Request for Proposal

Design and Develop IT Frameworks

November 03, 2025

1. Introduction

The Institute of Chartered Accountants of Pakistan (ICAP) is committed to strengthening its digital, technological, and information security capabilities to support its mission of excellence in professional education, regulation, and member services. In pursuit of this goal, ICAP seeks to engage a qualified consulting or technology partner to assist in developing a comprehensive IT Governance and Security Framework aligned with international best practices and standards such as ISO/IEC 27001, ISO 31000, ITIL, PMBOK, PRINCE2, and NIST.

ICAP' s technology environment supports a diverse portfolio of services — including member management systems, student examination platforms, portals, financial systems, and collaboration tools — across on-premises and cloud infrastructures. To ensure continued growth, compliance, and resilience, ICAP intends to modernize its IT policies, processes, and security posture through a structured, organization-wide framework.

This Request for Proposal (RFP) invites competent and experienced firms to propose methodologies, deliverables, timelines, and costs for designing and developing the required frameworks, policies, and tools as detailed in the scope of work.

2. Objective

The primary objective of this RFP is to engage a qualified partner capable of designing, developing, a holistic IT governance, risk, and security ecosystem that enables ICAP to align its IT strategy with the organization's vision and strategic goals, driving digital transformation and operational excellence. The selected partner will establish robust IT governance frameworks, policies, procedures, and controls to ensure effective decision-making, accountability, and compliance across all technology functions.

This initiative aims to enhance ICAP' s information security posture by implementing an ISO/IEC 27001–aligned Information Security Management System (ISMS) to safeguard the confidentiality, integrity, and availability of information assets, while also introducing standardized risk and compliance frameworks based on ISO 31000 and NIST SP 800-30 for proactive risk management and a live IT risk register.

The engagement further seeks to strengthen ICAP' s cyber resilience and business continuity by developing comprehensive BCP and DRP frameworks, modernize IT operations through an IT Service Management (ITSM) model aligned with ITIL and ISO 20000, and institutionalize data governance and privacy practices to ensure regulatory compliance and responsible data stewardship.

Additionally, the partner will define Minimum Baseline Security Standards (MBSS) and platform-specific security configurations for systems, networks, and cloud platforms; enhance institutional capability through training and awareness programs to foster a security-conscious workforce; and establish mechanisms for continuous improvement through measurable KPIs, KRIs, and dashboards to monitor IT performance, risk posture, and compliance maturity.

3. Scope of Work

a. IT Governance Framework

Define IT decision-making structures, roles, and committees (e.g., IT Steering Committee, Architecture Board). Establish processes for policy development, review cycles, compliance tracking, and reporting to management.

b. IT Strategy

Develop a 3–5-year IT vision and mission aligned with ICAP' s organizational goals. Define strategic objectives, key initiatives, digital transformation roadmap, and measurable performance indicators (uptime, automation, service quality, cost optimization).

c. IT Policy

Provide overarching guidelines for IT resource usage, access management, procurement, hardware/software standards, acceptable use, remote access, and monitoring. Ensure compliance with regulatory and internal governance requirements.

d. Information Security Policy (ISO/IEC 27001 Aligned)

Establish principles for protecting the confidentiality, integrity, and availability of information assets. Define security governance, risk management, access control, encryption, incident response, vendor security, and training requirements.

e. Data Governance & Privacy Framework

Develop policies for data classification, retention, quality, and protection. Define roles such as Data Owners and Data Stewards. Include procedures for compliance with data protection laws (GDPR/PDPA equivalents) and internal privacy controls.

f. Minimum Baseline Security Standards (MBSS)

Define the mandatory baseline configurations and security controls for systems, servers, endpoints, applications, and networks. Reference CIS Benchmarks, NIST controls, and ISO 27001 for configuration hardening and patch management.

g. Platform-Specific Security Policies

Develop tailored policies for:

- **Windows & Linux servers:** Hardening, patching, identity management.
- **Cloud (AWS/Azure):** Identity governance, encryption, compliance, and guardrails.

  Network devices: Firewalls, routers, wireless access controls, and monitoring standards.

h. IT Risk Management Framework

Define the methodology for risk identification, assessment, mitigation, and monitoring in line with ISO 31000 and NIST SP 800-30. Include a process for regular risk reviews, ownership, and escalation.

i. IT Project Management Framework

Establish project governance, stage gates, and documentation requirements aligned with PMBOK or PRINCE2. Include templates for business cases, risk registers, change control, and post-implementation reviews.

j. IT Service Management (ITSM) Framework

Design IT service processes aligned with ITIL or ISO 20000. Define incident, problem, and change management procedures, service desk workflows, and key performance metrics (MTTR, SLA compliance, CSAT).

k. IT Business Continuity Plan (BCP) & Disaster Recovery Plan (DRP)

Develop frameworks to ensure continuity of critical IT services during disruptions. Include risk analysis, RTO/RPO definitions, recovery strategies, DR tiers, testing plans, and documentation templates.

l. IT Backup Policy

Define standardized backup procedures covering data frequency, retention, encryption, and restoration testing. Include 3-2-1 backup methodology, success criteria, and recovery validation processes.

m. Vendor & Third-Party Security Management

Define due diligence, risk assessments, and contractual clauses for external vendors. Establish requirements for security questionnaires, SLAs, data protection, and incident reporting by third parties.

n. Security Awareness & Training Program

Develop ongoing awareness and training initiatives for all employees, including phishing simulations, compliance training, and specialized programs for IT and privileged users. Track completion and performance metrics.

o. Cloud Governance & FinOps Policy

Define cloud adoption, governance, and operational management principles. Include policies for cloud security posture management, identity, tagging, and cost optimization (FinOps).

p. Monitoring, Reporting & Metrics Framework

Establish performance monitoring for IT operations and security. Define KPIs, dashboards, and reporting cadence (monthly/quarterly) for uptime, risk, backup success, patch compliance, and user satisfaction.

4. Technical / Eligibility Criteria

Sr. No	Evaluation Area	Description / Assessment Focus	Weight (%)
1	**Relevant Experience**	Number, size, and complexity of similar IT governance, risk, and security projects delivered (preferably in public sector, education, or regulatory bodies).	**25%**
2	**Technical Expertise & Certifications**	Qualifications and certifications of key team members (ISO 27001, ITIL, PMP/PRINCE2, Cloud Security, etc.) and adequacy of resources.	**20%**
3	**Methodology & Approach**	Quality, completeness, and practicality of the proposed methodology, work plan, and alignment with global standards (ISO, NIST, ITIL, PMBOK).	**20%**
4	**Proposed Deliverables & Quality Assurance**	Clarity, completeness, and feasibility of deliverables, including templates, frameworks, and implementation roadmap.	**10%**
5	**Project Management Capability**	Demonstrated ability to manage timelines, communication, milestones, and governance reporting effectively.	**10%**
6	**Financial Stability**	Evidence of stable financial performance and capacity to sustain project operations.	**5%**
7	**Training & Knowledge Transfer Plan**	Inclusion of comprehensive training, workshops, and capability-building for ICAP staff.	**5%**
8	**Local Presence & Support**	Availability of local team or partner for onsite sessions, workshops, and ongoing coordination.	**5%**

5. Deliverables

The selected bidder will be responsible for producing comprehensive, actionable, and auditable documentation, frameworks, and implementation support aligned with global best practices. Key deliverables shall include but are not limited to:

a. Strategic & Governance Deliverables

- IT Strategy Document: Vision, mission, strategic objectives, digital transformation roadmap, KPIs, and governance structure.
- IT Governance Framework: Roles, committees, decision rights, reporting structures, and policy lifecycle management.

b. Policy & Framework Deliverables

- Information Security Policy aligned with ISO/IEC 27001.
- IT Policy covering acceptable use, access control, device, and software management.
- Data Governance & Privacy Framework including data classification, retention, and ownership.
- Minimum Baseline Security Standards (MBSS) for all systems, networks, and applications.
- Platform-Specific Security Policies for Windows, Linux, Cloud (AWS/Azure), and network devices.
- Vendor & Third-Party Security Policy with due-diligence and SLA requirements.
- IT Service Management (ITSM) Framework aligned with ITIL / ISO 20000.

c. Risk & Compliance Deliverables

- IT Risk Management Framework based on ISO 31000 and NIST SP 800-30.
- IT Risk Register Template (with sample populated entries).
- Compliance & Audit Framework including internal audit checklists and review process.
- Security Awareness & Training Program and communication plan.

d. Business Continuity & Resilience Deliverables

- Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) with RTO/RPO metrics.
- IT Backup Policy defining backup frequency, retention, encryption, and testing.
- Monitoring & Reporting Framework for service uptime, backup success, and recovery validation.
- Change & Configuration Management Policy for standard, normal, and emergency changes.

e. Implementation & Handover Deliverables

Upon completion, ICAP will possess a unified IT governance and security framework with:

- Editable templates, registers, and forms (Word/Excel).
- Training and knowledge-transfer sessions for ICAP IT staff.
- Final presentation, documentation set, and implementation roadmap.
- Project completion report summarizing outcomes, recommendations, and next steps.

6. Financial Proposal Submission Guidelines.

All vendors are required to submit **two sealed envelopes** as part of their response to this RFP:

- **Technical Proposal**

  The Technical Proposal must include:

  - All documents related to eligibility, technical compliance, and proposed solution design.
  - Must be clearly marked: "Technical Proposal – Design and Develop IT Frameworks"

- **Financial Proposal**

  The Financial Proposal must:

  - Quote all amounts in PKR, clearly inclusive of all applicable taxes.
  - Be submitted on the firm's official letterhead, duly signed by the head of the firm or an authorized representative.
  - Include a validity period of at least 120 calendar days from the date of submission.
  - Clearly mention quoted amounts in both words and figures.
  - Mention warranty details (if applicable), highlighted in bold.
  - Ensure no overwriting, cutting, or erasing in the document.
  - Be clearly marked: "Financial Proposal – Design and Develop IT Frameworks"

- **Additional Compliance Requirements**

  - The vendor must be:
    - Registered with Sales Tax and Income Tax authorities.
    - An active taxpayer, with NTN and GST registration in the firm's name (not an individual's).
  - Proposals with conditional, partial, or optional items will be rejected.
  - All applicable government taxes will be deducted from the billed amount as per law. A GST invoice must accompany the bill.
  - The quoted solution must include complete supply, delivery, and commissioning at: ICAP House, G-31, Chartered Accountants Avenue, Clifton Block 8, Karachi.
  - The Purchaser reserves the right to accept, reject, or cancel any or all bids without assigning any reason.

7. Clarification and Interpretation of the Document

The queries and clarification related to the document are to be submitted in writing to the stated address or email at imran.hafeez@icap.org.pk/ procurement@icap.org.pk . Such queries should refer to the Section, Subsection, and page number of the document.

The queries should reach ICAP by **15 November 2025** via email, post or other appropriate medium, and will be addressed/ answered by email in response time of one working day.

It should further be noted that the Institute solely reserves the right to interpret the document. The responses to such queries, clarifications and interpretations will be made in writing. No other Interpretations will be binding on the Institute.

8. Bid Document

Caution: All Vendors are requested to read this document carefully and must fulfill the mentioned requirements otherwise they will not be allowed to participate.

1. ICAP Karachi, (hereinafter referred to as "the Purchaser") invites / requests Proposals (hereinafter referred to as "the Bidders") for supply and delivery of required services.

   Queries of the Bidders seeking clarifications must be received in writing to the Purchaser within stipulated timeline. Any query received after deadline will not be entertained. ICAP Karachi may host a Q&A session, if required, at ICAP head office (Chartered Accountants Avenue Clifton block 8, Karachi). All Bidders shall be informed of the date and time in advance.

The Contact for all correspondence in relation to this bid is as follows:

Primary Contact

imran.hafeez@icap.org.pk

111-000-422-Ext:355
ICAP, Karachi

Secondary Contact

procurement@icap.org.pk

111-000-422-Ext:302
ICAP, Karachi.

2. Bidders should note that during the period from the receipt of the bid and until further notice from Primary Contact, all queries should be communicated via Primary Contact and in writing (e-mail) only. In the case of an urgent situation where Primary Contact cannot be contacted, the bidder may alternatively direct their enquiries through the Secondary Contact.
3. In accordance with these rules, interested Bidders applying for bids should submit two separate bids/envelopes for Financial Proposal and Technical Proposal. The envelopes shall be marked as "Financial Proposal" and "Technical Proposal" in bold and legible to avoid confusion. Initially, only the envelope marked "Technical Proposal" shall be opened. The envelope marked as "Financial Proposal" shall be retained in the custody of the ICAP Karachi without being opened.
4. ICAP Karachi shall evaluate the technical proposal in a manner prescribed in advance, without reference to the price and reject any proposal, which does not conform to the specified requirements.
5. Bidders will be solely responsible to deliver all required items/materials as well as to complete the project within the decided timeframe from all aspects.

The proposed schedule for the procurement process is as follows.

Activity	Date
RFP Advertisement ICAP Website	03 November 2025
Prospective bidders may submit questions and comments regarding RFP document by	15 November 2025

Activity	Date
ICAP responds to questions and comments via email to all bidder(s)	16 November 2025
Bid submission	17 November 2025 latest by 3 pm
Bid Opening – Technical Bid	17 November 2025 (4 pm)
Bid Opening – Financial Bid	Financial bids will be opened after technically qualified bidders evaluated

9. Project Execution Model for Implementation

The bidders are required to furnish a relevant and detailed execution model for Design and Development IT Frameworks.

10. Training plan

The Implementer is required to provide training to all Users of the Institute. The purpose of the training is to fully equip the users with skills and knowledge to carry out the business processes.

Therefore, the bidders are required to submit in detail the professionally designed Training Plan Road Map at the following two levels:

a) The *User Level Training* is mandatory part of implementation services and will be provided by the implementer to all the Users including Senior Management. The training should provide hands on learning to users to carry out day-to-day business activities and execute reports in the system.

b) The *Professional Level Training* is to be provided to ICAP admin users in selected portals. The purpose of the training is to identify the features available in all solutions. Understand the working, processes of the solution, to be able to handle and manage the implementation services at advance level with clear understanding of solutions.

11. Payment Schedule

A payment schedule will be prepared after mutual agreement based on bid price:

a. Deliverables as per agreement/Blueprint

b. Time frame of Overall Contract Execution.

c. Successful Acceptance Test.

d. Training plan.

e. Advance payment if required will be subject to separate advance payment.

12. Mode of Payment

- The development, deployment and Implementation rates are to be quoted in Pak Rupees.

13. Penalty Clause

The Penalty will be imposed @10% of quoted value, if project completion timelines are not

met.

14. Conditions of Contract

a. The bidder by submitting a proposal has agreed to abide by the Terms & Conditions and the Scope of work as defined in the document and is assumed to be 100% in agreement to terms and conditions floated in the document.
b. SECRECY
    a. The parties shall not at any time during or after the term of the agreement, divulge or allow to be divulged, to any person, any confidential information contractual arrangement, products, business or affairs of the parties.
    b. Notwithstanding anything contained in the paragraph, no party shall be precluded from disclosing any information to the extent required in any legal proceedings.
c. AMICABLE SETTLEMENT
    a. The parties shall use their best efforts to amicably settle all disputes arising out of or in connection with this contract or its interpretation. In case of failure to amiably resolve, the matter shall be referred to arbitration and Council of ICAP will be appointed as sole arbitrator, whose decision will be binding on both parties.
    In case of any Person/ Change of team, Firm will provide better or equal team at 'no' cost/disturbance of project.
d. PROTECTION OF ACCRUED RIGHTS
    a. The expiry or termination of this Agreement shall be without prejudice to any rights which have already accrued to either of the parties under this agreement.
e. GOVERNING LAWS:
    a. This Agreement shall be governed by and construed in accordance with Pakistan's law. The parties are entitled to amend the agreement, however, modification and amendments to this agreement shall be effective only if made in writing and signed by the parties or by their duty authorized representatives.

15. Client Reference – Successful Implementations

Sr. #	Client Name	Implementation Details	Contact Person (Name, Designation and Telephone no.)

16. Consultant/Project team Details

Sr. #	Consultant Name	Specialized Area	Firm Joining date	Total Experience in specialized area (No. of years)	Name of successful project in relevant expertise implemented