Points)**
  - The vendor should demonstrate a clear understanding of the project objectives, deliverables, and scope as outlined in the tender document.
- **1.2 Alignment with Authority's Goals (10 Points)**

  - The proposal should align with the Authority's strategic goals and address how the vendor's services will meet these objectives.

2. Experience and Expertise (30 Points)

- **2.1 Relevant Project Experience (15 Points)**
  - Provide examples of similar projects completed, highlighting outcomes and client satisfaction.
- **2.2 Qualifications of Project Team (10 Points)**
  - Include bios and certifications of key personnel who will be assigned to the project.
- **2.3 Knowledge of Standards and Frameworks (5 Points)**
  - Demonstrate familiarity with relevant industry standards and frameworks.

3. Methodology and Approach (25 Points)

- **3.1 Proposed Methodology (15 Points)**
  - Outline the approach for conducting the cyber risk assessment and developing the BCP.
- **3.2 Project Plan and Timeline (10 Points)**
  - Provide a detailed project plan with realistic timelines and milestones.

4. Cost Effectiveness (15 Points)

- **4.1 Cost Transparency (5 Points)**
  - Offer a clear and detailed breakdown of all costs associated with the project.
- **4.2 Value for Money (10 Points)**
  - The pricing should be competitive and reflect the quality and scope of services offered.

5. References and Past Performance (10 Points)

- **5.1 Client References (5 Points)**
  - Supply at least three client references who can attest to the vendor's performance on similar projects.
- **5.2 Track Record (5 Points)**
  - Demonstrate a history of completing projects on time and within budget.

Evaluation Process

The evaluation committee will review each proposal against the criteria listed in the compliance matrix. Points will be awarded based on the level of compliance and the quality of the vendor's response.

9. Submission Instructions

- **Proposal Submission Deadline**: **29th November 2024**
- **Submission Method**: Proposals must be submitted electronically in PDF format to **tenders@caaf.org.fj**.
- **Inquiries**: All questions or requests for clarification must be submitted in writing to **tender.enquiries@caaf.org.fj**
- **Proposal Validity**: Proposals must remain valid for a period of 90 days from the submission deadline.

10. Terms and Conditions

- The Authority reserves the right to accept or reject any or all proposals without assigning any reason.
- All costs incurred in the preparation of the proposal shall be borne by the vendor.
- The successful vendor will be required to enter into a formal agreement with the Authority.
- The vendor must comply with all applicable laws and regulations.
- All work products and deliverables developed during the project will become the property of the Authority.