INSTITUTE OF SINGAPORE CHARTERED ACCOUNTANTS
60 Cecil Street, ISCA House
Singapore 049709
Tel: 65 6749 8060
isca.org.sg

ICT-27-2025 AI Governance Policy Development & Cybersecurity Review

Introduction

Institute of Singapore Chartered Accountants, ISCA, will like to invite qualified cybersecurity service providers to submit proposals for the development of an Artificial Intelligence (AI) Governance Policy and related knowledge-sharing activities. The engagement is expected to be completed within a **one- to three-months** period.

The objective is to:

- Provide practical guidance to ISCA staff on the responsible and secure use of AI;
- Strengthen ISCA's cybersecurity posture; and
- Establish a structured governance framework for AI technologies.

ISCA maintains approximately **50 documents** (policies, procedures, guidelines, reports) relevant to this engagement.

1. Project Scope

1.1 Cybersecurity Posture Assessment

The selected vendor shall:

- Review ISCA's ISO 27001-related documents and ISO audit report to assess existing cybersecurity, governance, and operational practices, aligning to **NIST Cybersecurity Framework 2.0**.
- Conduct **interviews with key employees or nominated representatives** to understand the current cybersecurity posture.

  Specify in the proposal:

  - *The **maximum number of documents** included in the review, and*
  - *The **maximum number of interviews** to be conducted within the proposed 1–3 months period.*

1.2 AI Governance Framework and NIST 2.0 Framework Development

The selected vendor shall:

- Draft **one (1) AI Governance Policy** defining principles for responsible, ethical, and secure AI use. The policy should preferably align with **ISO 42001**.
- Draft **one (1) NIST Cybersecurity 2.0 Framework Policy**
- Based on the drafted policy, **review and update existing policies/procedures** related to AI usage, covering areas such as staff usage, internal system governance, and vendor management.

  *Provide upfront the **maximum number of documents** that will be updated.*

1.3 Knowledge Sharing & Implementation Support

Conduct **one (1) knowledge-sharing or briefing session** with management and key stakeholders to present both AI Governance Policy and NIST Cybersecurity Framework 2.0 Policy, outline responsibilities, and discuss implementation considerations.

1.4 Optional Component: AI Tabletop Exercise

Provide an **optional tabletop exercise** focusing on an employee-AI usage scenario and its potential impact on cybersecurity or governance.

2. Deliverables

The selected vendor shall provide:

- **NIST Cybersecurity Framework 2.0 Policy**, derived from the document review and interview, and
- **AI Governance Policy** and Procedures document, preferably align to ***ISO 42001***.
- Updated clauses and the relevant updated existing ISCA documents.
- One knowledge-sharing session with ISCA management and key stakeholders on the AI Governance Policy and NIST Cybersecurity Framework 2.0 Policy
- (Optional) Tabletop Exercise session

3. Proposal Submission Requirements

Vendors are required to submit the following:

- **Company Profile**, including brief examples of experience in cybersecurity assessment, governance, and AI-related policy development.
- **Proposed Methodology and Work Plan**, covering a 1–3 months timeline, including interview approach, document review process, and policy development workflow.
- **Team Composition** and key personnel assigned.
- **Deliverables and Milestones** aligned to the scope.
- **Fees and Pricing Structure**, including optional tabletop exercise cost.
- **Assumptions or Exclusions** included in the proposal.

4. Evaluation Criteria

Proposals will be evaluated based on:

- Relevant experience and expertise
- Quality and practicality of the proposed methodology
- Demonstrated understanding of requirements
- Pricing competitiveness
- Resource allocation and proposed timeline

5. Submission Details

Submission Deadline: 10 Dec 2025, 5pm Singapore Time (GMT+8)
Submission Format: Proposals must be submitted electronically in PDF format.
Email to: ict.tenders@isca.org.sg
Subject Line: ICT-27-2025

For clarification or further information, please contact: ict.tenders@isca.org.sg

6. Confidentiality

All information provided in response to this ITQ shall be treated as confidential and used solely for the purpose of evaluation.

7. Disclaimer

ISCA reserves the right to reject any or all proposals, to waive any irregularities, and to award the contract in part or in full, at its sole discretion. Submission of a proposal does not guarantee selection or contract award.