RFP Number: NICL/IT/RFP/VAPT_Cyber SecurityAudit_RedTeaming/18/2025

RFP for Selection of Vendor for Vulnerability Assessment and Penetration Testing - VAPT, Cyber Security Audit and Red Teaming Services

Disclaimer

The information contained in this Request for Proposal (RFP) document or information provided subsequently to Bidder(s) or applicants whether verbally or in documentary form by or on behalf of National Insurance Company Limited (NIC/NICL), is provided to the Bidder(s) on the terms and conditions set out in this RFP document and all other terms and conditions subject to which such information is provided.

This RFP is neither an agreement nor an offer and is only an invitation by NICL to the interested parties for submission of bids.

The purpose of this RFP is to provide the Bidder(s) with information to assist the formulation of their proposals. This RFP does not claim to contain all the information each Bidder may require. Each Bidder may conduct its own investigations and analysis and should check the accuracy, reliability and completeness of the information in this RFP and where necessary obtain independent advice.

NICL makes no representation or warranty and shall incur no liability under any law, statute, rules or regulations as to the accuracy, reliability or completeness of this RFP.

NICL may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP.

1 Overview

1.1 About National Insurance Company Limited

National Insurance Company Limited (hereinafter referred to as NIC or, NICL), with its registered office in Kolkata, is one of the leading public sector insurance companies of India. It was incorporated in 1906 and nationalized in 1972, before operating as a Government of India undertaking from 2002. National Insurance Company Ltd (NIC) is carrying out a non-life insurance business.

Headquartered in Kolkata, NICL's network of about 900 offices, manned by more than 7,000 skilled personnel, is spread over the length and breadth of the country covering remote rural areas, townships and metropolitan cities. NICL's foreign operations are carried out from its branch offices in Nepal.
NICL transacts general insurance business of Health, Motor, Fire, Marine and Miscellaneous insurance. Befittingly, the product ranges of more than 200 products offered by NICL cater to the diverse insurance requirements of its 17 million policyholders. Innovative and customized policies ensure that even specialized insurance requirements are fully taken care of.

Serving approximately two crore policy holders in a year with a product portfolio of about 200+ products targeting commercial, retail, rural and micro insurance market segments, the company handles direct non-life insurance, both in the retail and corporate segments, re-insurance and investment of funds. NICL's distribution network consists of over 65,000 different intermediaries comprising direct sales, individual and corporate Agents, Micro Agents, Brokers, Bancassurance, Motor Insurance Service Providers (MISPs) etc. NICL also partners with Garages, Third Party Administrators and Digital Service Providers for servicing Claims generated from customers for servicing Claims generated from customers. Their annual new and renewal policy transaction volume is about 2 crore and processed claims transaction volume is about 50 lakhs.

The Company has undertaken IT initiatives to address its core business requirements and all its offices are interconnected through a Wide Area Network.

1.2 Purpose of this document

This Request for Proposal (RFP) invites bids from CERT-In empanelled Information Security Auditing Organizations to provide comprehensive Vulnerability Assessment and Penetration Testing (VAPT), Cyber Security Audit, and Red Teaming services. The objective is to assess and enhance NICL's Cyber Security posture, ensure compliance with IRDAI Information and Cyber Security Guidelines, 2023 (as updated March 24, 2025), Digital Personal Data Protection Act (DPDP) 2023, and align with global standards such as ISO 27001:2022, NIST CSF 2.0, and OWASP frameworks. The selected vendor will deliver actionable insights, remediation roadmaps, and training to strengthen NICL's defenses against BFSI-specific cyber threats, with vendor selection based on eligibility, technical qualification, and lowest bid via reverse auction. The project period is 3 (three) years.

This RFP contains details regarding scope, project timelines, evaluation process, terms and conditions as well as other relevant details which Bidder needs to factor while responding to this RFP. The RFP document is not a recommendation, offer or invitation to enter into a contract, agreement or other arrangement in respect of the services. The provision of the services is subject to the observance of the selection process and appropriate documentation being agreed between NICL and any successful Bidder identified after completion of the selection process.

The Bidder is expected to examine all instructions, clarifications, forms, terms, specifications, and other information in the RFP Document, corrigendum, addendum etc. Failure to furnish all information required by any of these documents or to submit a Bid not substantially responsive to these documents in every respect will be at Bidder's risk and may result in the rejection of its Bid.

Bidders are advised to study the mentioned documents carefully before participating. It shall be deemed that submission of bid by the Bidder has been done after their careful study and examination of the mentioned documents with full understanding of its implications. Any lack of information shall not in any way relieve the Bidder of his responsibility to fulfill his obligations under the Bid.

In the event of default by the Bidder with respect to this RFP or the RFP Document, NICL may debar the Bidder from participating in future RFPs of NICL for a period not exceeding two years.

1.3 Important Dates and Information

Bid Reference	**RFP Number: NICL/IT/RFP/VAPT_Cyber SecurityAudit_RedTeaming/18/2025**
Date of Commencement of Bid	**03-12-2025**
Date and Time for Receipt of Bids (**Online for PQ, Technical and physical for Commercial Bid**)	**31-12-2025 up-to 1:00 PM (online)** **31-12-2025 up-to 3:00 PM (certified physical copy)**
Date and Time for request for clarification of Bids	**09-12-2025 up-to 6:00 PM**
Date and Time for Pre-Bid Meeting	**10-12-2025 at 3:00 PM (in-person or VC), if required**
Date and Time for publication of clarification, if required	**https://nationalinsurance.nic.co.in, https://eprocure.gov.in/cppp, and https://gem.gov.in/**
Time and Date of Opening of PART-I (Pre-Qualification and Technical Bid)	**31-12-2025 at 3:30 PM**
Time and Date of Opening of PART-II (Commercial Bid)	**To be intimated later to Participating Bidders**
Place of Opening of both PARTs of the Bids	**IT Department** **National Insurance Company Ltd.** **Premises No.18-0374, Plot No. CBD-81, New Town, Kolkata-700156**
Date till which the Bid is valid	**1 (one) year from the date of opening of the Commercial Bids**
Address for all Communication, including **request for clarification**, if required	**To,** **Chief Manager - IT Department** **National Insurance Company Ltd.** **Premises No.18-0374, Plot No. CBD-81, New Town, Kolkata-700156** **Email: Satish.Kumar@nic.co.in** **Cc:** **Anurag.Gupta@nic.co.in , Abhishek.Pramanik@nic.co.in**
Bank Details of NICL Head Office **Name as per Bank Account : National Insurance Company** **Limited Bank Account Number : 6762010554** **Type of Account : Current Account** **Name of the Bank : Indian Bank**	

Name of the Branch	**: 5B, Russell Street, Kolkata - 700071**
MICR Number of the Branch	**: 700019018**
IFSC No. of the Branch	**: IDIB000R024**

- Bids documents must be received by NICL at the specified address not later than the time and date specified in the **Section - Important Dates and Information**. In the event of the specified date for the submission of Bids being declared a holiday for NICL, the bids will be received up to the appointed time on the next working day.
- NIC may, at its discretion, extend this dead-line for the submission of Bids, in which case all rights and obligations of NICL and Bidders previously subject to the deadline will thereafter be subject to the deadline as extended.
- **NICL's incumbent VAPT auditor, SOC/NOC providers, and technology support vendors are ineligible to participate in this tender.**
- Late Bids: Any bid received by NICL after the deadline for submission of bids prescribed by NICL will be rejected and returned unopened to the Bidder.
- Clarification of Bids: To assist in the examination, evaluation and comparison of bids the Purchaser may, at their discretion, ask the Bidder for clarification of the bid.
    - The Bidder should send their queries, if any, through email to satish.kumar@nic.co.in, C.C. anurag.gupta@nic.co.in, abhishek.pramanik@nic.co.in, on or before the stipulated date and time. Bidders should submit the queries only in the format given in the RFP and in xlsx format. Queries which are not in the format specified in the format will be ignored. Bid is liable for disqualification in case of deviation.
    - No query / suggestions will be entertained after the opening of the Commercial offer.
    - Clarifications will be published in NICL's Corporate Website https://nationalinsurance.nic.co.in, GeM portal: https://gem.gov.in/). No other modes of communication will be used. Intending Bidders should check the website frequently to get updates on any such changes. NICL reserves the right to cancel the RFP at any time without incurring any penalty or financial obligation to any Bidder or potential Bidder.

2. Table of Contents

3. Scope of Work

The selected bidder shall:

- Deploy tool-mapped skilled manpower, as per **details** below
- Ensure tool-specific OEM certification for engineers, wherever applicable.
- Assign Level-1 to Level-3 roles based on requirements defined in the RFP
- Maintain **100% manpower availability** with backups as per SLA.
- Integrate staff into NICL's governance model: daily reporting, weekly reviews, and monthly dashboards.
- Facilitate HLD, LLD, As-built and SOP documentation.

Table - A

3.1 Scope of Work: VAPT

Objective:

To onboard a CERT-In empanelled Information Security Auditing Organization with active credentials to conduct a comprehensive Vulnerability Assessment and Penetration Testing (VAPT) across NICL's infrastructure, applications, APIs, and cloud environments. The vendor must align assessments with IRDAI Information and Cyber Security Guidelines, 2023 (as updated March 24, 2025), NIST SP 800-115, OWASP Top 10, SANS 25, and other relevant global standards, including amendments of such standards, delivering a detailed remediation roadmap.

Scope Includes:

- **Network Penetration Testing:**
  - External and internal IP ranges, subnets, VPN concentrators, wireless networks (Wi-Fi, IoT devices), and DMZ segments.
  - Testing of network segmentation controls, firewall rulesets, and IDS/IPS evasion techniques.
  - Assessment of remote access protocols (e.g., RDP, SSH) for weak configurations.
  - Web and Mobile Application Security Testing.
  - Coverage of latest OWASP Top 10 (e.g., Injection, Broken Authentication), SANS 25 Critical Security Controls, and API-specific vulnerabilities (e.g., Broken Object Level Authorization, Excessive Data Exposure per OWASP API Security Top 10).
  - Testing of single-page applications (SPAs), progressive web apps (PWAs), and mobile app binary analysis (iOS/Android).
  - Assessment of DevSecOps pipeline integration for CI/CD security (e.g., SAST/DAST tool integration).

- **Configuration Review:**
  - Operating systems (Windows, Linux, macOS), network devices (routers, firewalls, switches, load balancers), and virtualized environments for misconfigurations, unpatched vulnerabilities, and deviations from CIS Benchmarks, DISA STIGs, and NIST 800-53.
  - Review of endpoint security agents, patch management systems, and backup configurations.

- **Gap Analysis:**
  - Mapping against ISO 27001:2022 (Information Security Management), ISO 22301 (Business Continuity Management), and IRDAI annexures, including identification of control deficiencies and prioritized remediation plans.

- **Cloud Security VAPT:**
  - Assessment of public , private, and hybrid cloud deployments, including VMs, storage buckets , Kubernetes clusters, serverless functions, and identity federation (e.g., IAM roles, OAuth).
  - Compliance with Cloud Security Alliance (CSA) CCM and ISO 27017 controls.

- **Security Baseline Checks:**
  - Implementation of CIS Benchmarks, DISA STIGs, and NIST 800-53 recommendations for system hardening, including password policies, logging configurations, and encryption standards.

- **Reporting and Remediation Support:**
  - Detailed technical report with CVSS v3.1 scores, risk classification (Critical, High, Medium, Low), and exploitability evidence.
  - Executive management summary with business impact analysis.
  - Post-remediation revalidation testing with a verification report and residual risk assessment.
  - On-demand knowledge transfer sessions for internal IT teams on identified vulnerabilities and mitigation techniques.

- **Fraud Blackbox Testing:**

  Two cycles annually for fraud monitoring as per IRDAI 2025 Fraud Framework, integrated with VAPT, with ad-hoc for fraud/high-risk releases.

- **Asset Coverage:**
  - IP Addresses in DC: 512
  - IP Addresses in DR: 512
  - IP Addresses in Sample Offices: 1024
  - Number of Cloud Instances: 1
  - Number of Applications: 12
  - Number of APIs: 134

- **Manpower Deployment Requirements:**

  The selected vendor shall deploy skilled, certified personnel in accordance with the manpower plan detailed below. Adequate backup resources must be identified to ensure **100% resource availability** as per defined SLA metrics. All team members must have a **minimum of 5 years of experience in the BFSI sector**, and relevant certifications as outlined. Curriculum Vitae (CVs) must be submitted in the prescribed format (Annexure XII).

Role	Minimum Count	Responsibilities	Certifications Required
Lead VAPT Analyst	2	Oversee VAPT execution, report preparation, remediation guidance	OSCP, CEH, CREST CRT, CISSP
Security Tester	4	Conduct network, application, and cloud VAPT	OSCP, eCPPT, CEH, GWAPT
Lead Auditor	2	Lead Cyber Security audits, ensure IRDAI compliance	CISA, ISO 27001 Lead Auditor, CRISC
Compliance Analyst	2	Map controls to standards, validate compliance	CISSP, ISO 22301 Lead Auditor, CISM
Forensic Investigator	1	Conduct forensic analysis, evidence collection	CHFI, GCFA, EnCE
Red Team Leader	1	Design and execute red team exercises	OSCE, CRTO, LPT Master, GPEN

Exploit Developer	1	Develop custom exploits for red teaming	OSWE, GXPN, OSEE

Note:

- All personnel must be **direct employees** of the vendor or long-term deputed staff with verifiable background checks.
- Subcontracting of key roles is not permitted without prior written approval from NICL.
- The deployed team should be able to coordinate with NICL's SOC/NOC and Application/Infra teams during assessment and remediation phases.
- Replacement of resources should follow the resource replacement clause as specified in **Resource Continuity Clause:**

- **VAPT Schedule and Timeline Matrix: The following VAPT delivery schedule shall be followed per application/batch:**

Phase	Deliverable	Max Duration
Discovery & Planning	Scope confirmation, asset list, stakeholder mapping	3 working days
Testing Window	Live VAPT / Red Teaming Execution	5-7 working days
Initial Report Submission	Draft report with vulnerabilities & PoC	3 working days post-testing
Re-test and Final Report	Confirm fixes, update risk posture	5 working days from fix confirmation
RCA + Risk Sign-off	Final RCA + Residual Risk Certificate	3 working days

3.2 Scope of Work: Independent Cyber Security (Assurance) Audit as per IRDAI Information and Cyber Security Guidelines, 2023 (as updated March 24, 2025) Guidelines

Objective:

National Insurance Company Limited (NICL) seeks to commission an independent Cyber Security audit, to be performed by a CERT-In empanelled Information Security Auditing Organization, to assess compliance with the Insurance Regulatory and Development Authority of India (IRDAI) Information and Cyber Security Guidelines, 2023 (as updated March 24, 2025). The audit shall provide a consolidated view of policy/process conformance, technical control effectiveness, and regulatory preparedness, including evidence-based findings and a remediation roadmap. The audit must validate the Cyber Crisis Preparedness Plan (CCMP), 6-hour incident reporting to both IRDAI and CERT-In, and Network Time Protocol (NTP) synchronization for logs.

Note: IRDAI Information and Cyber Security Guidelines, 2023 (as updated March 24, 2025)" – should not be misinterpreted as a new guideline year, as it's an update to 2023.

Scope Includes:

- Confirm alignment of NICL's security program with IRDAI Information and Cyber Security Guidelines, 2023 (as updated March 24, 2025) and related directions.
- Test design and operating effectiveness of key controls across people, process, and technology.
- Validate readiness for regulatory notifications (e.g., CERT-In and IRDAI within 6 hours) and log retention (at least 180 days).
- Identify control gaps, rate risk (High/Medium/Low), and provide an actionable remediation plan with owners and timelines.
- **Validate readiness for regulatory notifications** (e.g., CERT-In and IRDAI within 6 hours), log retention (at least 180 days) and NTP synchronization across log sources
    - **6-Hour Incident Reporting Compliance**

      Verify that NICL has documented and tested workflows ensuring incident reporting to IRDAI and CERT-In within 6 hours of detection, as mandated under Clause 6.3.1 of IRDAI Information and Cyber Security Guidelines, 2023 (as updated March 24, 2025). The auditor shall review:
        - Evidence of past incident reports,
        - Escalation matrix, and
        - Automation/alerting mechanisms to trigger compliance actions.
          Evidence of past incident reports,
    - **NTP Synchronization Across Logging Sources**
      Confirm that all security event sources — including but not limited to SIEM, firewalls, endpoint agents, cloud-native audit trails, and critical infrastructure logs — are synchronized using a reliable Network Time Protocol (NTP) source.
        - The audit shall include timestamp accuracy checks across logs to ensure forensic traceability.
- **Mandatory VAPT audit** as per IRDAI Information and Cyber Security Guidelines, 2023 (as updated March 24, 2025)
- **Mandatory Assurance audit** as per IRDAI Information and Cyber Security Guidelines, 2023 (as updated March 24, 2025), including a signed compliance certificate.
- **Cyber Crisis Preparedness Plan (CCMP) Validation**

- Validate the design and implementation of NICL's Cyber Crisis Preparedness Plan (CCMP) in accordance with IRDAI Information and Cyber Security Guidelines, 2023 (as updated March 24, 2025), and aligned with CERT-In CCMP Guidelines (2017, as updated 2023).This includes assessment of:
  - Defined roles and responsibilities across stakeholders.
  - Crisis communication protocols (internal and external).
  - Execution of simulation exercises and lessons learned integration.

- Intentionally Kept Blank
- **Board-Level Compliance Minutes**
  Confirm that **quarterly Cyber Security compliance reports and meeting minutes** have been submitted to NICL's Board of Directors, as per the updated Insurance Regulatory and Development Authority of India (IRDAI) Information and Cyber Security Guidelines, 2023 (as updated March 24, 2025)..
  The audit shall assess consistency, completeness, and traceability of Board communications related to Cyber Security posture, risks, and incident reports.

Scope of Systems, Locations, and Domains:

The scope is enterprise-wide and includes all data (in-transit and at-rest), information systems, networks, and third parties, as follows:

- Governance: Organization IS Policy (parent), ISRMC governance, ISF operations, Annexure A (Document Master List).
- Regulatory: Incident reporting timelines (CERT-In ≤6h; IRDAI ≤6h), RCA ≤14 days, regulatory disclosure workflow.
- Monitoring/Logging: SIEM coverage; ≥180-day online retention; immutability/WORM; legal hold; export hashing/manifests.
- Network & Perimeter: MBSS baselines (FW/IPS/WAF/VPN/ADC/DNS/DHCP), Entry-Point Register and approvals, WAF policies, network segmentation.
- Wi-Fi & Remote Sites: WPA3-Enterprise/802.1X (or WPA2-Enterprise AES fallback); PSK branches with unique ≥16-char PSKs, rotation every 90 days; guest SSID isolation; remote audits.
- Remote Work & RTO: ZTNA/VPN, MFA, device posture checks, Return-to-Office quarantine/VLAN and reintegration SOP evidence.
- Email/DNS & Endpoint: DMARC/SPF/DKIM enforcement (steady-state p=reject), DNS filtering resolvers and egress blocks, macro/VBA default-deny + ASR, EDR/AV posture.
- Email Security: Assess NICL's email gateway configuration for spoofing protections (SPF, DKIM, DMARC), and simulate phishing attacks with payload delivery success measurement.
- Cloud Security: Multi-tenant isolation, cloud audit trails, DR tests witnessed/approved, exit processes with deletion certificates, virtualization/MBSS hardening; regulator audit/inspection rights embedded in contracts.
- Application & SDLC: Pre-prod security gates (SAST/DAST/SCA, threat modeling), change control, version control, release documents with rollback, test data management (no real PII).
- Cryptography: In-transit and at-rest encryption, key lifecycle (activation/deactivation, cryptoperiods), HSM/KMS operations and dual control.
- **Third Parties:** Due diligence, security clauses, right to audit, regulator inspection allowances, termination (≤4h access revocation), data return and deletion certificates.

- The vendor shall conduct independent cybersecurity audits of NICL's third-party partners (including bancassurance partners, TPAs, intermediaries, and IT vendors) on a risk-based frequency:
  - High-risk partners: Quarterly
  - Medium-risk partners: Half-yearly
  - Low-risk partners: Annually
- Audits shall be performed independent of the partner's own VAPT/audit reports and shall include verification of compliance with NICL's security standards, review of any change in risk posture, and follow-up on previously reported non-compliances. Findings shall be presented to NICL's ISRMC with recommended actions.

- BCM/DR: Technology & network scope, utilization monitoring and capacity forecasting, joint DR tests/evidence, crisis governance.
- Physical & Environmental: Lightning protection (LPS/SPD), secure transit chain-of-custody, visitor/device controls.
- Dealing Room Operations: Secure recorded lines (SIP-TLS/SRTP) in office and WFH, voice logger governance and independent review, maker-checker (including disruption), MFA on financial terminals, VLAN segregation.
- API Security Testing: The selected vendor must conduct in-depth API security assessments to ensure secure integration and exposure of NICL's API infrastructure. Evaluate all external and internal API endpoints for vulnerabilities based on **OWASP API Security Top 10**, including but not limited to:
  - Broken Object Level Authorization (BOLA)
  - Excessive Data Exposure
  - Improper Asset Management
  - Broken Function Level Authorization
  - Verify enforcement of API-level security controls:
    - **Rate limiting, throttling**, and abuse protection mechanisms (e.g., spike arrest, circuit breakers)
    - **Token lifecycle** handling (secure generation, renewal, expiration, and revocation for OAuth, JWT, etc.)
    - Role/attribute-based access models (**RBAC/ABAC**), validating privilege enforcement across role
    - Ensure logging of access attempts, failures, and abuse patterns for integration with SIEM systems
- Container and Orchestration Security: Vendors are required to assess NICL's containerized environments for misconfigurations and security lapses.

  Audit security of container images using tools such as **Trivy, Clair**, and validate against **CIS Benchmarks**

  Test Kubernetes or equivalent orchestration environments for:

  - Insecure pod privileges or **hostPath mounts**
  - Insecure **RBAC**, namespace isolation, and unencrypted etc stores
  - Misconfigured **network policies**, service mesh exposure (e.g., Istio), and open ports

Validate runtime protection measures and assess lateral movement opportunities within the cluster

- Intentionally Kept Blank

Standards, Methodology and Practice:

The bidder shall adopt a **risk-based, industry-aligned audit methodology** for conducting independent Cyber Security audits at NICL, ensuring alignment with the following standards and best practices:The bidder shall adopt a risk-based, standards-driven methodology that ensures comprehensive coverage of Cyber Security and data protection controls. The assessment must be aligned with the following standards and frameworks:

- IRDAI Information and Cyber Security Guidelines, 2023 (as updated March 24, 2025).
- CERT-In auditing practices and advisories (updated October 2025).
- ISO/IEC 27001:2022 and ISO/IEC 27002:2022 (information security controls).
- NIST Cyber Security Framework (CSF) 2.0 (including Govern function).
- Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) v4.0.3.
- Digital Personal Data Protection Act (DPDP) 2023 (data privacy and breach notification).
- OWASP Testing Guide v4.2, CIS Benchmarks, and MITRE ATT&CK Framework for technical testing.
- Audit shall validate controls across ISO 27001:2022 (A.5-A.18), NIST CSF 2.0 functions (Identify, Protect, Detect, Respond, Recover, Govern), and CSA CCM v4.0.3 domains (e.g., GRM, AIS).

Audit Expectations

The audit shall:

- Validate **implementation and effectiveness** of controls across the domains listed above.
- Provide **clause-by-clause mapping** to standards and regulations in the final report (see Compliance Mapping Matrix).
- Identify **residual risks**, and propose **remediation plans** with risk prioritization (based on CVSS/CRR/NIST scores).
- Include **Board-level and regulator-ready** documentation for IRDAI, CERT-In, and Data Protection Board compliance.

Audit findings shall be mapped to regulatory and best-practice controls, with references to observed evidence, non-compliance, and recommendations for remediation. Testing will comprise documentation review, interviews/walkthroughs, configuration reviews, log analysis, sampling, and technical testing (internal/external VAPT, application security, and cloud configuration reviews).

Auditors may propose adjustments to sampling with NICL CISO approval, subject to risk justification.

Data Flow Threat Modelling

STRIDE-based threat model diagrams must be submitted for each app/audit, showing ingress/egress controls and data classification risks. The Vendor shall, as part of every VAPT or Audit engagement, deliver detailed data flow threat model diagrams. These shall be:

- Based on the STRIDE framework (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege).
- Include clear depiction of ingress and egress control points across the application stack and network.
- Reflect actual data classification risks at each stage of the data lifecycle (collection, transmission, processing, storage, archival).
- Serve as a visual aid in understanding systemic risks, privilege boundaries, and residual vulnerabilities.

The submission must be in presentation-ready format, included as an annexure to each audit/VAPT report, and may be used for internal InfoSec or Board-level reporting.

Technical Testing Components:

- External & Internal Vulnerability Assessment and Penetration Testing (VAPT).
- Application Security Testing: Web/mobile/API (OWASP Top 10, auth/session, business logic).
- Configuration & MBSS Review: Operating systems, middleware, databases, perimeter and security appliances.
- Cloud Posture Review: IAM controls, logging, encryption, networking, backup/DR, key management, workload baselines.
- Wi-Fi Assessment: Controller/AP configs, EAP methods, PSK controls, guest isolation, rogue detection.
- Email/DNS Controls: DMARC/SPF/DKIM alignment, DNS sinkhole/filtering effectiveness, egress restrictions.
- Logging/Immutability: SIEM ingestion completeness, 180-day online window validation, WORM/retention-lock controls, export hashing.
- Dealing Room Controls: Voice recording completeness and integrity checks, sampling for independent review, terminal MFA verification.

Coordination with SOC Team: Vendor must coordinate with NICL's SOC and internal Security Tools Team for activities such as:

- Evidence collection
- Exploit validation
- Detection logic tuning

Sampling & Evidence:

Minimum sampling shall be risk-based and include:

- Access Management: 25 privileged accounts; 2 cycles of periodic attestation; sample JML records.
- Change/Release: 20 change records across normal/emergency; 10 release packages with rollback evidence.
- Applications: **10** critical applications (internet-facing, internal, and cloud-hosted).
- IP Addresses: 128

- Endpoints & Branches: 100 endpoints across business units; 10 branches/sites for Wi-Fi/remote audit evidence.
- Third Parties: 7 critical providers (contracts, due-diligence, exit evidence).
- Cloud Workloads: 5 priority workloads for DR test evidence and logging coverage.
- Incidents: Last 7 High/Medium incidents (classification, notification, RCA, lessons learned).
- Logs: 12 log sources (firewall, VPN, EDR, AD, WAF, DNS, cloud audit, app/API, DB etc) to prove 180-day online retention and immutability.

Deliverables & Milestones:

- Inception Report & Audit Plan (scope, schedule, sampling strategy) in word and pdf.
- Daily/Weekly Status & Observation Log (with tracker IDs, owner, target date).
- Interim Technical Findings (critical/high issues with immediate recommendations).
- Asset Classification-Based Reporting: "Vulnerabilities and threats must be classified as per asset criticality:
    - High (Mission-critical / Customer-facing)
    - Medium (Internal-facing systems)
    - Low (Support utilities)
- IRDAI Mapping Matrix (clause-by-clause compliance view).
- Draft IRDAI Assurance Audit Report (executive summary, methodology, domain-wise findings, risk ratings, evidence).
- Remediation Plan (owner, action, target date) and Quick-Wins list.
- All evidence (logs, screenshots, exploit chains) gathered during Red Teaming must be securely retained for **3 years**, and made available to NICL, CERT-In, or IRDAI upon request.
- Final Audit Report with Management Responses, and Closure Validation Plan (re-test scope).
- DPDP Act 2023 Compliance: Assess alignment with Digital Personal Data Protection Act 2023 for data handling, consent management, and breach notification.
- All reports (audit, VAPT, RCA) must use formats compliant with CVSS v3.1, MITRE ATT&CK, OWASP, STRIDE, NIST CSF unless specified as per the regulator mandated format.
- Board Presentation Deck: Deliver a 10-15 slide deck summarizing audit findings, heatmaps, and strategic recommendations for Board review.

Compliance Mapping Matrix:

Compliance Mapping Matrix (Updated as per IRDAI Information and Cyber Security Guidelines, 2023 (as updated March 24, 2025) and NIST CSF 2.0)

The vendor shall deliver a detailed Compliance Mapping Matrix as part of the audit report, mapping NICL's security controls to IRDAI Information and Cyber Security Guidelines, 2023 (as updated March 24, 2025), ISO/IEC 27001:2022, NIST CSF 2.0, CSA CCM v4.0.3, and the DPDP Act 2023. This matrix shall include clause-wise compliance status, mapped evidence, and specific remediation actions wherever applicable.

- **IRDAI Information and Cyber Security Guidelines 2023** (including updates dated **March 24, 2025**)
- **ISO/IEC 27001:2022** and **ISO/IEC 27002:2022**
- **NIST Cyber Security Framework (CSF) 2.0**
- **Cloud Security Alliance (CSA) CCM v4.0.3**

- **Digital Personal Data Protection (DPDP) Act, 2023**

The matrix must include:

- **Clause/Control Reference** from the relevant standard
- **Description** of the requirement/control
- **NICL's Compliance Status**: *Compliant*, *Partial*, or *Non-Compliant*
- **Evidence**: Supporting documentation, logs, configurations, reports, etc.
- **Remediation Plan** (if applicable): Clearly defined mitigation activities, owners, and timelines

Format: The matrix must be delivered in **editable Excel (.xlsx)** format and embedded in the **Final Audit Report**. It should be suitable for **Board-level compliance reporting** and support tracking by the NICL CISO team.

Coverage Requirements:

- IRDAI Clauses updated as of March 24, 2025 (e.g., time sync, SOC audit trail, forensic expert empanelment, cyber insurance validation)
- ISO 27001:2022 (Annex A controls A.5–A.18)
- NIST CSF 2.0 functions: *Identify, Protect, Detect, Respond, Recover, Govern*
- CSA CCM v4.0.3 domains including GRM, AIS, IVS, SEF
- DPDP Act 2023 Sections 4–9 (obligations, notice, consent, breach reporting, data principal rights)

Standard/Regulation	Clause/ Control	Description	NICL Compliance Status	Evidence	Remediation (if needed)
IRDAI Information and Cyber Security Guidelines, 2023 (as updated March 24, 2025)	Clause 3.1.6	Annual Cyber Security audit	Compliant	Signed compliance certificate, audit report	N/A

IRDAI Information and Cyber Security Guidelines, 2023 (as updated March 24, 2025)	Clause 4.4.1	Annual VAPT with remediation	Partial	VAPT report with CVSS scores	Complete remediation by Q1 2026
IRDAI Information and Cyber Security Guidelines, 2023 (as updated March 24, 2025)	Clause 5.2.5	Third-party due diligence	Compliant	Vendor contracts, SOC 2 reports	N/A
IRDAI Information and Cyber Security Guidelines, 2023 (as updated March 24, 2025)	Clause 6.2.1	Security awareness training	Partial	Training logs, phishing simulation results	Achieve <5% click-rate by Q2 2026
IRDAI Information and Cyber Security Guidelines,	Clause 6.2.2	Cyber Crisis Preparedn	Partial	CCMP document, simulation logs	Conduct quarterly simulations by Q3 2026

2023 (as updated March 24, 2025)		ess Plan (CCMP)			
IRDAI Information and Cyber Security Guidelines, 2023 (as updated March 24, 2025)	Clause 6.3.1	6-hour incident reporting to IRDAI/CERT-In	Compliant	Incident response logs, notification records	N/A
ISO/IEC 27001:2022	A.18.2.1	Independent review of information security	Compliant	Audit reports, peer review documentation	N/A
ISO/IEC 27001:2022	A.14.2.8	System security testing	Partial	VAPT findings, security testing results	Address high/critical vulnerabilities
NIST CSF 2.0	GV.OC-05	Independent Cyber Security assessments	Compliant	External audit reports	N/A

NIST CSF 2.0	PR.PS-07	Security testing controls (Protect Function)	Partial	Penetration test results	Revalidate post-fixes
CSA CCM v4.0.3	GRM-02	Governance risk management reviews	Compliant	Governance meeting minutes, risk dashboards	N/A
CSA CCM v4.0.3	AIS-04	Application security testing	Partial	SAST/DAST reports	Enhance CI/CD integration
DPDP Act 2023	Section 8	Data breach notification within mandated timeline	Compliant	Incident logs, breach notification tracker	N/A
IRDAI Information and Cyber Security Guidelines, 2023 (as updated March 24, 2025)	Clause 4.7.1	Time sync across all systems using NTP	Compliant	NTP audit logs, sync configuration files	N/A

IRDAI Information and Cyber Security Guidelines, 2023 (as updated March 24, 2025) 2023 (2025 Update)	Clause 6.5.3	Empanelment of forensic experts	Partial	Empanelment letters, vendor onboarding docs	Empanel top 3 CERT-In certified forensic vendors

Note:

- *The matrix must be submitted in **editable Excel format** as part of the **Final Audit Report**.*
- *It shall serve as the basis for **Board-level Cyber Security compliance tracking**.*
- *Vendor must ensure inclusion of **additional IRDAI clauses added in March 2025**, including those related to:*
    - *Time synchronization (Clause 4.7.1),*
    - *Forensic expert empanelment (Clause 6.5.3),*
    - *Enhanced breach notification procedures and threat-sharing mechanisms (Clauses 6.3.2, 6.4).*

Quarterly Executive Risk Summary Reporting for Board Consumption:

The selected vendor shall prepare and submit a **Quarterly Board-Level Executive Risk Summary Report** in a **presentation-ready format**. This report shall include:

- An executive summary of the prevailing **cyber threat landscape**, including trends and sector-specific insights.
- **Heatmaps** and **risk severity visualizations**, including risk rating timelines, trend analysis, and exposure deltas.
- Summarized findings from **Red Team** engagements conducted during the quarter.
- Highlighted risks that require **Board-level intervention**, funding, or strategic decisions.
- Summary of **remediation efforts** and **overdue items**.
- The format shall follow best practices for Board reporting. Reports are to be delivered in both editable document and slide format to support presentation during internal governance reviews.
- Residual Risk Reporting: Residual Risk Report with CVSS re-score, RCA, compensating control identification, and sign-off from concerned NICL business owner

Note: Remediation Support Workshops:

- *At least **2 workshops per VAPT/Audit cycle**:*
    - *RCA (Root Cause Analysis)*
    - *Tool replay and retesting*
    - *Guidance for mitigation*
    - *To be conducted within 10 working days post report submission*

Suggested timeline (indicative, to be finalized in Inception):

- T0: Kick-off, logistics, access, and audit plan sign-off.
- T+5 business (working days of NICL) days: Discovery completed.
- T+6 to T+20: Fieldwork (testing, walkthroughs, evidence).
- T+21 to T+25: Analysis & mapping; management debrief.
- T+26: Draft report submission.
- T+30: Final report (post management responses).
- Within 30–60 days of final: Re-test/closure validation (in-scope fixes).

Acceptance Criteria:

- Completeness: All in scope domains and samples covered; IRDAI clause mapping provided.
- Evidence: Screenshots/config dumps/log extracts with timestamps; reproducible steps.
- Severity & Risk: Findings rated (High/Medium/Low) with business impact and likelihood.
- Actionability: Remediation steps, owners, and target dates documented; quick-wins identified.
- Quality: Logical consistency; peer review by bidder; executive summary fit for Board/ISRMC.

Constraints, Assumptions & Out of Scope:

- Vendors must sign an NDA for handling sensitive data (e.g., logs, PII samples).
- All evidence must be encrypted during transfer (e.g., AES-256) and retained for 3 years per IRDAI requirements.

Assumptions: Timely access to environments, documents, SMEs and test windows, read only access for configuration/log review, safe test windows for VAPT.

Out-of-Scope (unless specifically authorized in writing):

- Denial of Service or destructive testing in production.
- Unapproved social engineering or phishing against employees/customers.
- Code changes or production deployments by the bidder.
- Data exfiltration or use of real customer PII beyond approved sampling windows.

3.3 Scope of Work: Red Teaming Services

Objective:
To simulate real-world Advanced Persistent Threat (APT) attacks using the MITRE ATT&CK framework, evaluating the NICL's cyber resilience, detection capabilities, and response effectiveness, with a focus on BFSI-specific threats.

Rules of Engagement (RoE)

The vendor shall submit a detailed RoE document before initiating red team exercises, to be approved by NICL's CISO.

RoE must define:

- Authorized testing scope (e.g., specific IPs, applications, departments).
- Prohibited actions (e.g., no production data deletion, no unapproved DoS).
- Consent for social engineering (e.g., employee-signed agreements for phishing).
- Notification protocols for critical findings (e.g., immediate escalation to SOC).

Physical penetration testing requires written approval from NICL's Facilities Head and must comply with Indian Penal Code provisions

Scope Includes:

- Adversary Simulation:
  - Emulation of TTPs from MITRE ATT&CK (e.g., Initial Access, Persistence, Lateral Movement) using tools like Cobalt Strike and Metasploit Pro.
  - Simulation of nation-state or ransomware group TTPs relevant to the BFSI sector.
  - The vendor should use current threat intelligence sources (CERT-In, ISACs, MISP, etc.) to emulate realistic threats.
  - Red Team operations shall be designed in alignment with recent threat intelligence received from CERT-In, FS-ISAC, and industry-specific advisories to simulate real-world APT actors (e.g., APT38, Lockbit).
- Social Engineering:
  - Phishing campaigns (spear-phishing, vishing), pretext calls, and bait media drops (e.g., infected USBs) targeting employees.
  - Assessment of security awareness training effectiveness.
  - The vendor shall obtain **prior written consent** from all NICL employees who are proposed to be targeted during red teaming engagements involving social engineering techniques such as simulated phishing, vishing, baiting, USB drops, etc.
  - Consent shall be recorded using a **standardized consent form**, approved by NICL, and compliant with the **Indian IT Act, 2000**, **IT Rules 2021**, and **DPDP Act 2023**.
  - The form must clearly inform the employee of the nature, purpose, and limitations of the test, and be signed **prior to initiation of the test**.
  - All signed forms shall be **submitted to the NICL CISO** before test commencement.
  - A template for the consent form is provided in **Annexure XIII**..
- Physical Penetration Testing:
  - Facility infiltration, camera and access control evasion, and testing of physical security controls (e.g., badge cloning, tailgating).
- Data Exfiltration Simulation:
  - Testing of Data Loss Prevention (DLP) systems, network segmentation, and encryption controls during simulated exfiltration attempts.
  - Validation of backup integrity and ransomware resilience.

- Simulated Attacks:
  - Targeted attacks on high-risk departments (e.g., Investment, Finance, IT, HR) to test security awareness and incident response.
  - Evaluation of SIEM/SOC mean-time-to-detect (MTTD) and mean-time-to-respond (MTTR).
- Blue Team Assessment:
  - Red vs. Blue engagement followed by purple teaming to refine detection rules, improve defensive controls, and document lessons learned. Ensure mandatory documentation of all improvements made to alerting and detection logic.

*Note: **Red Teaming Learnings – Purple Team Output***

*For every Red Teaming engagement, the vendor shall deliver documented **Purple Team learnings** by working in collaboration with NICL's Blue Team (SOC/NOC). These learnings should include:*

- ***Improvement of detection logic** in correlation rules and SIEM dashboards.*
- ***Tuning of existing alerting rules** to improve Mean Time to Detect (MTTD).*
- ***Adversary simulation coverage report**, detailing tactics and techniques mimicking real-world APTs (e.g., **APT38**, **FIN7**, **LockBit** ransomware chain).*
- ***Validation of log sources and telemetry** across endpoint, network, and cloud layers to ensure completeness and visibility.*
- *The Vendor must share the final output as a **Purple Team Report**, highlighting Blue Team improvements, residual detection gaps, and strategic recommendations for defense hardening.*

Note: Red Teaming (addition)

- *Red Teaming exercises, particularly those simulating ransomware, credential harvesting, or lateral movement, must be aligned with **IRDAI Information and Cyber Security Guidelines, 2023 (as updated March 24, 2025)** requirements for engaging **pre-empanelled forensic experts**.*
- *The simulation environment, logging artefacts, and exploit chains must support **forensic readiness assessments**, including log integrity, time synchronization, and audit trail completeness.*
- *Red Teaming results must directly **feed into the Cyber Crisis Preparedness Plan (CCMP)** validation process and include actionable inputs for periodic updates to CCMP.*
- *The final Red Teaming Report must include a **Forensic Simulation Log Summary**, to be shared with NICL's Incident Response and SOC Teams*

3.4 Required Certifications for Vendor Manpower

The vendor's deployed personnel must possess valid and verifiable certifications aligned with their designated service domain, ensuring subject-matter expertise across all service areas — VAPT, Cyber Security audits, digital forensics, and red teaming exercises.

Certification Matrix

Service Domain	Role	Required Certifications* (Please see Note below the table)	Compliance (Yes/No)
VAPT	Lead VAPT Analyst	OSCP, CEH, CREST CRT, CISSP	
VAPT	Security Tester	OSCP, eCPPT, CEH, GWAPT	
Audit	Lead Auditor	CISA, ISO 27001 Lead Auditor, CRISC, CIA	
Audit	Compliance Analyst	CISSP, ISO 22301 Lead Auditor, CISM	
Forensics	Forensic Investigator	CHFI, GCFA, EnCE, CFCE	
Forensics	Malware Analyst	GREM, GCFA, GCFE	
Red Teaming	Red Team Leader	OSCE, CRTO, LPT Master, GPEN	
Red Teaming	Exploit Developer	OSWE, GXPN, OSEE	

***Note**:*

- *At least **75%** of the vendor's deployed resources must hold one or more of the required certifications relevant to their assigned role.*
- *All personnel must possess **a minimum of 5 years' experience in BFSI or regulated sectors**, including previous assignments of similar scale.*
- ***CVs and experience summaries** must be submitted in the format defined in **Annexure XII**, with necessary documentary proof for audit.*

3.5 Tools Required by Service Domain

The vendor must possess and utilize the following proven and industry-standard (NIST SP 800-115 CIS Benchmarks, CERT-In Guidelines) tools to ensure high-quality service delivery across Vulnerability Assessment & Penetration Testing (VAPT), Cyber Security Audit, Forensics, and Red Teaming domains. The use of licensed versions is mandatory where applicable, and proof of licensing must be submitted as part of the technical bid. Tools may be open-source or commercial but must be demonstrably effective.

Service Domain	Tool Name	Tool Type	Purpose / Use Case	Compliance (Yes/No)

VAPT	Burp Suite Pro	Licen sed	Web Application Security Testing	
VAPT	Nessus Pro	Licen sed	Network Vulnerability Scanning	
VAPT	Nmap	Free ware	Network Discovery & Port Scanning	
VAPT	Nikto	Free ware	Web Server Vulnerability Scanning	
VAPT	Metasploit	Free ware	Exploitation Framework	
VAPT	Acunetix	Licen sed	Automated Web Vulnerability Scanning	
VAPT	Trivy	Free ware	Container Image Vulnerability Scanning	
Audit	Qualys Compliance Suite	Licen sed	Compliance Scanning & Benchmarking	
Audit	Rapid7 InsightVM	Licen sed	Vulnerability Management	
Audit	OpenVAS	Free ware	Network Vulnerability Scanning	

Audit	CIS-CAT Pro	Free ware	Configuration Assessment (CIS Benchmarks)	
Audit	Nessus Compliance	Licen sed	Audit-Specific Compliance Checks	
Forensics	FTK Imager	Licen sed	Forensic Disk Imaging	
Forensics	Autopsy	Free ware	GUI-based Forensic Analysis	
Forensics	Volatility	Free ware	Memory Forensics & RAM Analysis	
Forensics	EnCase	Licen sed	Digital Forensics & Evidence Collection	
Forensics	Magnet AXIOM	Licen sed	Mobile & Cloud Forensics	
Red Teaming	Cobalt Strike	Licen sed	Adversary Emulation	
Red Teaming	Metasploit Pro	Licen sed	Penetration Testing & Exploit Development	
Red Teaming	Empire	Free ware	PowerShell-based Post-Exploitation	

Red Teaming	BloodHound	Free ware	Active Directory Enumeration	
Red Teaming	Mimikatz	Free ware	Credential Dumping	

Note:

- *Tools mentioned here represent a baseline. Vendors may propose additional tools that enhance capability, provided they adhere to NICL's data handling and security requirements.*
- *Custom/internal tools can be used with prior approval of NICL. All tools should be compliant with Data Residency requirements of the DPDP,2023 Act.*
- *Vendors must demonstrate proficiency in the above tools either via submission of past sanitized project reports or live demos during the bid evaluation phase.*

3.6 Table 1: SLA (Service Level Agreement) Metrics by Service Type

The vendor shall adhere to the following Service Level Agreement (SLA) metrics to ensure timely and effective delivery of Vulnerability Assessment and Penetration Testing (VAPT), Cyber Security Audit, Red Teaming, Forensic Services, and Training. Penalties apply for breaches exceeding 10% of target timelines, with evidence required for compliance verification.

Service	SLA Parameter	Target	Remarks	Penalty Clause (Y/N)	Evidence Required
VAPT	Initiation after request	Within 5 working days	Post asset list finalization and contract signing	Y (Rs. 5000/- per day of delay)	Signed work order, discovery phase report
VAPT	Report submission post-assessment	Within 10 working days	Includes preliminary and final reports with CVSS v3.1 scores	Y (Rs. 5000/- per day of delay)	Technical report, executive summary
VAPT	Revalidation testing after fixes	Within 7 working days of request	Post mitigation confirmation by NICL	Y (Rs. 5000/- per day of delay)	Revalidation report, residual risk assessment

Cyber Security Audit	Compliance audit coverage	100% of scoped systems annually	Covers IRDAI-mandated scope (e.g., CCMP, 6-hour reporting)	Y (Rs. 10,000/- per day of delay)	Compliance Mapping Matrix, signed certificate
Cyber Security Audit	Draft report delivery	Within 15 working days of audit completion	Preliminary draft for NICL review	N	Draft report (Word/PPT)
Cyber Security Audit	Final report submission	Within 5 working days of NICL feedback	Incorporates NICL comments and board-ready deck	Y (Rs. 10,000/- per day of delay)	Final report, board presentation (10–15 slides)
Red Teaming	Tabletop exercise execution	Quarterly (within 5 working days of quarter start)	Simulated engagement for awareness and CCMP validation	N	Tabletop exercise report, lessons learned
Red Teaming	Full red team assessment	Twice a year (within 10 working days of scheduled start)	APT-style emulation with MITRE ATT&CK TTPs	Y (Rs. 7500/- per day of delay)	Red team report, purple teaming debrief
Red Teaming	Debrief and mitigation walkthrough	Within 10 working days of exercise completion	Includes SOC purple teaming and RoE review	N	Debrief slides, mitigation plan
Training	Initial training completion	Within 30 days of engagement	Covers all employees, prioritized for high-risk departments	Y (Rs. 7500/- per day of delay)	Training logs, completion certificates
Training	Quarterly refresher training	Within 5 working days of quarter start	Includes phishing simulation results (<5% click-rate target)	Y (Rs. 7500/- per day of delay)	Effectiveness report, pre/post-assessment scores

Training	Training effectiveness reporting	Within 7 working days post-training	Measures awareness improvement (80% pass rate target)	Y (Rs. 7500/- per day of delay)	Quarterly report with metrics

Notes:

- *Vendors must submit monthly SLA compliance reports to NICL's CISO, including supporting evidence (e.g., logs, reports).*
- *Penalties are cumulative per breach instance and capped at 20% of contract value per service.*
- *All timelines are measured in working days (Monday–Friday, excluding public holidays).*
- *SLA breaches trigger escalation as per Section 3.9: Escalation Matrix.*

3.7 Table 2: Frequency of Each Service

Service	Activity Type	Frequency	Regulatory/Best Practice Reference:
VAPT	Network VAPT	Twice a year	IRDAI Information and Cyber Security Guidelines, 2023 (as updated March 24, 2025), Clause 4.4.1
VAPT	Application VAPT	After every major release OR twice a year	IRDAI Clause 4.4.2; OWASP Testing Guide v4.2
VAPT	Cloud Infrastructure VAPT	Twice a year	NIST CSF 2.0 (PR.PS-07); ISO 27017; CSA CCM v4.0.3 (AIS-04)
VAPT	Ad-hoc VAPT**	Post-significant incidents (as needed)**	CERT-In Best Practice; IRDAI Clause 6.2.2
	***Ad-hoc ethical hacking engagements (e.g., for high-severity incidents or post-deployment vulnerabilities) shall be triggered by NICL CISO request, with the vendor deploying certified ethical hackers (e.g., OSCP/CEH qualified) within 48 hours. Scope includes targeted black-box testing, exploit validation, and remediation recommendations, at a fixed rate per engagement (quoted in Commercial Bid, Section 7)*		
Audit	Security Compliance Audit	Annually	IRDAI Clause 3.1.6; ISO 27001:2022 (A.18.2.1), *(Annexure-V , Certificate on Cyber Security Controls is a deliverable)*

Audit	Configuration and Patch Review Audit	Half-yearly	IRDAI Clause 3.1.6; CIS Controls v8
Audit	Third-Party Hosted Systems Audit	Annually	IRDAI Clause 5.2.5; NIST CSF 2.0 (ID.SC)
Forensics	Forensic Readiness Check	Annually	NIST SP 800-86; IRDAI Clause 6.2.2
Red Teaming	Tabletop Simulation Exercise	Quarterly	IRDAI Clause 6.2.2 (CCMP); MITRE Engage Framework
Red Teaming	Full Red Team Engagement	Twice a year	NIST SP 800-115; MITRE ATT&CK Framework
Training	Security Awareness Training	Quarterly	IRDAI Clause 6.2.1; NIST CSF 2.0 (PR.AT)

Notes:

- *Frequencies are aligned with **SLA metrics** (Section 3.6) and **Payment Milestones** (Section 7.1).*
- *VAPT cycles (twice yearly) shall cover **all assets** – network, applications, cloud – as defined in Section 3.1.*
- ***Ad-hoc VAPT** to be initiated **after major incidents**, which must be reported within **6 hours** as per **IRDAI Clause 6.3.1**.*
- *Forensic readiness and Red Team engagements are integral to the **Cyber Crisis Management Plan (CCMP)** requirements.*
- *VAPT to be conducted for all changes to internet facing information assets or systems and reported gaps should be closed before moving into production.*
- *Business applications including APIs or Web Services etc. to undergo VAPT Testing including secure code review periodically & before going live.*
- *External Blackbox Penetration Testing (PT) to be conducted for all internet facing information assets and systems once in 6 months.*
- *Business applications including APIs or Web Services etc. to undergo Security Audit, VAPT Testing including secure code review periodically & before going live.*

3.8 Training and Awareness

To complement the technical services provided by the vendor, it is recommended to mandate vendor-led security awareness training for employees. This initiative will enhance the organization's human firewall, reduce the risk of social engineering attacks, and align with IRDAI Information and Cyber Security Guidelines, 2023 (as updated March 24, 2025) Clause 6.2.1 (Security Awareness and Training).

Detailed Components:

- **Training Scope:**

  - **Target Audience:**

  All employees, with specialized sessions for high-risk departments (e.g., Investment, Finance, IT, HR).

  - **Topics Covered:**
    - Phishing identification and response (e.g., email spoofing, vishing).
    - Password hygiene and multi-factor authentication (MFA) best practices.
    - Safe handling of USBs, external devices, and cloud storage.
    - Incident reporting procedures and escalation protocols.
    - Overview of VAPT findings and remediation relevance to employees.

  - **Delivery Methods:**

  In-person workshops, e-learning modules, and simulated phishing exercises.

- **Training Frequency:**
  - Initial onboarding training within 1 month of vendor engagement.
  - Quarterly refreshers, aligned with Red Teaming tabletop exercises (Section 7).
  - Ad-hoc sessions post-significant incidents or VAPT findings.

- **Vendor Responsibilities:**
  - Design and deliver customized training content tailored to BFSI operations.
  - Provide certified trainers (e.g., with CEH or equivalent certifications).
  - Conduct pre- and post-training assessments to measure awareness improvement (target: 80% pass rate).
  - Supply training materials (e.g., handouts, videos) and a completion certificate for each participant.

- **Metrics and Reporting:**
  - Track participation rate (target: 100% attendance).
  - Measure reduction in phishing click-through rates during simulated exercises.
  - Submit a quarterly training effectiveness report to NICL's CISO, CTO.
  - Integration with Red Teaming:
  - Use insights from social engineering campaigns (Section 3) to tailor training content.
  - Conduct follow-up training within 2 weeks of a failed phishing simulation to address gaps.

Actionable Steps:

- Appoint an internal training coordinator to liaise with the vendor and track compliance.
- Escalation should be followed by RCA.

3.9 Escalation Matrix

To ensure timely resolution of SLA breaches, incident response delays, or other critical issues, a detailed Escalation Matrix is recommended. This matrix will define roles, contact points, and timelines for escalating concerns, ensuring accountability and swift action.

Detailed Components:

- **Escalation Levels:**

  - **Level 1: Operational Team (0-2 hours):**
    - Contact: Vendor's Project Manager or Technical Lead.
    - Responsibility: Address minor SLA delays (e.g., report submission overdue by <2 days) or initial incident response.
    - Contact Method: Email (response within 2 hours) or 24x7 hotline.

  - **Level 2: Management Team (2-12 hours):**
    - Contact: Vendor's Account Manager or Delivery Head.
    - Responsibility: Resolve moderate issues (e.g., SLA breach >2 days).
    - Contact Method: Phone call or video conference (response within 4 hours).

  - **Level 3: Senior Leadership (12-24 hours):**
    - Contact: Vendor's CEO or Regional Director.
    - Responsibility: Handle escalations or legal/compliance risks.
    - Contact Method: Immediate phone call and written notice (response within 12 hours).

  - **Level 4: Organization's CISO/Board (24+ hours):**
    - Contact: Organization's CISO and vendor's legal counsel.
    - Responsibility: Escalate to terminate contract or invoke penalty clauses if unresolved.
    - Contact Method: Formal letter and legal notice.

- **Trigger Conditions:**
  - SLA breaches exceeding 10% of the target timeline (e.g., VAPT initiation delayed).
  - Failure to deliver critical reports within RFP mandated timelines.
  - Detection of vendor non-compliance with CERT-In or IRDAI standards.

- **RCA:**
  - The vendor will submit a root cause analysis (RCA) report within 48 hours of Level 2 escalation.

- **Documentation and Tracking:**
  - Maintain a log of all escalations, including timestamps, actions taken, and outcomes.
  - Share a monthly escalation summary with the organization's Risk Management Committee.

3.10 Points of Contact for Cyber Security Audit:

- **IT Security Team (IS Team):** Oversee Implementation and training coordination
  - Conduct a kick-off meeting with the vendor to review the matrix and assign contacts.
  - Develop an escalation matrix document and include it as an annexure in the vendor contract.
  - Set up an internal escalation monitoring dashboard to track incidents in real-time.

- **Points of Contact for Cyber Security Audit:**
  - NICL: CISO (Sponsor), IS Team (SOC) - Coordinator, SOC Lead, CITSO, CTO, GM-IT, Ops, GM-Enterprise Risk, Chief Compliance Officer, Investment (Dealing Room Head).
  - Bidder: Engagement Partner/Director, Lead Auditor, Technical Lead, Cloud Lead, Report Coordinator.

3.11 Appendix A: Clauses

Secure Code Review:

- Perform Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) using licensed tools such as Fortify SCA, Checkmarx, or equivalent.
- Perform Dynamic Application Security Testing (DAST) using tools such as Burp Suite Pro or AppScan.
- Ensure source code analysis covers common issues like injection flaws, insecure cryptography, and hardcoded credentials.
- Include secure code review as part of CI/CD pipeline wherever DevSecOps is implemented.
- Deliver findings with CWE IDs and severity using CVSS v3.1 scores.

Cloud VAPT with CSPM:

- Include CSPM checks using licensed tools like Prisma Cloud, AWS Security Hub, Azure Security Center, or GCP Security Command Center.
- Assess misconfigurations in IAM policies, security groups, storage buckets, and other cloud-native resources.
- Map findings to CSA CCM, NIST 800-53, and ISO 27017/27018 requirements.
- Include a visual cloud security heatmap and prioritized remediation plan.

Zero Trust Testing:

- Test access control policies on APIs and internal apps for least privilege enforcement.
- Validate session management, token refresh, and expiration mechanisms.
- Conduct abuse testing for API rate limiting, authentication bypass, and JWT manipulation.
- Ensure alignment with NIST Zero Trust Architecture (SP 800-207).

***Note:** The Vendor shall ensure the inclusion of **Zero Trust Architecture (ZTA)** principles as part of the application, API, and cloud security assessments. The scope of testing must mandatorily cover the following advanced areas:*

- ***Token Lifecycle Management**: Evaluate the entire lifecycle of access tokens and refresh tokens (e.g., JWT, OAuth), including token expiration, renewal, revocation mechanisms, and secure storage practices.*
- ***API Rate Limiting and Abuse Detection**: Assess rate limiting protections, spike arrest configurations, and API gateway thresholds to detect abuse or denial-of-service vectors.*
- ***Access Control Models**: Validate enforcement of fine-grained access controls using:*
  - ***Role-Based Access Control (RBAC)** – role hierarchy, privilege escalation paths*
  - ***Attribute-Based Access Control (ABAC)** – context-aware, claim-based, or policy-driven access conditions*
- ***Header and CORS Configuration Review**:*

- *Detection of **misconfigured or missing HTTP security headers**, including Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, etc.*
- *Validation of **Cross-Origin Resource Sharing (CORS)** policies to identify over-permissive configurations that allow cross-domain data leaks or abuse.*

*These tests shall be applicable across internet-facing and internal APIs, especially those used in customer journeys, partner integrations, and mobile applications. The vendor must use **automated and manual techniques** to simulate attacker TTPs, aligned with OWASP API Top 10, OWASP MASVS, and MITRE ATT&CK Framework.*

Phishing Simulation Clause:

- Vendor to conduct quarterly phishing simulations targeting various departments.
- Report click-through rates and aim for <5% within a quarter.
- Assist in profiling user risk and recommend tailored awareness campaigns.

Note: Phishing Simulation and User Awareness Enhancement

*The Vendor shall design and conduct a structured **Phishing Simulation & Awareness Program** as part of the Cyber Security services provided to NICL. This initiative aims to assess and enhance employee resilience against social engineering threats and will include the following minimum deliverables:*

- ***Quarterly Phishing Campaigns**: Execute **one phishing simulation per quarter**, covering various templates and complexity levels, including business email compromise (BEC), credential harvesting, and malicious attachments.*
- ***Click-Through Rate Targets**: The goal is to achieve a **click-through rate of less than 5%** across NICL employees within **two consecutive quarters** of campaign rollout.*
- ***User Risk Profiling**:*
  - *Maintain anonymized records of user response patterns (e.g., clicks, credentials entered, reporting behavior).*
  - *Generate **risk profiles for users/departments** based on susceptibility to phishing.*
  - *Use these profiles to **deliver tailored awareness interventions** (e.g., custom emails, short videos, tooltips, LMS-based microlearning modules).*
- ***Dashboard & Reporting**:*
  - *Provide executive dashboards showing campaign participation, risk segments, and improvements over time.*
  - *Submit quarterly reports summarizing campaign metrics, targeted training impact, and reduction trends.*
- ***Integration with Cyber Hygiene Programs**: Coordinate the phishing awareness efforts with ongoing NICL Acceptable Usage, Cyber Hygiene, and DPDP sensitization initiatives.*

Remediation Workshops:

- Conduct at least two remediation support workshops per audit/VAPT cycle for IT and Dev teams.
- Workshops should include walkthroughs of findings, secure design principles, and code-level fix demonstrations.
- Submit a formal RCA report identifying root causes and misconfigurations.

- Provide residual risk validation and verification report post remediation.

Chain of Custody:

- Should ensure audit to validate chain-of-custody logs, log retention, and secure evidence handling procedures.

Red Team Adversary Simulation:

- Vendor to ensure BFSI-relevant APT actor simulations like FIN7, APT38, Conti, etc.
- Red vs. Blue engagements must result in documented purple team takeaways and updated detection logic.

Tools:

- All tools listed must be licensed (where applicable), updated, and the vendor must ensure validity throughout engagement.
- Custom tools require prior written approval from NICL.

Resource Continuity Clause:

- At least 80% of proposed technical team members must remain unchanged throughout the engagement.
- Replacement of key resources must be approved by NICL with equal or higher certified personnel.

Report Standardization:

- All reports must conform to RBI, IRDAI reporting formats or standard formats (e.g., CVSS v3.1, NIST, MITRE ATT&CK, CWE, CAPEC references).
- Reports should include business impact mapping and technical details.
- The Vendor should align audit checks with IRDAI, NIST, ISO 27001, ISO 22301, ISO 27017/27018, and CSA CCM requirements.

Risk Register Mapping:

- The Vendor must map all high-risk findings to NICL's Enterprise Risk Register.
- Each mapped risk should have an owner and mitigation timeline defined.

Transition Period for Knowledge Transfer:

- The Vendor must allocate 2 weeks prior to actual assessment for knowledge transfer and onboarding of NICL IT and SOC teams.

Data Residency:

- The Vendor must sign a binding NDA and confirm all sensitive data will reside and be processed within India.
- Cross-border data transfer is prohibited unless explicitly approved in writing by NICL.

SLA Breach Clause:

- If SLA violations occur in 2 or more consecutive quarters, a formal performance review shall be initiated. Additionally, each instance of SLA violation across two consecutive quarters will incur a penalty of 5% of the Annual Rate.

- Such recurring breaches shall be penalized as per penalty clauses and may result in vendor replacement.

Vendor Declaration:

- The Vendor must declare if they have been blacklisted or involved in legal disputes in the BFSI sector in India or globally over the last five years.
- Non-disclosure or false disclosure will lead to disqualification and contract cancellation.

Confidentiality, Independence & Compliance:

- The bidder shall maintain independence, execute NICL NDAs, comply with applicable laws and CERT-In quality requirements, store working papers within India, and follow NICL's data handling and classification policies. All artifacts remain confidential.

Board-Level Reporting and Executive Summary Compliance:

The Vendor shall submit quarterly Board Summary Reports as part of the deliverables. These shall include:

- Executive summary of risk posture, key findings, and emerging threats
- Summary of remediation status (open/closed risks, overdue items, etc.)
- Heat maps and trend visuals on vulnerability posture
- Summary of Red Teaming events (if any during the quarter)
- High-priority risks requiring Board-level intervention or funding

The format shall be aligned with IRDAI Information and Cyber Security Guidelines, 2023 (as updated March 24, 2025) and shared in a presentation-ready format for Board consumption.

Security Assessment of Third-Party Hosted Platforms and SaaS Tools:

Any engagement, testing or integration involving external SaaS platforms, cloud-native tools, or hosted Cyber Security utilities by the vendor must be pre-approved by NICL. The vendor must:

- Disclose all third-party or cloud-hosted tools used during delivery
- Submit technical and legal compliance declarations for each such tool
- Confirm compliance with NICL's Data Residency and Sovereignty policies
- Prefer on-premises or NICL-controlled instances wherever feasible

Use of any externally hosted platform for scanning, or reporting **without explicit written approva**l shall be considered a material breach of contract.

Only licensed and updated tools must be used. Community tools (e.g., Metasploit) must be accessed through commercial variants (e.g., Metasploit Pro). No freeware-only execution will be allowed.

Note: Restriction on External SaaS/Cloud-Hosted Tools

*The Vendor **shall not use any external SaaS-based, cloud-hosted, or internet-accessible scanning, crawling, logging, or reconnaissance tool** for performing any Vulnerability Assessment, Penetration Testing (VAPT), or security audit activities **without prior written approval** from NICL.*

This restriction applies to:

- *Online vulnerability scanners (e.g., Qualys Cloud, OpenVAS Cloud, Nessus Online)*

- *Cloud-based crawlers or spidering tools*
- *External sandboxing environments for malware analysis or payload validation*
- *Logging/telemetry collection platforms hosted on public infrastructure*

*Any violation will be treated as a **material breach** of the contract and will attract penalties or termination, as deemed fit by NICL.*

Exception Handling:
In exceptional cases where usage of such tools is necessary due to technical feasibility, the Vendor shall submit a written request with tool details, usage scope, data handling mechanism, and confirmation of compliance with data residency and IRDAI regulations.

Security Posture Audit of Intermediaries and Digital Supply Chain:
Wherever NICL has digital integrations with intermediaries (agents, brokers, TPAs, etc.), the vendor shall perform sampling-based audits to assess their security posture. This will include:

- Sampling model to cover at least **5% of active digital intermediaries with integration**
- Intermediaries shall be selected based on business volume, customer data access, or API-based integration risk.
- Verification of Cyber Security practices, endpoint hygiene, access control
- Email security (SPF/DKIM/DMARC), browser hardening, basic awareness
- Reporting of critical or high-risk intermediaries requiring follow-up

The audit findings shall be incorporated in NICL's extended attack surface analysis and reported to the Information Security Committee quarterly.

*Note: **Sampling-Based Audit of Intermediaries***

*As part of the security audit deliverables, the vendor shall conduct sampling-based audits of **at least ten (ten) high-impact intermediaries**, APIs, or third-party entities that are digitally integrated via the NICL portal or backend systems.*

These audits must:

- *Assess cyber hygiene, endpoint security, and patching status.*
- *Check authentication and token management controls of integrated APIs.*
- *Include incident handling readiness and incident escalation mechanisms.*
- *Highlight any gaps that may impact NICL's extended attack surface or data flow risks.*

Findings should be documented with remediation advisories and escalated if they impact core NICL systems or sensitive customer data.

Threat Modelling and Data Flow Risk Mapping:
As part of application security testing and risk assessments, the vendor shall provide STRIDE-based Threat Models and Data Flow Diagrams (DFDs) for the following:

- All customer-facing portals, APIs, and mobile apps
- Cloud-hosted or hybrid environments with third-party interconnects

- Internal high-risk applications (claims, payments, CRM, etc.)

  Each model must include:
  - Entry and exit points (ingress/egress)
  - Trust boundaries and access control layers
  - Identified threats as per STRIDE classification (Spoofing, Tampering, etc.)
  - Validation of compensating controls (WAF, IAM, token enforcement, etc.)

These diagrams will serve as part of compliance artefacts and support IRDAI, ISO, and internal audit reviews.

Onboarding, Transition & Exit Planning: *Structured Knowledge Transition to NICL's Internal Teams*

The selected vendor shall ensure a structured **Knowledge Transition Period** to facilitate effective handover and operational readiness for NICL's internal IT, SOC, and NOC teams.

- A **minimum two (2) week period** shall be earmarked **before the start** of the active engagement and **after its completion** to allow for comprehensive knowledge sharing and documentation transfer.
- The transition activities shall include:
  - Walkthrough of assessment methodology and scope.
  - Sharing of runbooks, templates, test cases, and tool usage guides.
  - Familiarization with dashboards, portals, and reporting interfaces used during the engagement.
  - Explanation of threat scenarios, red teaming simulations, workflows, and identified risks.
  - Clarification of remediation responsibilities and expected inputs from NICL teams.
- The vendor shall submit a **Knowledge Transition Plan** upfront, outlining timelines, session topics, documentation to be handed over, and personnel responsible.
- All knowledge transfer sessions must be **recorded and shared** for future reference and internal training purposes.
- This transition period shall **not be clubbed with actual execution timelines** and shall be treated as a separate, billable milestone.
- The vendor must deploy technically competent personnel during this phase who have directly worked on NICL's assessments.

Regulatory Alignment and Compliance Mandate

All activities under this engagement — including scoping, testing, red teaming, assessments, reporting, remediation validation, and knowledge transfer — **must strictly adhere to** the following:

- **IRDAI Information and Cyber Security Guidelines, 2023 (as updated March 24, 2025),** and future **updates, amendments, or circulars** issued under the authority of IRDAI;
- **Relevant mandates under the Government of India**, including but not limited to:
  - CERT-In Guidelines & Advisories
  - Ministry of Electronics and Information Technology (MeitY) Cyber Security Frameworks

- Department of Financial Services (DFS) Security Directives
- National Cyber Security Policy and initiatives from NCSC/NCIIPC

- **Applicable Data Protection Laws and Directives**, including the **Digital Personal Data Protection (DPDP) Act, 2023** (2025 Update), and other sector-specific data retention and breach reporting requirements;
- Globally accepted frameworks such as **ISO/IEC 27001:2022**, **NIST CSF 1.1**, and **CSA Cloud Controls Matrix**, where applicable.

Output and Deliverable Compliance

The following must be ensured throughout the project lifecycle:

- **All reports, templates, trackers, evidence, and executive summaries** must be in a format compatible with **regulatory submission** and **board-level consumption**.
- Risk findings must be **mapped** to the respective **IRDAI sections/sub-clauses**, with clear cross-referencing wherever applicable.
- VAPT, Audit and red teaming outputs must be designed to support **incident disclosure and legal action** as per IRDAI/CERT-In protocols.
- Evidence handling and PII exposure must comply with **DPDP Act** and **CERT-In 6-hour notification mandate**.

Legal & Regulatory Support

Vendor shall support NICL in legal or regulatory proceedings that arise as a consequence of audit, or red teaming outcomes.

3.13 Appendix A: Glossary of Acronyms

This appendix provides an exhaustive list of acronyms used in this RFP to ensure clarity for bidders and stakeholders. It covers terms related to Vulnerability Assessment and Penetration Testing (VAPT), Cyber Security Audit, Red Teaming, regulatory compliance, and technical standards relevant to National Insurance Company Limited (NICL).

Acronym	Definition	Context
ABAC	Attribute-Based Access Control	Access control model used in API security testing (Section 3.2)
ADC	Application Delivery Controller	Network device assessed in VAPT for perimeter security (Section 3.1)
AES	Advanced Encryption Standard	Encryption protocol for in-transit/at-rest data (Section 3.2)

API	Application Programming Interface	Endpoints tested for vulnerabilities per OWASP API Top 10 (Sections 3.1, 3.2)
APT	Advanced Persistent Threat	Simulated in red teaming exercises using MITRE ATT&CK (Section 3.3)
ASR	Attack Surface Reduction	Endpoint security control for macro/VBA restrictions (Section 3.2)
AV	Antivirus	Endpoint protection assessed in audit (Section 3.2)
BCM	Business Continuity Management	Assessed in gap analysis and DR audits (Sections 3.1, 3.2)
BFSI	Banking, Financial Services, and Insurance	Industry context for NICL's Cyber Security requirements
BOLA	Broken Object Level Authorization	OWASP API Top 10 vulnerability tested in VAPT (Sections 3.1, 3.2)
CCMP	Cyber Crisis Preparedness Plan	Validated per IRDAI 2025 updates for crisis management (Section 3.2)
CEH	Certified Ethical Hacker	Certification for VAPT and red teaming personnel (Section 3.4)
CERT-In	Indian Computer Emergency Response Team	Empanelment required for vendor; 6-hour incident reporting (Sections 3.1, 3.2)
CFCE	Certified Forensic Computer Examiner	Certification for forensic investigators (Section 3.4)
CHFI	Computer Hacking Forensic Investigator	Certification for forensic investigators (Section 3.4)
CIA	Certified Internal Auditor	Certification for audit personnel (Section 3.4)
CIS	Center for Internet Security	Source of benchmarks for system hardening (Sections 3.1, 3.2)
CISA	Certified Information Systems Auditor	Certification for audit personnel (Section 3.4)

CISM	Certified Information Security Manager	Certification for compliance analysts (Section 3.4)
CISSP	Certified Information Systems Security Professional	Certification for VAPT and audit personnel (Section 3.4)
CRISC	Certified in Risk and Information Systems Control	Certification for audit personnel (Section 3.4)
CRTO	Certified Red Team Operator	Certification for red team leaders (Section 3.4)
CSA	Cloud Security Alliance	Source of CCM v4.0.3 for cloud security controls (Sections 3.1, 3.2)
CVSS	Common Vulnerability Scoring System	Scoring system for VAPT findings (Section 3.1)
DAST	Dynamic Application Security Testing	Tool integration in DevSecOps pipeline (Section 3.1)
DHCP	Dynamic Host Configuration Protocol	Network service assessed in VAPT (Section 3.2)
DISA	Defense Information Systems Agency	Source of STIGs for configuration hardening (Sections 3.1, 3.2)
DLP	Data Loss Prevention	Assessed in red teaming for exfiltration simulation (Section 3.3)
DMARC	Domain-based Message Authentication, Reporting, and Conformance	Email security control (Section 3.2)
DNS	Domain Name System	Network service assessed for filtering and security (Section 3.2)
DPDP	Digital Personal Data Protection Act, 2023	Data privacy and breach notification compliance (Sections 3.2, 3.3)
DR	Disaster Recovery	Assessed in BCM/DR audits (Section 3.2)
EDR	Endpoint Detection and Response	Endpoint security control (Section 3.2)

eCPPT	eLearnSecurity Certified Professional Penetration Tester	Certification for VAPT testers (Section 3.4)
EnCE	EnCase Certified Examiner	Certification for forensic investigators (Section 3.4)
FTK	Forensic Toolkit	Tool for forensic disk imaging (Section 3.5)
GCFA	GIAC Certified Forensic Analyst	Certification for forensic investigators (Section 3.4)
GCFE	GIAC Certified Forensic Examiner	Certification for malware analysts (Section 3.4)
GPEN	GIAC Penetration Tester	Certification for red team leaders (Section 3.4)
GREM	GIAC Reverse Engineering Malware	Certification for malware analysts (Section 3.4)
GWAPT	GIAC Web Application Penetration Tester	Certification for VAPT testers (Section 3.4)
HLD	High-Level Design	Documentation required from vendor (Section 3)
HSM	Hardware Security Module	Used in cryptography key management (Section 3.2)
IAM	Identity and Access Management	Assessed in cloud security VAPT (Section 3.1)
IDS	Intrusion Detection System	Tested for evasion in VAPT (Section 3.1)
IOCs	Indicators of Compromise	Identified in forensic analysis (Section 3.3)
IPS	Intrusion Prevention System	Tested for evasion in VAPT (Section 3.1)
IRDAI	Insurance Regulatory and Development Authority of India	Regulatory body; guidelines updated March 24, 2025 (Sections 3.1, 3.2)
ISF	Information Security Forum	Part of governance framework (Section 3.2)

ISRMC	Information Security Risk Management Committee	Governance body assessed in audit (Section 3.2)
JWT	JSON Web Token	Token type assessed in API security (Sections 3.1, 3.2)
KMS	Key Management Service	Used in cryptography operations (Section 3.2)
LLD	Low-Level Design	Documentation required from vendor (Section 3)
LPT	Licensed Penetration Tester	Certification for red team leaders (Section 3.4)
MFA	Multi-Factor Authentication	Security control for remote access and terminals (Section 3.2)
MTTD	Mean Time to Detect	Metric assessed in red teaming (Section 3.3)
MTTR	Mean Time to Respond	Metric assessed in red teaming (Section 3.3)
NDA	Non-Disclosure Agreement	Required for data protection (Section 3.11)
NICL	National Insurance Company Limited	Organization issuing the RFP
NIST	National Institute of Standards and Technology	Source of CSF 2.0 and SP 800-series (Sections 3.1, 3.2)
NTP	Network Time Protocol	Synchronization for log accuracy (Section 3.2)
OAuth	Open Authorization	Authentication protocol in API security (Sections 3.1, 3.2)
OSCE	Offensive Security Certified Expert	Certification for red team leaders (Section 3.4)
OSEE	Offensive Security Exploitation Expert	Certification for exploit developers (Section 3.4)
OSCP	Offensive Security Certified Professional	Certification for VAPT analysts (Section 3.4)

OSWE	Offensive Security Web Expert	Certification for exploit developers (Section 3.4)
OWASP	Open Web Application Security Project	Source of Top 10 and API Security Top 10 (Sections 3.1, 3.2)
PII	Personally Identifiable Information	Protected data in SDLC and DPDP compliance (Section 3.2)
PSK	Pre-Shared Key	Wi-Fi security control (Section 3.2)
RBAC	Role-Based Access Control	Access control model in API security (Sections 3.1, 3.2)
RCA	Root Cause Analysis	Required for incidents within 14 days (Section 3.2)
RoE	Rules of Engagement	Document for red teaming scope (Section 3.3)
SAST	Static Application Security Testing	Tool integration in DevSecOps pipeline (Section 3.1)
SCA	Software Composition Analysis	Tool in SDLC security gates (Section 3.2)
SIEM	Security Information and Event Management	Log monitoring system (Section 3.2)
SIP-TLS	Session Initiation Protocol - Transport Layer Security	Used in secure recorded lines (Section 3.2)
SOP	Standard Operating Procedure	Documentation required from vendor (Section 3)
SPF	Sender Policy Framework	Email security control (Section 3.2)
SRTP	Secure Real-time Transport Protocol	Used in secure recorded lines (Section 3.2)
STIG	Security Technical Implementation Guide	DISA guidelines for hardening (Sections 3.1, 3.2)
TTP	Tactics, Techniques, and Procedures	Assessed in red teaming per MITRE ATT&CK (Section 3.3)

UEBA	User and Entity Behavior Analytics	Used in forensic insider threat analysis (Section 3.3)
VLAN	Virtual Local Area Network	Used for segmentation and RTO controls (Section 3.2)
VPN	Virtual Private Network	Assessed in network VAPT (Sections 3.1, 3.2)
WAF	Web Application Firewall	Perimeter security control (Section 3.2)
WORM	Write Once, Read Many	Log immutability requirement (Section 3.2)
WPA2	Wi-Fi Protected Access 2	Fallback Wi-Fi security protocol (Section 3.2)
WPA3	Wi-Fi Protected Access 3	Primary Wi-Fi security protocol (Section 3.2)
ZTNA	Zero Trust Network Access	Remote access security control (Section 3.2)

3.14 Appendix B: Summary of Key Requirements and References

This appendix provides a consolidated overview of the key requirements, regulatory and standards references, deliverables, and SLA metrics for the Vulnerability Assessment and Penetration Testing (VAPT), Cyber Security Audit, Red Teaming, and Training services as outlined in this RFP. It serves as a reference for bidders to ensure alignment with NICL's expectations and compliance with **IRDAI Information and Cyber Security Guidelines, 2023 (as updated March 24, 2025).**

Service Domain	Key Requirements	Regulatory/Standards References	Deliverables	SLA Metrics (Penalty Y/N)

VAPT	- Conduct comprehensive VAPT on network (external/internal IPs, VPN, Wi-Fi, DMZ), applications (web, mobile, APIs), and cloud (VMs, storage, Kubernetes). - Assess DevSecOps pipeline (SAST/DAST), API security (OWASP API Top 10), and container security (CIS Benchmarks). - Perform gap analysis against ISO 27001:2022, ISO 22301, and IRDAI annexures. - Provide remediation roadmap and knowledge transfer.	- IRDAI Guidelines, 2023 (2025 Update): Clauses 4.4.1 (Annual VAPT), 4.4.2 (Application VAPT). - NIST SP 800-115, OWASP Top 10, OWASP API Top 10, SANS 25. - ISO 27001:2022 (A.14.2.8), ISO 27017, CSA CCM v4.0.3 (AIS-04).	- Technical report with CVSS v3.1 scores, risk classification (Critical/High/Medium/Low), and exploitability evidence. - Executive summary with business impact analysis. - Revalidation report post-remediation. - STRIDE-based threat model diagrams per application.	- Initiation: Within 5 working days (Y) - Report submission: Within 10 working days (Y) - Revalidation: Within 7 working days (Y)

Cyber Security Audit	- Validate compliance with IRDAI 2025, including CCMP, 6-hour incident reporting to IRDAI/CERT-In, NTP synchronization, and quarterly board minutes. - Test controls across governance, monitoring, network, cloud, SDLC, cryptography, and third parties. - Review 7 high/medium incidents and 7 critical third-party vendors. - Assess DPDP Act 2023 compliance (data handling, breach notification).	- IRDAI Guidelines, 2023 (2025 Update): Clauses 3.1.6 (Annual Audit), 5.2.5 (Third Parties), 6.2.2 (CCMP), 6.3.1 (6-hour Reporting). - ISO 27001:2022 (A.5-A.18), NIST CSF 2.0 (Govern, Protect), CSA CCM v4.0.3 (GRM-02). - DPDP Act 2023 (Section 8).	- Compliance Mapping Matrix (Excel) for IRDAI, ISO, NIST, CSA, DPDP. - Signed compliance certificate. - Remediation plan with owners/timelines. - Board presentation deck (10–15 slides).	- Audit coverage: 100% of scoped systems annually (Y) - Draft report: Within 15 working days (N) - Final report: Within 5 working days of response (Y)

Red Teaming	- Simulate APT attacks using MITRE ATT&CK TTPs (e.g., phishing, lateral movement, exfiltration). - Conduct social engineering with employee consent forms (Annexure XIII). - Perform physical penetration testing (if authorized) and purple teaming. - Assess forensic readiness with pre-empanelled experts.	- IRDAI Guidelines, 2023 (2025 Update): Clause 6.2.2 (Forensic Readiness). - NIST SP 800-115, MITRE ATT&CK Framework, OWASP Testing Guide v4.2. - Indian IT Act, 2000; DPDP Act 2023.	- Red team report with TTPs, detection gaps, and mitigation steps. - Purple teaming debrief with SOC. - Rules of Engagement (RoE) document. - Lessons learned documentation.	- Tabletop exercise: Quarterly (N) - Full assessment: Twice a year (Y) - Debrief: Within 10 working days (N)
Training	- Deliver security awareness training for all employees, with focus on high-risk departments (Finance, IT, HR). - Conduct phishing simulations targeting <5% click-rate. - Integrate red teaming findings into training content. - Provide training materials and certificates.	- IRDAI Guidelines, 2023 (2025 Update): Clause 6.2.1 (Awareness). - ISO 27001:2022 (A.6.3), NIST CSF 2.0 (PR.AT). - DPDP Act 2023 (data protection awareness).	- Training materials (handouts, videos). - Pre/post-assessment reports (80% pass rate target). - Quarterly training effectiveness report. - Completion certificates for p	

4. Eligibility Criteria

The following are the conditions, which are to be necessarily fulfilled, to be eligible for technical evaluation of the Bid. Non-compliance of any of criteria will entail summary rejection of the bid offer. Photocopies of relevant documents / certificates should be submitted as proof in support of the claims made along with tender. NICL also reserves the right to verify / evaluate the claims made by the vendor independently. Only those interested Bidders who satisfy the following eligibility criteria should respond to this RFP. **The Bidder undertakes that in competing for the RFP and if the award is made to the Bidder in executing the contract, the Bidder will strictly observe the laws against fraud and corruption in force in India namely "Prevention of Corruption Act 1988" and any revision thereof.**

Table - B

Sl. No.	Criteria	Supporting Documentation, with Annexure reference and Page number	Compliance (Yes/no)
1	Should be a public / private limited company or a Partnership Firm registered under the Companies Act, 1956 / 2013 or The Partnership Act 1932, for a minimum period of five years, in India as on 31.March.2025. The Bidder should be empanelled as a VAPT vendor by CERT-iN. In case the Bidder is a wholly owned subsidiary, then the relevant project experience of the parent company would be considered for compliance	Self attested copy of Certificate of Incorporation	
2	The Bidder should hold a valid GST Number & PAN Card and should be registered with the appropriate authorities for all applicable statutory taxes/duties.	• Copy of GST certificate to be submitted • Copy of PAN Card to be submitted	
3	The Bidder should be an established Information Technology company or a Professional Services Firm and in operation for at least 5 years in India as on 31.03.2025. In case the Bidder is a wholly owned subsidiary, then the relevant project experience of the parent company would be considered for compliance.	Self attested copy of Certificate of Incorporation	

Sl. No.	Criteria	Supporting Documentation, with Annexure reference and Page number	Compliance (Yes/no)
4	The bidder must have successfully executed at least two projects of Vulnerability Assessment and Penetration Testing (VAPT), Cyber Security Audit, Red Teaming Services in Public Sector BFSI / PSU/ Private Sector BFSI/ NBFC / Govt. of India (considering one or more orders in at least 5 tools) viz. VAPT Tools : Burp Suite Pro/Nessus Pro / Metasploit / Nikto / Acunetix, Cyber Security Audit Tools : CIS-CAT Pro / Nessus Compliance / Qualys Compliance Suite / Rapid7 InsightVM, Red Teaming Tools : Cobalt Strike / Empire / BloodHound / Metasploit Pro / Mimikatz / PowerSploit, and should be older than 3 years as on RFP date. At least one Cyber Security Audit or Remediation Audit as mandated by the Regulator, should have been completed by the Bidder in any Bank / Insurer in India, in the last 3 years. In case the Bidder is a wholly owned subsidiary, then the relevant project experience of the parent company would be considered for compliance.	● Purchase order/s for procurement and implementation older than 3 years as on RFP date. PO should clearly indicate the tools count. ● Project Sign off / Installation report / customer letter.	
5	The bidder should have an overall annual turnover of minimum Rupees Twenty Crores in each of the last (4) Four Financial Years (2021-22, 2022-23, 2023-24 and 2024-25). In case the Bidder is a wholly owned subsidiary, then the audited financials of the parent company can be considered for compliance. In case of merger or acquisition, financials of merged or acquired companies may be considered in case of new companies.	● Audited Financial statements for the respective financial years and/or Published Balance Sheet and/or CA Certificate	

Sl. No.	Criteria	Supporting Documentation, with Annexure reference and Page number	Compliance (Yes/no)
6	The Bidder should have a positive net worth in each of the last (4) Four financial years (2021-22, 2022-23, 2023-24 and 2024-25). In case of merger or acquisition, financials of merged or acquired companies may be considered in case of new companies. In case the Bidder is a wholly owned subsidiary then the relevant financials of the Parent Company will be considered for eligibility criteria compliance.	● Audited Financial statements for the respective financial years and/or Published Balance Sheet and/or CA Certificate	
7	The Bidder should have Net Profit in any of the last Three years out of the(4) Four financial years (2021-22, 2022-23, 2023-24 and 2024-25). In case of merger or acquisition, financials of merged or acquired companies may be considered in case of new companies. In case the Bidder is a wholly owned subsidiary then the relevant financials of the Parent Company will be considered for eligibility criteria compliance	● Audited Financial statements for the respective financial years and/or ● Published Balance Sheet and/or ● CA Certificate	
8	The Bidder should be ISO 9000/9001, ISO 20000 and ISO/IEC 27001:2022 certified, with certifications valid at the time of bid submission.	Self attested copy of relevant certifications,	
9	The Bidder should have manpower with certifications in Vulnerability Assessment and Penetration Testing - VAPT, Cyber Security Audit and Red Teaming Services. The Bidder should have at least 20 certified professionals	Declaration from HR along with proof of certifications.	

Sl. No.	Criteria	Supporting Documentation, with Annexure reference and Page number	Compliance (Yes/no)
	on their payroll.		
10	The Bidder / Group company should have support offices in any of the (Four) Metro Locations Kolkata, Mumbai, New Delhi, Chennai and Bangalore.	List of Bidder's support centers	
11	The Bidder should not be blacklisted by any Government or PSU enterprise in India as on the date of the submission of bid. And, Ineligible Bidders - Any Bidder who has within the period of last 2 Years (counted from the date 31-Aug-2025), has refused to accept Purchase Order or having accepted Purchase Order failed to carry out the obligations mentioned therein or denied or failed to provide product and/or services after being adjudged as the L1 Bidder in any RFP process of NICL, is debarred from participating in this RFP. Bid, if any, from any such Bidder will be automatically rejected.	Self-Declaration letter by Bidder authorized signatory.	
12	The Bidder should not have filed for Bankruptcy in any country.	Self-declaration confirming the criteria.	
13	• Integrity Pact and Declaration on absence of Conflict of Interest - to be submitted along-with the Bid		
14	• Power of Attorney, - in favor of the official signing the Bid		

Sl. No.	Criteria	Supporting Documentation, with Annexure reference and Page number	Compliance (Yes/no)

Note: Professional Indemnity & Liability Insurance

The Bidder must maintain valid Professional Indemnity Insurance of minimum ₹ 5 Crore to cover errors, breaches, or failures during engagement. Proof of policy to be submitted before onboarding.

Note: Conflict of Interest Declaration

The Bidder must declare that it is not the current developer / maintainer of any system it is auditing or testing, including intermediaries connected via NICL platforms.

Note: The Bidder undertakes that in competing for the RFP, the Bidder shall abide by the Code of Integrity as contained in Rule 175 of GFR 2017. *No official of a procuring entity or a Bidder shall act in contravention of the codes which includes (i) prohibition of*

- *Making offer, solicitation or acceptance of bribe, reward or gift or any material benefit, either directly or indirectly, in exchange for an unfair advantage in the procurement process of to otherwise influence the procurement process*
- *Any omission or misrepresentation that may mislead of attempt to mislead so that financial of other benefit may be obtained or an obligation avoided*
- *Any collusion, bid rigging or anticompetitive behavior that may impair the transparency, fairness and the progress of the procurement process*
- *Improper use of information provided by the procuring entity to the Bidder with an intent to gain unfair advantage in the procurement process or for personal gain*
- *Any financial of business transactions between the Bidder and any official of the procuring entity related to tender of execution process of contract; which can affect the decision of the procuring entity directly or indirectly*
- *Any coercion of any threat to impair or harm, directly or indirectly, any party or its property to influence the procurement process*
- *Obstruction of any investigation or auditing of a procurement process*
- *Making false declaration or providing false information for participation in tender process or to secure a contract*
- *Disclosure of conflict of interest*
- *Disclosure by the Bidder of any previous transgressions made in respect of the provisions of sub-clause (i) with any entity in any country during the last three years of being debarred by any other procuring entity*

5. Selection of Supplier

5.1 Evaluation Methodology

- The RFP will be in two stages, viz., 1st Stage (Pre-Qualification and, Technical) and the 2nd Stage (Commercial bid).

- NICL shall evaluate Pre-qualification Bid first and shortlist the Bidders who qualify for further evaluation.
- The Technical Bid shall be evaluated only for those responses that have qualified in the Pre-Qualification Bid.
- Commercial bids of only those Bidders who qualify in the Technical Bid shall be opened at a later date.
- All Minimum Criteria specified in RFP needs to be fulfilled by the Bidder to proceed to the next stage of evaluation/selection.
- NICL reserves the right to accept/reject any deviation in the Technical and Commercial Bids of any Bidder.
- **Bids that are not substantially responsive are liable to be disqualified at NICL's discretion.**

Eligibility Evaluation

- Pre-Qualification (Eligibility) criterion for the Bidders to qualify this stage is clearly mentioned in Table - B.
- The Bidder would also need to provide supporting documents as proof of eligibility. All credentials submitted by the Bidder must be relevant to the objective and scope of this RFP. The relevance and adequacy of such credentials will be assessed objectively by NICL, at its sole discretion. .
- The Bidders who meet ALL these criteria would only qualify for the second stage of evaluation. NICL will open the Technical bids of the Bidders who qualify in the Pre-Qualification stage.
- The decision of NICL shall be final and binding on all the Bidders to this document. NICL may accept or reject an offer without assigning any reason whatsoever.

Technical Evaluation

- Technical criterion for the Bidders to qualify this stage is clearly mentioned in Table - C.
- The technical soundness of Bidder's proposals will be rated as per the **Table-C** above.
- The Technical bids of bidders qualifying the eligibility criteria will be opened and reviewed to determine whether the technical bids are substantially responsive, evaluation of the Technical Bid submitted along-with compliance to the Minimum Technical Specifications mentioned for each of the products/solutions, as applicable. Where details have been sought, the Bidder should provide specific responses.
- Presentation by the Bidders on their solution and understanding of the Project, if required by NICL.
- Demonstration of functionalities as per NICL's requirements, if required by NICL.
- **A masked copy of the original commercial offer, is to be submitted with the Technical Bid, failing which the bid will be rejected.**
- **The masked copy should not contain price related information, failing which the bid will be rejected outright.**

Table-C: Minimum Technical Specifications

For all line items in the following table, please provide the supporting documentation annexure reference and page number in the corresponding table rows.

Technical Evaluation Matrix				
Sl. No.	**Criteria**	**Technical Evaluation Parameter**	**Evaluation Methodology**	**Compliance (Yes/No)**
Note: • In case of merger or acquisition, financials of merged or acquired companies may be considered in case of new companies.				

• In case the Bidder is a wholly owned subsidiary, then the relevant financials of the parent company would be considered for compliance.				
1	Bidder's Technical Criteria (1)	The bidder should have active CERT-In empanelment and compliance with renewal requirements Documents Required: • Valid CERT-In empanelment certificate and audit reports on the day of the RFP response submission.	• Minimum 4 Years of Empanelment	
5	Bidder's Technical Criteria (2)	Public Sector BFSI / PSU/ Private Sector BFSI/ NBFC / Govt. of India Experience for handling projects of Vulnerability Assessment and Penetration Testing (VAPT), Cyber Security Audit and Red Teaming Services and should be **older than 3 years** as on RFP date. Documents required: • Purchase Order / Contract - multiple POs would be considered • Project Sign off / Installation Report / Customer Letter (**Max – 15 Marks**)	• Minimum of 2 Customers	
6	Bidder's Technical Criteria (3)	The Bidder/group company should have Manpower with Certifications in Vulnerability Assessment and Penetration Testing (VAPT), Cyber Security Audit and Red Teaming Services. In case of mergers / acquisitions / de-mergers / restructuring or name change, the employees of the Group Company will be considered for compliance.	(A) **VAPT Certifications**: • **10** resources with Advanced Certifications (OSCP/CREST CRT/CISSP) and **10** resources with Basic Certifications (OSCP/eCPPT/CEH/GWAPT) (B) **Cyber Security Audit Certifications**: • **7** resources with CISA/CISSP/ISO 27001 Lead Auditor/CRISC/CIA/CISM/OSCP/CREST	

		Documents required: ● Declaration from HR along with proof of certifications	(C) **Red Teaming Certifications**: ● **6** resources with CISA/CISSP/ISO 27001 Lead Auditor/CRISC/CIA/CISM/OSCP/CREST	
7	Bidder's Technical Criteria (4)	The Bidder/group company should have **Technical Capability and Toolset** in Vulnerability Assessment and Penetration Testing (VAPT), Cyber Security Audit and Red Teaming Services. Documents required: ● Tool licenses and past project reports showing Tool usage. ● Customer Letter.	(A) **VAPT Tools**: ● Burp Suite Pro ● Nessus Pro ● Metasploit ● Nikto ● Acunetix (B) **Cyber Security Audit Tools**: ● CIS-CAT Pro ● Nessus Compliance ● Qualys Compliance Suite ● Rapid7 InsightVM (C) **Red Teaming Tools**: ● Cobalt Strike ● Empire ● BloodHound ● Metasploit Pro ● Mimikatz ● PowerSploit	
9	Proposal	Bidder's Proposal	The bidders of this RFP have to submit a proposal to NICL on the methodology/approach, time frame for various activities, strengths of the bidders on such projects The technical competence and capability of the bidder should be clearly reflected in the proposal. The proposal should contain, Sample Templates for Reporting Deliverables	

Commercial Evaluation

The commercial bids for the technically qualified Bidders will be opened and reviewed to determine whether the commercial bids are substantially responsive. Bids that are not substantially responsive are liable to be disqualified at NICL's discretion. The total cost of ownership for the purpose of evaluation shall be calculated over the contract period.

- **The final price would be decided on the basis of RA in the GeM portal.**

- **50% of commercially qualified bidders (Starting from L1) will be allowed to participate in RA.**
- **RA will start immediately after commercial bid evaluation and will be valid for 48 hours.**
- **Participated bidders will be notified through GeM for Reverse Auction.**
- **The products and price offered cannot be withdrawn by the bidder from GeM during the bid validity period.**
- **During Reverse auction, Start / Reference Price and Step Value of Decrement will be indicated to the Bidders at the start of the auction through the GeM portal. Any participating bidder can bid one or multiple Step Decrement lower than the prevailing Lowest Bid at that time.**
- **The Bidder shall be able to view Bid Start Price, Bid Decrement Value, Prevailing Lowest Bid value and last Bid Placed by him.**
- **Whenever a lower price bid is received in the closing moment i.e. within 15 minutes of existing end time of Reverse Auction, the end time of reverse auction will be extended automatically by another 15 minutes. All participant sellers of that RA shall be notified by the GeM system about extension of time through email and/or SMS and they shall be allowed to submit revised bids under the RA. The same process shall be repeated, if there is another lower bid received in the RA during the last 15 minutes of RA.**
- **NIC will not have any liability to bidders for any interruption or delay in access to the GeM site / Reverse Auction link etc., irrespective of the cause.**
- **The L1 bidder after completion of RA has to submit a hard copy in their letterhead duly signed that they agree with the price quoted by them during RA pertaining to RA No: XXXXXXX to NICL within 24 hours (Twenty Four) of Reverse Auction without fail. If not submitted, bids will be rejected.**

The total cost of ownership for the purpose of evaluation shall be calculated over the contract period.

5.3 Intentionally Kept Blank

6. Bid Submission Details

- Mode: Online (GeM/eProcure).
- EMD: INR 10 Lakhs
- RFP Fee: INR 25,000
- PBG: 3% of Total Contract Value

Note: EMD will be refunded to unsuccessful bidders within 45 working days from the date of finalization of the successful bidder, without any interest, subject to receipt of application from the Bidder.

7. Commercial Bid

Table – D

Sl. No.	Particulars	Frequency	Unit	Scope Description (Brief)	Cost per Unit / Cycle (INR, Excl. Taxes)	Annual Cost (INR, Excl. Taxes)
1	IRDAI Annual Cybersecurity Assurance Audit	Annual (1 cycle)	Per Cycle	Full independent audit per IRDAI Clause 3.1.6 including Compliance Mapping Matrix, Board Deck, signed certificate	[Insert]	[Insert]
2	VAPT – Network & Infrastructure	Twice Yearly (2 cycles)	Per Cycle	External/Internal IPs, VPN, Wi-Fi, IoT, DMZ, segmentation, IDS/IPS evasion, remote access (RDP/SSH)	[Insert]	[Insert]
3	VAPT – Web & Mobile Applications + APIs	Twice Yearly (2 cycles)	Per Cycle	OWASP Top 10, OWASP API Top 10, SPA/PWA, mobile binary (iOS/Android), DevSecOps pipeline	[Insert]	[Insert]
4	VAPT – Cloud Infrastructure	Twice Yearly (2 cycles)	Per Cycle	AWS/Azure/GCP/hybrid – VMs, storage, Kubernetes, serverless, IAM	[Insert]	[Insert]
5	Red Teaming – Full APT Simulation	Twice Yearly (2 cycles)	Per Cycle	MITRE ATT&CK TTPs, social engineering (with consent), physical (if authorized), purple teaming	[Insert]	[Insert]
6	Red Teaming – Tabletop Simulation Exercise	Quarterly (4 exercises)	Per Exercise	CCMP-aligned crisis simulation with CCMP validation	[Insert]	[Insert]
7	Forensic Readiness Assessment & Retainer	Annual Assessment + 24×7 Retainer	Lump Sum	Pre-empanelled forensic experts, readiness check, 4-hour response SLA (retainer)	[Insert]	[Insert]

8	DPDP Act 2023 Readiness & Compliance Assessment	Annual	Per Assessment	Data classification, consent management, DPIA, breach notification process validation	[Insert]	[Insert]
9	Third-Party Partner Cyber Risk Audit	Annual + Quarterly for High-Risk Partners (estimated 8 high-risk + 10 Medium.low)	Lump Sum	Independent audit of NICL partners (sampling based on risk posture), non-compliance reporting, follow-up	[Insert]	[Insert]
10	Ad-Hoc Ethical Hacking / Incident Response Support	On-demand (up to 4 engagements/year)	Per Engagement	Triggered by CISO for high-severity incidents or post-deployment vulnerabilities	[Insert]	[Insert]
11	Security Awareness Training & Phishing Simulations	Quarterly (4 sessions)	Per Session	All employees + targeted for high-risk depts, <5% click-rate target	[Insert]	[Insert]
12	Governance, Reporting & Documentation	Ongoing Annual	Lump Sum	Daily/weekly/monthly reports, dashboards, HLD/LLD/SOP, quarterly board reporting	[Insert]	[Insert]
Total						[Insert Sum of 1 to 12]

***Notes**:*

- *Costs are indicative and will be finalized via reverse auction on the NICL e-procurement platform **[Insert Platform Name, e.g., NICL e-Tender Portal]** as per Section 3.12.*

- *Bidders must specify taxes (e.g., GST rate) separately in their proposals.*
- *Annual costs reflect the total for the specified frequency (e.g., 2 VAPT cycles, 4 training sessions).Price to be quoted excluding GST*

Total Amount in Words: INR ..... only, excluding GST

8. Intentionally Kept Blank

9. Contract Terms

- Duration: **3 Years** from Purchase Order plus 2 months for exit management
- Performance Bank Guarantee: 3% of contract value
- Liquidated Damages: Applicable on breach of SLA clauses
- Exit Management: 2-month overlap with incoming team
- The Contract between NICL and the Supplier shall be initiated within **30 working days** of issuance of Purchase Order.

10. General Terms & Conditions

- **Bid Conditions:**
  - All bids are to be submitted in Indian Rupees
  - NICL reserves the right to reject any/all bids.
  - Conditional bids will be rejected.
  - Disputes subject to jurisdiction of Kolkata High Court.
  - Intending Bidders who satisfy the eligibility criteria laid down under this document can bid for the RFP. Intending Bidders may also download this document from the company's website (https://nationalinsurance.nic.co.in) or from GeM portal between dates (refer – Section Important Dates and Information) and the Bidder has to submit a non-refundable RFP Document Fee of Rs. 25,000/- Only (Rupees Twenty Five Thousand Only) to National Insurance Company Limited payable through NEFT/RTGS only prior to Pre-Bid Meeting Date (if the Bidder wishes to participate in the Pre-Bid meeting).
    - Non-furnishing of RFP Document Fee/s, till the time of submission of the bid will disqualify the bidder. A copy of proof of payment of non-refundable RFP Fee has to be sent to the Email IDs mentioned in **Section 1.3 Important Dates and Information**
    - Intending Bidders who wish to participate in the Pre-Bid Meeting shall submit the proof of payment of non-refundable RFP Document Fee of Rs. 25,000/- only (Rupees Twenty Five Thousand only) to National Insurance Company Limited payable through NEFT/RTGS only, prior to the Pre-Bid Meeting Date.
    - Only authorized representatives of Bidder are allowed to participate in the pre-Bid meeting. Documentary proof of payment of the RFP Document Fee by intending bidders by mail/hard copy, is a pre-requirement for participation in the Meeting.
- **Ineligible Bidders**: Any Bidder who has within the period of last 2 Years (counted from the date 1st Oct, 2025), has refused to accept Purchase Order or having accepted Purchase Order failed to carry out the obligations mentioned therein or denied or failed to provide product and/or services after being

adjudged as the L1 Bidder in any RFP process of NICL, is debarred from participating in this RFP. Bid, if any, from any such Bidder will be automatically rejected.

- **Clarification of Bids:** No query / suggestions will be entertained after the opening of the Commercial offer. Clarifications will be published in NICL's Corporate Website: https://nationalinsurance.nic.co.in, GeM portal: https://gem.gov.in/ and CPP Portal). No other modes of communication will be used. Intending Bidders should check the website frequently to get updates on any such changes. NICL reserves the right to cancel the RFP at any time without incurring any penalty or financial obligation to any Bidder or potential Bidder.
- **Governing Language:** The bid prepared by the Bidder and all correspondence and documents relating to the bids exchanged by the Bidder and the Purchaser, shall be written in the English language, provided that any printed literature furnished by the Bidder may be in any other language so long the same is accompanied by an English translation in which case, for purposes of interpretation of the bid, the English translation shall govern.
- **Bid Submission:** Bids must be received by NICL at the specified address not later than the time and date specified in the **RFP**. In the event of the specified date for the submission of Bids being declared a holiday for NICL, the bids will be received up to the appointed time on the next working day. NICL may, at its discretion, extend this dead-line for the submission of Bids, in which case all rights and obligations of NICL and Bidders previously subject to the deadline will thereafter be subject to the deadline as extended. **Any bid received by NICL after the deadline for submission of bids prescribed by NICL will be rejected and returned unopened to the Bidder.**
- **Acceptance of Terms:** The Bidder will, by responding to RFP, be deemed to have accepted the terms of the RFP Document.
- **No legal relationship:** No binding legal relationship will exist between any of the Bidders and NICL, until execution of the Contract.
- **Contract:** Template of Contract is provided in Annexure. NICL may, at its sole discretion, choose to extend the contract by a period not exceeding one year on the same terms and conditions, with mutual agreement of the Supplier.
- **Contract Amendment:**
  No variation in the satisfaction of the terms of the Contract shall be made except by the written amendment agreed and signed by the parties.

    - If the Supplier fails to render services within the time period(s) specified in the Contract or any extension period thereof granted by the Purchaser, or
    - If the Supplier fails to perform any other obligations under the Contract

- **Applicable Law:**

  The Contract shall be construed, interpreted and applied in accordance with and shall be governed by the laws applicable in India including applicable export and import laws. The courts at Kolkata shall have the exclusive jurisdiction to entertain any dispute or proceeding arising out of or in relation to the Contract.

- **Arbitration:**

  If any dispute or difference shall arise, such difference shall independently of all other questions be referred to the decision of a sole arbitrator to be appointed in writing by the parties or if they cannot agree upon a single arbitrator within 30 days of any party invoking arbitration, the appointment shall be made upon request by a party, by the Chief Justice of the High Court at Calcutta, or any person or institution designated by him in accordance with the provisions of the Arbitration and Conciliation Act, 1996 as

amended or re-enacted from time to time. It shall be a condition precedent to any right of action or suit upon the Contract that award by such arbitrator/arbitrators of the amount of the loss or damage shall be first obtained. The seat of such arbitration shall be at Kolkata.

- **Notice:**

  Any notice by one party to the other pursuant to the Contract shall be sent in written format by fax/email and confirmed in writing to the address specified for that purpose in the Contract.

- **PBG:**

  Performance Bank Guarantee (PBG) of 3% of 'Contract Value' should be submitted by the successful Bidder, (as per format given within 30 working days of issue of Purchase Order). Failure to submit the PBG within the mentioned period will attract SLA. Once this PBG i.e. 3% of 'Contract Value', in the form of Bank Guarantee is received by NICL, the EMD as Bid Security in respect of NICL/IT/RFP/VAPT_Cyber SecurityAudit_RedTeaming/18/2025 *will* be returned to the successful Bidder. No advance payment will be made by 'NICL'.

- **Payment Terms:**

  Payments shall be released based on the milestones below, contingent upon the vendor's adherence to the Scope of Work (Section 3), SLA Metrics (Section 3.6), and Governance Requirements (Section 8.1). NICL reserves the right to request additional documents for payment release, which the vendor shall provide within 5 working days. All payments are in Indian Rupees (INR), subject to applicable taxes (e.g., GST), and finalized via reverse auction per Section 3.12.

Milestone	Description	Documents Required	Verification Process

Completion of VAPT, Audit, and Red Teaming Activities	Successful execution of VAPT (network, applications, APIs, cloud), Cyber Security Audit (IRDAI compliance, CCMP, board reporting), and Red Teaming (APT simulations, purple teaming) per Sections 3.1–3.3. Includes forensic readiness assessments and quarterly training sessions.	- Preliminary VAPT report (CVSS v3.1 scores) - Draft audit report (Compliance Mapping Matrix) - Red teaming report (TTPs, RoE) - Forensic readiness summary - Training logs (80% pass rate)	NICL CISO/IT team review; compliance with SLAs (Section 3.6)
Submission of Final Reports and Recommendations	Delivery of final reports for VAPT (technical, executive summary, revalidation), Audit (final report, board deck, signed certificate), Red Teaming (debrief, mitigation plan), Forensics (legal-format dossier), and Training (effectiveness report). All deliverables in specified formats (Word/PPT/Excel).	- Final VAPT report (Word/PDF) - Final audit report with board deck (PPT) - Red teaming debrief slides (PPT) - Forensic dossier (PDF, hash-verified) - Training effectiveness report (Excel)	NICL CISO approval; verification of remediation recommendations

Acceptance of Reports and Sign-Off	NICL's formal acceptance of all deliverables and sign-off by CISO, confirming compliance with IRDAI Guidelines, 2023 (2025 Update), NIST CSF 2.0, and DPDP Act 2023. Includes post-remediation revalidation results and training completion certificates.	- Signed acceptance letter - Revalidation report (VAPT) - Compliance certificate (Audit) - Training completion certificates	NICL CISO sign-off; audit trail of acceptance

Service	Payment Breakdown	Penalty
Audit	100 % on acceptance (steps: draft submission, review, final report submission, acceptance).	₹10,000/day
VAPT (2 cycles)	100 % on acceptance (steps: report submission, revalidation, final, acceptance).	₹5,000/day
VAPT (Two Cycles) - change in internet facing applications	40% report, 30% revalidation, 30% acceptance. 100 % on acceptance (steps: report submission, revalidation, final, acceptance). Cut-off for invoice: VAPT acceptance, upto 15th of the last month of the past quarter.	₹5,000/day
Red Teaming	100 % on acceptance (steps: assessment, debrief, acceptance).	₹7500/day
Training	25% post each quarter	₹7500/day

Note**: **Payment Terms

- *Payments are released within **30 working days** of milestone completion, subject to NICL verification.*
- *Vendors must submit deliverables via **secure channels** (e.g., AES-256 encrypted) per DPDP Act 2023.*
- *Non-compliance with SLAs (Section 3.6) may result in **payment withholding or penalties**.*

- *Additional documents (e.g., **SLA compliance logs, escalation reports**) may be requested for verification.*
- *Final payment is contingent on **reverse auction pricing** and contract terms.*
- *All payments to the Supplier will be made by NICL through NEFT/RTGS Only.*

Note: Technical Resource Continuity

*The Vendor shall ensure that **at least 80% of the originally proposed and evaluated technical personnel** remain unchanged throughout the duration of the engagement, covering activities such as VAPT, Red Teaming, Cyber Security Assurance Audit, unless otherwise approved in writing by NICL.*

*Replacement of any core resource shall only be permitted under **force majeure circumstances** (e.g., medical emergency, resignation, or similar unavoidable situations).*

*Any such replacement must be **notified in advance**, with submission of:*

- *Credentials and certifications of the new proposed personnel.*
- *Detailed knowledge transition plan.*
- *Justification for replacement.*
- *Written **approval obtained from NICL's designated authority** prior to deployment.*

*Repeated or unjustified changes in key personnel may be treated as a **non-performance issue** and may attract penalties or be considered a ground for termination.*

- **Delays in the Supplier's performance: Delivery and performance of the services shall be made by the Supplier in accordance with the time schedule mentioned.**
- Any delay by the Supplier in the performance of its delivery obligations shall render the Supplier liable for imposition of liquidated damages, and/or termination of the Contract for default, besides encashment of the PBG.
- If at any time during the performance of the Contract, the Supplier should encounter the conditions impeding the timely performance of the services, the Supplier shall promptly notify the Purchaser in writing of the fact of the delay, its likely duration and its cause(s). As soon as practicable after receipt of the Supplier's notice, the Purchaser shall evaluate the situation and may at its discretion extend the Supplier's time for performance in which case the extension shall be recorded by the parties.
- Any delay by the Supplier in the performance of its service obligations, other than the delay which occurs due to reasons beyond the Supplier's control, shall render the Supplier liable for termination of the contracts for default. Any incidental taxes and levies on account of delay in performance caused by Supplier shall be on the Supplier's account.

- **Liquidated Damages:**
  - Non-compliance of the SLA, penalty would be as per defined in SLA. The overall penalty cap would be 10% of the Contract Value of the RFP . After the cap is reached, NICL may cancel the contract.

- Once this amount reaches 10% of the Contract Value, NICL may cancel the contract, and encash the PBG. Encash of the Performance Bank Guarantee shall not endanger any provisions of warranty/AMC written or otherwise expressed and the concerned warranty/AMC will remain in full force.
- The aggregate of all penalties and liquidated damages under this Contract shall not exceed 10% of the Contract Value.
- In case Services are not fully completed within the stipulated period, Liquidated Damage condition shall be invoked if such delay is not attributable to "Force Majeure". NICL reserves the right to extend the Time Period, where the delay is due to NICL responsibility.

- **Resort to Liquidated Damages:**

  In the event the Purchaser terminated the Contract in whole or in part, the Purchaser shall:

  - En-cash the PBG/not refund the performance security amount.
  - Deduct Liquidated damages as specified in respective Clause/s
  - May procure, upon such terms and in such manner as it deems appropriate, services similar to those undelivered and/or not performed, and the Supplier shall be liable to the Purchaser, for any excess costs up to a maximum value of 10% of the Contract Value, for such similar Services. However, the Bidder shall continue performance of the Contract to the extent not terminated.

- **Termination on Insolvency:**

  The agreement can be terminated by giving written notice to the Supplier, without compensation to them if:

  - The Supplier becomes bankrupt or is otherwise declared insolvent;
  - The Supplier being a company is wound up voluntarily or by the order of a court or a receiver, or manager is appointed on behalf of the debenture holders or circumstances occur entitling the court or debenture holders to appoint a receiver or a manager, provided that such termination will not prejudice or affect any right of action or remedy accrued or that might accrue thereafter to the Purchaser.
  - The Purchaser shall however pay the Supplier for all products and services provided up to the effective date of termination.

- **Termination for Defaults:**

  The Purchaser may, without prejudice to any other remedy for Breach of the Contract, by written notice of 90 days of default to the Bidder, terminate the Contract in whole or in part;

  - If the Supplier fails to render services within the time period(s) specified in the Contract or any extension period thereof granted by the Purchaser, or
  - If the Supplier fails to perform any other obligations under the Contract
  - All payments due to the Supplier till the effective date of termination will be made by NICL within 60 days' of such written notice of termination, subject to applicable penalties.

- **Termination for Convenience:**
  - The Purchaser may by written notice of 90 days sent to the Supplier terminate the Contract, in whole or in part, any time for its convenience. The notice of termination shall specify that

termination is for the Purchaser's convenience, the extent to which performance of work under the Contract is terminated and the date on which such termination becomes effective.

- The Purchaser may purchase the ordered goods that are complete and ready for installation after the Supplier's receipt of notice of termination at the Contract terms and prices. For the remaining goods and services, the Purchaser may elect:
- To have any portion completed and delivered at the contract terms and prices; and/or
- To cancel the remainder and pay to the supplier an agreed amount for partially completed goods and services and for materials and parts previously procured by the Supplier.
- All payments due to the Supplier till the effective date of termination will be made by NICL within 60 days' of such written notice for termination.

- **Consequences of Termination of Selected Bidder:**

  In the event of termination of the selected Bidder due to any cause whatsoever, [whether consequent to the stipulated terms of the RFP or otherwise], NICL shall be entitled to impose any such obligations and conditions and issue any clarifications as may be necessary to ensure an efficient transition and effective business continuity of the Service(s) which the terminated Bidder shall be obliged to comply with and take all available steps to minimize loss resulting from that termination/breach, and further allow the successor to take over the obligations of the terminated Bidder in relation to the execution/continued execution of the scope of the work defined in RFP.

  Nothing herein shall restrict the right of NICL to invoke the Performance Bank Guarantee and take other actions as defined in this RFP and pursue such other rights and/or remedies that may be available under law or otherwise. The termination hereof shall not affect any accrued right or liability of either Party nor affect the operation of the provisions of the RFP that are expressly or by implication intended to come into or continue in force on or after such termination.

  In all cases of termination, the obligation of the NICL to pay shall be limited to the period up to the date of termination. Notwithstanding the termination of this Agreement, the parties shall continue to be bound by the provisions of this Agreement that reasonably require some action or forbearance after such termination.

  Survival: The following clauses survive the termination and expiry of the contract:

  - Intellectual Property Rights;
  - Protection of personal information
  - Exit Management
  - Compliance to Security;
  - Indemnity;
  - Confidentiality and Non-Disclosure;
  - Audit Access - Right to Audit

- **Limitation of Liability:**

  Supplier's aggregate liability for actual direct damages shall be limited to a maximum of the Contract Value, provided that this limit shall not apply to (1) the infringement indemnity; or (2) bodily injury (including death) and damage to real property and tangible personal property caused by Supplier's negligence. Supplier shall not in any event be liable for any indirect or consequential damages, or for loss of profit, business, revenue, goodwill, anticipated savings or data, or third party claims except with respect to bodily injury (including death) and damage to real and tangible personal property for which

Supplier is legally liable. For the purposes of this Section, "Contract Value" at any given point in time, means the aggregate value of purchase orders placed by NICL on the Bidder under this project.

- **Income/Corporate Taxes:**
  - The Supplier shall be liable to pay all the Corporate Taxes, and the Income Tax, that shall be levied according to the laws and regulations applicable from time to time in India.
  - Wherever the laws and regulations require deduction of such taxes at the source of payments, the Purchaser shall effect such deductions from the payment due to the Supplier. The remittance of amounts as deducted and issuance of Certificate for such deductions shall be made by the Purchaser as per the regulations in force. Nothing in the Contract shall relieve the Supplier from their responsibility to pay any tax that may be levied in India on income and profits made by the Bidder in respect of the Contract.
  - The relevant deduction certificate shall be provided to the Supplier within 90 days of deduction at source.
  - Supplier will be entirely responsible for making the payments in respect of all taxes, stamp duties, fees, etc. in connection with delivery of service at site/s including taxes and levies to be charged in connection with incidental services etc. For procurement of way-bills if any, necessary arrangements shall be made by the Bidder. Service Taxes will be payable as per rules prevalent at the time of submission of bid response.

- **Indemnity Clause:**

  The Supplier shall, at its own expense, defend, indemnify, and hold harmless National Insurance Company Limited (NICL), its officers, employees, and agents from and against any and all claims, demands, actions, liabilities, losses, damages, costs and expenses (including reasonable attorney's fees) arising out of or in connection with:
  - **Employment-related Claims:** Any claim, action, or demand by the personnel deployed by the Supplier under this RFP, including but not limited to claims related to wages, benefits, injuries, terminations, statutory dues, or conditions of employment
  - **Breach of Statutory Obligations:** Any violation by the Supplier or its personnel of applicable laws, regulations or codes including but not limited to labour laws, EPF/ESI/Gratuity/Minimum Wages Acts, Industrial Disputes Act, Contract Labour (Regulation and Abolition) Act, Shops and Establishments Act, Income Tax laws and applicable State regulations.
  - **Misconduct or Negligence of Personnel:** Any act or omission of the Supplier's personnel including misconduct, fraud, breach of confidentiality, misuse of NICL's assets or infrastructure, or any negligent act causing loss or damage to NICL or any third party.
  - **Breach of Contractual Terms:** Any failure by the Supplier to perform its obligations under this RFP including failure to provide qualified, certified or background-verified personnel or failure to meet service levels and timelines.
  - NICL shall notify the Supplier promptly upon becoming aware of any such claim and shall provide reasonable cooperation in the defense and settlement of such claim. NICL shall not admit any liability or agree to any settlement without the prior written consent of the Supplier.
  - If the Supplier fails to fulfill its indemnification obligations within the period specified in a notice issued by NICL, NICL shall have the right to recover the due amount from any sums payable to the Supplier under this RFP or any other contract.
  - These indemnities are in addition to, and not in substitution of, any other remedies or indemnities available to NICL under this RFP, law, or equity.

- **Confidentiality:**

  The Supplier and NICL (each a "Receiving Party" when receiving information) agree to: Confidentiality Obligations

  - Keep all confidential Information received from the other party ("Disclosing Party") strictly confidential during the contract term and for ten (10) years after termination.
  - Use such information only for fulfilling contractual obligations, and not for personal or third-party benefit.
  - Restrict disclosure to only those employees, officers, directors, professional advisors, or affiliated group companies who require it for contract performance, and ensure they are bound by confidentiality terms no less stringent than those herein.
  - Remain liable for any unauthorized disclosures made by such individuals.
  - **Return or Destruction of Information:** Upon request by the Disclosing Party, the Receiving Party shall return or securely destroy all confidential Information, unless retention is legally required or essential to enforce rights under the contract.
  - **Exclusions from Confidentiality**: These obligations shall not apply to information that the Receiving Party can prove:

    - Is or becomes public (not due to breach),
    - Was already lawfully in its possession without obligation of confidentiality,
    - Was lawfully received from a third party without breach,
    - Was independently developed without reference to the Disclosing Party's Confidential Information.
  - **Disclosure under Law or Authority:** Disclosure is permitted where required by applicable law or a competent authority, provided that:
    - The Disclosing Party is notified in writing (unless prohibited by law),
    - Reasonable efforts are made to obtain written assurance from the authority to maintain confidentiality.
  - **Access Control:** Access to Logs / Data Clause: Vendor shall be granted read-only access to logs or data required for assessment. Export or off-site storage of logs or artifacts shall only be allowed with written approval of NICL.
  - **Additional Commitments by Supplier:** Comply with the Digital Personal Data Protection Act, 2023 (DPDP Act), as and when relevant rules and guidelines come into force.
    - Refrain from publishing or disclosing any details about security safeguards implemented for NICL without prior written consent.
    - If any legal/statutory demand for data disclosure arises from government authorities:

      - Seek NICL's explicit written concurrence before any disclosure,
      - Resist unlawful or unauthorized demands, and
      - Avoid using NICL's name/ logo in publicity without NICL's written permission.
- **Assignment:**
  - Assignment by the Supplier:
    The Supplier shall not assign, transfer, delegate or otherwise deal with, in whole or in part, any of its obligations, responsibilities, or rights under this RFP or the resulting contract, without the prior

written consent of NICL. Any attempted assignment in violation of this clause shall be null and void.

- Assignment by NICL:
  NICL reserves the right to assign, novate, or transfer the services procured under this RFP, in whole or in part, as part of any internal reorganization, corporate restructuring, merger, consolidation, or sale of its assets. Additionally, NICL may assign the services to a third-party contractor or agency in the event of any of the following occurrences:

  - The Supplier refuses to perform its obligations;
  - The Supplier becomes incapable of performing its obligations;
  - Termination of the contract with the Supplier, for any reason whatsoever;
  - Expiry of the contract period.
  - Such right of assignment shall be without prejudice to any other rights and remedies available to NICL under this RFP or at law.

- **Continuation of Services Post-Assignment:** In the event of an assignment by NICL, the Supplier shall ensure that any third-party sub-contractors or personnel originally deployed are willing to continue providing services to NICL or its nominee at terms no less favorable than those agreed under the original contract. The Supplier shall include appropriate binding provisions in its agreements with such subcontractors or personnel to ensure compliance.

- **Prohibition of Subcontracting and Consortium:**

  No subcontracting or consortium arrangements shall be permitted under this RFP. The Supplier must itself possess the necessary qualifications and capabilities to execute the scope of work outlined. Participation by multiple entities from the same group company or parent entity under separate bids is strictly prohibited.

- **Obligations:**

  The entire responsibility of the Scope of Work and all related activities in respect of the RFP lies with the Supplier on whom the Purchase Order is placed and with whom the Contract is signed. The Supplier would be responsible and bear the additional cost (if any), incurred by the Purchaser on account of the above-mentioned obligations

- **Outsourcing Agreement:**

  The contract between Supplier and National Insurance Company Limited (NIC/NICL/Purchaser), inter alia, shall be deemed to include the following conditions listed below:-

  - **Contingency Planning:** The Supplier is responsible for contingency planning of the outsourcing service to provide business continuity for the outsourced arrangements that are material in nature.
  - **Express Clause:** The contract shall neither prevent nor impede the company from meeting its respective regulatory obligations, nor the IRDAI from exercising its regulatory powers of conducting inspection, investigation, obtaining information from either the company or the Bidder.

- **Handing over of the Data, Assets etc.:** In case of termination of the contract, the Supplier is responsible for handing over of the data, assets (hardware/software) or any other relevant information specific to the contract and ensure that there is no further use of the same by the Supplier.
- **Inspection and Audit by the company:** The Company may conduct periodic inspection or audit on the Bidder either by internal auditors or by Chartered Accountant firms appointed by the Company to examine the compliance of the outsourcing agreement while carrying out the activities outsourced.
- **Legal and Regulatory Obligations:** The Bidder shall ensure that the outsourcing contract/ arrangements do not:-
  - Diminish the Company's ability to fulfill their obligations to Policyholders and the IRDAI.
  - Impede effective supervision by the IRDAI.
  - Result in Company's internal control, business conduct or reputation being compromised or weakened.
- **Applicability of the laws/regulations:** The Regulations apply irrespective of whether the outsourcing arrangements are entered into with an affiliated entity within the same group as the Company, or an outsourcing service Provider external to the group or the one who has been given sub-contract. The Outsourcing Agreement shall not diminish the obligations of the Company and its Board and Senior Management to comply with the relevant law/s and regulations. The Bidder engaged by the company is subject to the provisions of the Insurance Act 1938, IRDA Act 1999, rules and regulations and any other order issued thereunder.
- In case, the Bidder operates from outside India, it shall ensure that the terms of the agreement are in compliance with respective local regulations governing the Bidder and laws of the country concerned and such laws and regulations do not impede the regulatory access and oversight by the Authority.

- **Principal to Principal Liability:**

  The employees engaged by the Bidder shall be deemed to be the employees of Bidder only, and the NICL shall not be connected with the employment or the terms and conditions thereof in any way. The Bidder alone would comply with the statutory obligations and Labour Regulations/ Rules in this regard. None of the terms of this Contract shall be deemed to constitute a partnership or joint venture or employee-employee relationship between the parties hereto, and neither party shall have authority to bind the other except as specifically provided for hereunder. Neither party hereto is the agent of the other nor is there any master–servant relationship between the parties. The relationship is on a principal to principal basis. The Bidder shall be responsible for payments of all statutory dues with respect to each of his personnel/employees engaged by him to render service under this Agreement with respect to each applicable/extant labor law, including but not limited to, the Minimum Wages Act, 1948, The Payment of Wages Act, 1936, The Payment of Bonus Act, 1965, Code on Wages, 2019 as and when is notified by Government, The Employees' State Insurance Act, 1948, The Payment of Gratuity Act, 1972, The Maternity Benefit Act, 1961, The Employees' Provident Funds and Miscellaneous Provisions Act, 1952, etc. No dues/contributions under any labor legislations as applicable, remain payable with respect to his personnel/employees. The Bidder shall have no claims whatsoever against the NICL with respect to payment of statutory dues/contributions to its personnel/employees under applicable labor legislations/rules/regulations.

- **Force Majeure:**

  Notwithstanding the provisions contained herein the Supplier shall not be liable for liquidated damages or termination for default, if and to the extent that its' delay in performance or other failure to perform its obligations under the Contract is the result of an event of Force Majeure.

  - For the purpose of this clause "Force Majeure" means an event beyond the control of the Supplier and not involving the Supplier's fault or negligence and not foreseeable. Such events may include, but are not restricted to, acts of the purchaser, in the contractual capacity, wars or revolution, fires, floods, epidemic, pandemic, quarantine restrictions and freight embargoes.
  - If a Force Majeure situation arises, the Supplier shall promptly notify the Purchaser in writing of such condition and the cause thereof. Unless otherwise directed by the Purchaser in writing the Supplier shall continue to perform their obligations under the Contract as far as reasonably practicable, and shall adopt all reasonable alternative means for performance not prevented by Force De Majeure clause.
  - In case of any delay in performance of the scope of work, due to Force Majeure event, the timeline for such work shall automatically get extended for such period, affected due to Force Majeure event.

- **Exit Management:**

  The Supplier shall ensure a smooth and structured exit process at the end of the contract period or upon termination, to facilitate full transition of services and operational responsibility to NICL or any third party designated by NICL, without disruption.

  - Exit Management Plan:

    The Supplier shall submit a detailed Exit Management Plan within Six (6) months of contract signing. The plan must address:
    - Knowledge transfer, including documentation (As-Built, HLD, LLD, SOPs, asset registers)
    - Transfer of information assets, operational artifacts, and intellectual property (if applicable)
    - Support for transitioning services, tools, and processes to NICL or a successor entity

    The Exit Plan must be reviewed and updated annually, and approved by NICL.

  - Transition Obligations
    - The Supplier shall support a minimum **two-month transition** period, extendable at NICL's discretion, under the same terms as the existing contract.
    - During transition, no key resources may be removed or reallocated without NICL's written consent.
    - The Supplier shall ensure all deployed infrastructure and services are handed over in operational condition.
    - All data, configurations, logs, and system access credentials must be returned to NICL in native formats.

  - Continuity & Compliance
    - Services must continue as per SLA during transition, without any degradation.
    - The Supplier shall not introduce any changes during this period unless approved by NICL.
    - Reverse transition support must be provided to enable takeover by NICL or its designated vendor.

- The Supplier must comply with all regulatory and audit requirements during handover.

- Knowledge Transfer: The Supplier shall:
  - Train NICL's personnel or successors on service delivery tools, procedures, and configurations
  - Provide documentation, release/version details of tools, and assist in software/hardware transitions
  - Explain operational processes (e.g., incident, change, and problem management)
  - Support NICL in coordinating with third-party vendors for continuity

- Default & Penalties: Failure to support transition or unwillingness to cooperate during exit may attract penalties and deductions from the Supplier's payments or performance guarantee, at NICL's discretion. This Exit Management Clause shall survive the expiration or termination of the contract, regardless of cause.

- **Compliance:**
  - Compliance with NICL's Information Security Policies; Prior to Supplier deploying any of its Personnel or engaging any person to perform Services for NIC; the Supplier shall, at a minimum, with respect to each such Personnel comply with NICL's Information security policy/ies (ISP/s), as may be amended from time to time. Supplier hereby acknowledges that it has received a copy of the current ISP/s simultaneously with the execution of this Agreement. Supplier shall not assign any Personnel to perform the Services under this Agreement who does not comply with the provisions of the ISP/s. NICL shall have the right to audit Supplier's books and records/facilities / location / places prepared or kept in connection with the Services provided under this RFP, at all reasonable times and places to ensure compliance with the ISP/s, to the extent applicable.

  - **Compliance with all applicable laws:** The Bidder shall undertake to observe, adhere to, abide by, comply with and notify NICL about all laws in force or as are or as made applicable in future, pertaining to or applicable to them, their business, their employees or their obligations towards them and all purposes of this RFP and shall indemnify, keep indemnified, hold harmless, defend and protect NICL and its employees/ officers/ staff/ personnel/ representatives/agents from any failure or omission on its part to do so and against all claims or demands of liability and all consequences that may occur or arise for any default or failure on its part to conform or comply with the above and all other statutory obligations arising there from. Supplier agrees that it will abide by the provisions of the DPDP Act, 2023 - 11th August, 2023; CG-DL-E-12082023-248045 as and when the relevant rules and guidelines come into force.

  - **Compliance in obtaining approvals/permissions/licenses:** The Bidder shall promptly and timely obtain all such consents, permissions, approvals, licenses, etc., as may be necessary or required for any of the purposes of this project or for the conduct of their own business under any applicable Law, Government Regulation/Guidelines and shall keep the same valid and in force during the term of the project, and in the event of any failure or omission to do so, shall indemnify, keep indemnified, hold harmless, defend, protect and fully compensate NICL and its employees/ officers/ staff/ personnel/ representatives/ agents from and against all claims or demands of liability and all consequences that may occur or arise for any default or failure on its part to conform or comply with the above and all other statutory obligations arising there from

and NICL will give notice of any such claim or demand of liability within reasonable time to the Bidder. This indemnification is only a remedy for NICL. The Bidder is not absolved from its responsibility of complying with the statutory obligations as specified above. Indemnity would be limited to court awarded damages and shall exclude indirect, consequential and incidental damages. However indemnity would cover damages, loss or liabilities suffered by NICL arising out of claims made by its customers and/or regulatory authorities.

- The Supplier shall ensure that all data, including logs, configurations, reports, and event records generated or handled under this contract shall reside and be processed within India, in compliance with prevailing GoI data localization directives.
- **The Bidder shall comply with all the terms and conditions given in this RFP Document.**

- **Personnel:**

  The Supplier shall remain solely responsible for the conduct, performance, and safety of its employees, agents, and representatives ("Personnel") deployed under this contract. NICL shall not be liable for any act or omission of the Supplier's Personnel.

  - **Conduct and Compliance**
    - Personnel must adhere to NICL's policies, maintain discipline, and conduct themselves in a professional and non-disruptive manner at all times.
    - Each deployed individual must carry a valid ID card issued by the Supplier.
    - NICL reserves the right to reject or request replacement of any Personnel without assigning reasons. Replacement shall be provided promptly without service disruption.

  - **Behavior and Accountability**
    - Personnel must not engage in unlawful, negligent, or unauthorized activities, including tampering with or misusing NICL's systems, data, or property.
    - The Supplier shall be liable for any loss or damage to NICL caused by such acts and shall compensate NICL accordingly.

  - **Background Checks and Safety**
    - Only Personnel who have cleared appropriate background verification shall be deployed at NICL premises.
    - The Supplier shall maintain adequate insurance coverage for all legal liabilities, including injury, death, or property damage related to its Personnel.
    - NICL shall bear no responsibility for any personal claims or liabilities arising in connection with the Supplier's Personnel.

  - **Security and Access**
    - Personnel must comply with NICL's security protocols and exercise care in the use of facilities and infrastructure.
    - Any violation of NICL's access, data, or security requirements may result in immediate denial of entry or removal from premises.

  - **Handover Obligations**

On written instruction from NICL, the Supplier shall promptly return all materials, documents, and equipment provided by NICL. Damage or loss to such items shall be compensated by the Supplier.

- **Liability and Indemnity:**
  The Supplier shall be fully accountable for:
  - **Any** damage or loss suffered by NICL due to acts or omissions of its Personnel; and
  - Any penalties or sanctions imposed on NICL due to misconduct or non-compliance by the Supplier or its Personnel.

- **Notice**

  Any notice by one party to the other pursuant to the Contract shall be sent in written format by fax/email and confirmed in writing to the address specified for that purpose in the Contract.

- **Applicable Law**

  This Agreement shall be construed, interpreted and applied in accordance with and shall be governed by the laws **applicable in India** including applicable export and import laws. The **courts at Kolkata** shall have the exclusive jurisdiction to entertain any dispute or proceeding arising out of or in relation to this Agreement.

- **Arbitration**

  If any dispute or difference shall arise, such difference shall independently of all other questions be referred to the decision of a sole arbitrator to be appointed in writing by the parties or if they cannot agree upon a single arbitrator within 30 days of any party invoking arbitration, the appointment shall be made upon request by a party, by the Chief Justice of the High Court at Calcutta, or any person or institution designated by him in accordance with the provisions of the Arbitration and Conciliation Act, 1996 as amended or re-enacted from time to time. It shall be a condition precedent to any right of action or suit upon the Contract that award by such arbitrator/arbitrators of the amount of the loss or damage shall be first obtained. The seat of such arbitration shall be at Kolkata.

  Note: The Arbitral Tribunal shall determine all matters in disputes other than EXCEPTED MATTERS as below:-

  - *Scope of Work,*
  - *SLA,*
  - *Minimum Technical and Function Specification,*
  - *Discrepancies (varying or conflicting provisions among documents, agreement),*
  - *Suspension or discontinuation of work,*
  - *Acceptance of deliverables*
  - *In the above EXCEPTED MATTERS, the decision of NICL will be final, conclusive and binding on the parties hereto and shall be without appeal*

- **Cyber Security Insurance:**

  The selected vendor shall maintain a valid **Cyber Security Insurance Policy** to cover potential liabilities arising from the execution of services, including:

- Accidental data exposure,
- Disruption of services,
- Breach of confidentiality,
- Malicious code deployment, or
- Errors arising from vulnerability assessments, penetration testing, audit, forensics, and red team activities.

  Minimum Insurance Coverage: INR **5 Crores** (₹5,00,00,000).

  The insurance policy must be:
- Issued by a reputed insurer authorized to operate in India,
- Valid throughout the duration of the contract,
- Specific to the activities outlined in this RFP.
- **Proof of Insurance** (e.g., certificate of insurance, policy document) must be submitted by the vendor **prior to signing the Contract** with NICL.
- NICL reserves the right to verify and demand renewal/extension of the insurance if services continue under any extension clause.

- **Non-Disclosure Agreement (NDA):**

  The vendor shall sign a **Non-Disclosure Agreement (NDA)** prior to onboarding, to safeguard all confidential information shared or accessed during the engagement, including but not limited to:

  - Infrastructure diagrams,
  - System logs,
  - Personally Identifiable Information (PII),
  - VAPT findings,
  - Audit reports,
  - Forensic evidence,
  - Exploit chain details, etc.

    The NDA shall be binding on:
- All employees and subcontractors of the vendor involved in the engagement.
- Any third-party subcontractors or entities engaged by the vendor for part of the scope, subject to NICL's approval.

  The vendor shall ensure:
- All shared data and evidence are encrypted using **AES-256 or equivalent** during transmission.
- All sensitive evidence is stored in secure, access-controlled systems.
- Data retention aligns with applicable laws and regulations.

  Minimum Retention Period: **3 years** from date of collection/submission, unless otherwise specified by NICL or regulatory authorities.

  The vendor shall **comply with the provisions of the DPDP Act 2023**, and **IRDAI Information and Cyber Security Guidelines, 2023 (as updated March 24, 2025)**, especially those pertaining to:
- Protection of personal data,

- Confidentiality,
- Data retention and disposal,
- Reporting of breach or misuse

- Intentionally Left Blank
- Intentionally Left Blank
- Intentionally Left Blank

11. Annexures

- **Annexure I: Pre-Qualification and Technical Bid Letter**

To

NATIONAL INSURANCE COMPANY LIMITED
Head Office: Premises No.18-0374, Plot No. CBD-81, New Town, Kolkata-700156

Dear Sir,

Sub.: RFP Number - NICL/IT/RFP/VAPT_Cyber SecurityAudit_RedTeaming/18/2025

Date:

Sir,

We hereby declare

1. We/our principals are equipped with adequate manpower for providing the Services as per the parameters laid down in the RFP Document and we are prepared for live/technical demonstration of our capability and preparedness before the representatives of NICL. We/our principals are also equipped with adequate maintenance and service facilities within India for supporting the offered document.
2. We hereby offer to provide the Services at the prices and rates as mentioned in the Commercial Bid .
3. We do hereby undertake that, in the event of acceptance of our bid, the Services shall be provided as stipulated in the RFP and that we shall perform all the incidental services.
4. We enclose herewith the complete Technical Bid as required by you. This includes:

    - **Pre-Qualification Bid - Table-B and supporting Annexures**
    - **Undertaking for providing authorized representatives of IRDAI the right to inspection, investigation, obtaining information:**
    - **Declaration by Bidder: No Conflict of Interest**
    - **EMD/Bid Security**
    - **Proof of Payment of Bid Fee**
    - **Power of Attorney - in favor of the official signing the Bid**
    - **Format of Certificate for Tenders for Works under Rule 144 (xi) in the General Financial Rules (GFRs), 2017**
    - **Integrity Pact**

- **Technical Bid Letter**
- **Technical Bid Particulars: Table- C, Section - 3.4, Section - 3.5 and supporting Annexures**
- **Details of the proposed manpower deployment**
- **Details of proposed methodology and timeline (in a separate sheet)**

We agree to abide by our offer for a period of one year from the date fixed for opening of the Commercial Bid and that we shall remain bound by a communication of acceptance within that time.

We have carefully read and understood the terms and conditions of the RFP Document and the conditions of the Contract applicable to the bid and we do hereby undertake to provide services as per these terms and conditions.

We do hereby undertake, that, until a formal contract is prepared and executed, this bid, together with your written acceptance thereof or placement of letter of intent awarding the contract, shall constitute a binding contract between us.

Dated this, the day of 20

Signature: .....

Name of the authorized signatory .....

Designation .....

Duly authorized to sign the RFP Response for and on behalf of: ..... (Name and Address of Company)

Company Seal:

- **Annexure II: Commercial Bid Letter**

To

NATIONAL INSURANCE COMPANY LIMITED
Head Office: Premises No.18-0374, Plot No. CBD-81, New Town, Kolkata-700156

Dear Sir,

Sub.: RFP Number - NICL/IT/RFP/VAPT_Cyber SecurityAudit_RedTeaming/18/2025

Date:

Sir,

We hereby declare

1.We hereby offer to provide the Services at the prices and rates mentioned in the Commercial Bid.

2.We do hereby undertake that, in the event of acceptance of our bid, the Services shall be provided as stipulated in the RFP Document and that we shall perform all the incidental services.

3.We enclose herewith the complete Commercial Bid as required by you. This includes:

Table-D:

We agree to abide by our offer for a period of one year from the date of opening of the Commercial Bid and that we shall remain bound by a communication of acceptance within that time.

We have carefully read and understood the terms and conditions of the RFP Document and the conditions of the Contract applicable to the bid and we do hereby undertake to provide services as per these terms and conditions.

We do hereby undertake, that, until a formal contract is prepared and executed, this bid, together with your written acceptance thereof or placement of letter of intent awarding the contract, shall constitute a binding contract between us.

Dated this, the day of 20

Signature: .....

Name of the authorized signatory .....

Designation .....

Duly authorized to sign the RFP Response for and on behalf of: ..... (Name and Address of Company)

Company Seal:

- **Annexure III: Format of Contract between Supplier and NICL**

THIS Memorandum of Understanding/Agreement is made on this day of , 20 BETWEEN M/s. and carrying on business at

(hereinafter referred to as "SUPPLIER" and shall include its heirs, successors or permitted assigns) of the First Part and NATIONAL INSURANCE COMPANY LIMITED, a Company registered under the Companies Act, 1956 having its registered Head Office at Premises No.18-0374, Plot No. CBD-81, New Town, Kolkata-700156 (hereinafter referred to as "PURCHASER" and shall include its heirs, successors or permitted assigns) of the Second Part.

WHEREAS the Vendor is in the business of a) Vulnerability Assessment and Penetration Testing - VAPT, Cyber Security Audit and Red Teaming Services,

AND WHEREAS the Purchaser intends to Procure b)Vulnerability Assessment and Penetration Testing - VAPT, Cyber Security Audit and Red Teaming Services as detailed in the RFP and has explained to the Supplier the purposes and uses for which the procurement is being made.

AND WHEREAS the Supplier has assured that the Solution in respect of " b" as mentioned above which they would supply would be fit for the purposes of the Purchaser and has been agreed to relieve the "PURCHASER" from the Principle of "CAVEAT EMPTOR" being the Purchaser is a mere consumer hereby it is better to rely on SUPPLIER as to the fulfillment of the purpose/s of the purchase/procurement and/or installation and maintenance.

AND WHEREAS the Purchaser invited bids from Bidders for submitting bids for supply of all the mentioned in the Purchaser's Invitation in the RFP Document , containing broad terms and conditions, for the supply, installation, commissioning, maintenance etc. as detailed in the RFP document.

AND WHEREAS the Supplier submitted a bid and bids were submitted by some other Bidders.

AND WHEREAS out of the several bids when opened the Purchaser found the price quoted by the Supplier to be eligible to be awarded the contract.

AND WHEREAS the Purchaser would place orders on the Supplier for the purchase as mentioned in the RFP Document and in the bid/offer Papers on the terms, conditions and specifications mentioned therein and in the Purchase Order issued on 20 .

AND WHEREAS the parties herein intend to set out the terms and conditions for such purchase and maintenance and matters connected therewith and to define the mutual rights and obligations of the parties herein.

NOW THESE PRESENTS WITNESSETH and the parties herein agree as follows:

1.Scope:

The RFP Document , along with Corrigendum and Addendums and the bid/offer documents will form part of and shall be deemed to have been incorporated in these presents but in case of any conflict between any term in the said documents and in these presents the term of these presents will have overriding effect and the said documents have to be read and will have effect subject to these presents.

2.Resolution of Disputes: Insert Section - 2.54

i)Prevention of Corruption: Each Party shall comply with all Applicable Laws relating to bribery and corruption and shall not do, or omit to do, any act that will cause the other Party to be in breach of any such Applicable Law, and in doing so: (i) shall not give or receive any bribes, including in relation to any public official; and (ii) shall maintain an effective anti-bribery compliance regime, that monitors compliance and detects violations.

ii)Notices:For the purpose of all notices, the address of the Supplier and the Purchaser shall be those given in the beginning of these presents.

As the Purchaser's Registered Head Office is situated within the Jurisdiction of the High Court at Calcutta all disputes and differences are subject to the Jurisdiction of The Calcutta High Court.

3.Compliance with Terms and Conditions: The Supplier will comply with all the Terms and Conditions given in this RFP Document, and the Corrigendum, Addendums in respect of the same and in line with its bid and Offer. The Service Level Agreement and the Purchase Order shall be deemed to form and be read and construed as part of this Contract.

IN WITNESS WHEREOF the parties hereto have executed these presents on the day, month and year first above written.

SIGNED SEALED AND DELIVERED FOR

By the hands of Shri/Smt.

In presence of Shri/Smt.

In presence of Shri/Smt.

SIGNED SEALED AND DELIVERED FOR 'NICL'

By the hands of Shri/Smt. In presence of Shri/Smt. In presence of Shri/Smt.

- **Annexure IV: Format for Integrity Pact:**

IEM Details: https://nationalinsurance.nic.co.in/en/independent-external-monitors-iems

On non-judicial stamp paper INTEGRITY PACT

Between

National Insurance Company Limited (NICL) hereinafter referred to as "The Principal"

And

hereinafter referred to as "The Bidder/ Contractor" Preamble

e Principal intends to award, under its laid down organizational procedures, the contract for the deployment of skilled manpower resources for operations, maintenance, monitoring, and support of tools and technologies under various SOC initiatives as outlined in the Objective of the RFP. The Principal emphasizes full compliance with all applicable laws, regulations, and guidelines, and upholds principles of transparency, fairness, and responsible resource utilization in its engagement with Bidder(s) and Contractor(s).

In order to achieve these goals, the Principal will appoint Independent External Monitors (IEMs) who will monitor the tender process and the execution of the contract for compliance with the principles mentioned above.

Section 1- Commitments of the Principal

1.The Principal commits itself to take all measures necessary to prevent corruption and to observe the following principles:

a.No employee of the Principal, personally or through family members, will in connection with the tender for, or the execution of a contract, demand, take a promise for or accept, for self or third person, any material or immaterial benefit which the person is not legally entitled to.

b.The Principal will, during the tender process, treat all Bidder(s) with equity and reason. The Principal will in particular, before and during the tender process, provide to all Bidder(s) the same information and will not provide to any Bidder(s) confidential / additional information through which the Bidders could obtain an advantage in relation to the tender process or the contract execution.

c.The Principal will exclude from the process all known prejudiced persons.

2.If the Principal obtains information on the conduct of any of its employees which is a criminal offense under the IPC/PC Act, or if there be a substantive suspicion in this regard, the Principal will inform the Chief Vigilance Officer and in addition can initiate disciplinary actions.

Section 2- Commitments of the Bidder(s)/ Contractor(s)

1.The Bidder(s)/ Contractors(s) commit themselves to take all measures necessary to prevent corruption. The Bidder(s)/ Contractors(s) commit themselves to observe the following principles during participation in the tender process and during the contract execution:

a.The Bidder(s)/ Contractors(s) will not, directly or through any other person or firm, offer, promise or give to any of the Principal's employees involved in the tender process or the execution of the contract or to any third person any material or other benefit which he/she is not legally entitled to, in order to obtain in exchange any advantage of any kind whatsoever during the tender process or during the execution of the contract.

b.The Bidder(s)/ Contractors(s) will not enter with other Bidders into any undisclosed agreement or understanding, whether formal or informal. This applies in particular to prices, specifications, certifications, subsidiary contracts, submission or non-submission of bids or any other actions to restrict competitiveness or to introduce cartelization in the bidding process.

c.The Bidder(s)/ Contractors(s) will not commit any offense under the relevant IPC/PC Act, further the Bidder(s)/ Contractor(s) will not use improperly, for purposes of competition or personal gain, or pass on to others, any information or document provided by the Principal as part of the business relationship, regarding plans, technical proposals and business details, including information contained or transmitted electronically.

d.The Bidder(s)/ Contractors(s) of foreign origin shall disclose the name and address of the Agents/ representatives in India, if any. Similarly the Bidder(s)/Contractor(s) of Indian Nationality shall furnish the name and address of the foreign principals, if any.

e.The Bidder(s)/ Contractor(s) will, when presenting their bid, disclose any and all payments made, committed to or intended to make to agents, brokers or any other intermediaries in connection with the award of the contract.

f.Bidder(s)/Contractor(s) who have signed the Integrity Pact shall not approach the Courts while representing the matter to IEMs and shall wait for their decision in the matter.

2.The Bidder(s)/ Contractor(s) will not instigate third persons to commit offenses outlined above or be an accessory to such offenses.

Section 3 - Disqualification from tender process and exclusion from future contracts

If the Bidder(s)/Contractor(s), before award or during execution has committed a transgression through a violation of Section 2, above or in any other form such as to put their reliability or credibility in question, the Principal is entitled to disqualify the Bidder(s)/Contractor(s) from the tender process..

Section 4 - Compensation for Damages

1.If the Principal has disqualified the Bidder(s) from the tender process prior to the award according to Section 3, the Principal is entitled to demand and recover the damages equivalent to Earnest Money Deposit/ Bid Security.

2.If the Principal has terminated the contract according to Section 3, or if the Principal is entitled to terminate the contract according to Section 3, the Principal shall be entitled to demand and recover from the Contractor liquidated damages of the Contract value or the amount equivalent to Performance Bank Guarantee.

Section 5- Previous transgression

1.The Bidder declares that no previous transgressions occurred in the last three years with any other Company in any country conforming to the anti-corruption approach or with any Public Sector Enterprise in India that could justify his exclusion from the tender process.

2.If the Bidder makes an incorrect statement on the subject, he can be disqualified from the tender process.

Section 6 -Equal treatment of all Bidders / Contractors / Subcontractors

1.In case of Subcontracting (only, if allowed in writing by the Principal, refer Section - 46), the Principal Contractor shall take the responsibility of the adoption of Integrity Pact by the Sub-contractor.

2.The Principal will enter into agreements with identical conditions as this one with all Bidders and Contractors.

3.The Principal will disqualify from the tender process, all Bidders who do not sign this Pact or violate its provisions.

Section 7- Criminal charges against violating Bidder(s)/Contractor(s) / Subcontractor(s)

If the Principal obtains knowledge of conduct of a Bidder, Contractor or Subcontractor, or of an employee or a representative or an associate of a Bidder, Contractor or Subcontractor which constitutes corruption, or if the Principal has substantive suspicion in this regard, the Principal will inform the same to the Chief Vigilance Officer.

Section 8- Independent External Monitor

1.The Principal appoints competent and credible Independent External Monitor for this Pact after approval by Central Vigilance Commission. The task of the Monitor is to review independently and objectively, whether and what extent the parties comply with the obligations under this agreement.

2.The Monitor is not subject to instruction by the representatives of the parties and performs his her functions neutrally and independently. The Monitor would have access to all Contract documents, whenever required. It will be obligatory for him / her to treat the information and documents of the Bidder(s)/ Contractor(s) as confidential. He/ she reports to the Chairman Cum Managing Director, NICL.

3.The Bidder(s)/Contractor(s), accepts that the Monitor has the right to access without restriction to all Project documentation of the Principal including that provided by the Contractor. The Contractor will also grant the Monitor, upon his/her request and demonstration of a valid interest, unrestricted and unconditional access to the project documentation. The same is applicable to Subcontractors.

4.The Monitor is under contractual obligation to treat the information and documents of the Bidder(s)/Contractor(s)/ Sub-contractor(s) with confidentiality. The Monitor has also signed declarations on

'Non-Disclosure of Confidential Information' and 'Absence of Conflict of Interest'. In case of any conflict of interest arising at a later date, the IEM shall inform Chairman Cum Managing Director, NICL and recuse himself / herself from that case.

5.The Principal will provide to the Monitor sufficient information about all meetings among the parties related to the Project provided such meetings could have an impact on the contractual relations between the Principal and the Contractor. The parties offer to the Monitor the option to participate in such meetings.

6.As soon as the Monitor notices, or believes to notice, a violation of this agreement, he/she will inform the Management of the Principal and request the Management to discontinue or take corrective action or to take other relevant action. The monitor can in this regard submit non-binding recommendations. Beyond this, the Monitor has no right to demand from the parties that they act in a specific manner, refrain from action or tolerate action.

7.The Monitor will submit a written report to the Chairman Cum Managing Director, NICL within 8 to 10 weeks from the date of reference or intimation to him by the Principal and should the occasion arise, submit proposals for correcting problematic situations.

8.If the Monitor has reported to the Chairman Cum Managing Director, NICL, a substantiated suspicion of an offense under relevant IPC PC Act, and the Chairman Cum Managing Director, NICL has not within the reasonable time taken visible action to proceed against such offense or reported it to the Chief Vigilance Officer, the Monitor may also transmit this information directly to the Central Vigilance Commissioner.

9.The word 'Monitor' would include both singular and plural.

The Principal has appointed below independent external monitors for this program

1.**Shri Animesh Chauhan**

Address: Flat No. 948, G Block, 6th Avenue, Gaur City 1,

Sector 4, Greater Nadia (West), Uttar Pradesh - 201009

e-mail id: animeshchau@gmail.com

2.**Shri S Srinivasan**

Address: 0-5-107, Block No. 5, V-Floor, Kendriya Vihar, B.B. Road,

(Bangalore-Bellary Road), Yelahanka, Bangalore-560064 Karnataka

e-mail id: s.srinivasan1980@gmail.com

***Note: Appointment of Independent External Monitors (IEMs)**

The Principal had earlier appointed the above Independent External Monitors (IEMs) for this program in accordance with the guidelines issued by the Central Vigilance Commission (CVC):

However, both the above-mentioned IEMs have since retired, and the appointment of new IEMs by the CVC is currently awaited. In view of project timelines and the need to initiate the procurement process without delay, the RFP is being issued in the interim.

The names and contact details of the newly appointed IEM(s), once communicated by the CVC, shall be duly shared with all participating Bidders during the course of the RFP process.

*Bidders are advised to take note of the above. This arrangement is made to ensure adherence to transparency and integrity principles without delaying the procurement timelines.***

Section 9 - Pact Duration

This Pact begins when both parties have legally signed it. It expires for the Contractor 12 months after the last payment under the contract, and for all other Bidders 6 months after the contract has been awarded. Any violation of the same would entail disqualification of the Bidders and exclusion from future business dealings.

If any claim is made / lodged during this time, the same shall be binding and continue to be valid despite the lapse of this pact as specified above, unless it is discharged / determined by Chairman Cum Managing Director of NICL.

Section 10- Other provisions

1.This agreement is subject to Indian Law. Place of performance and jurisdiction is Registered Office of the Principal, i.e. Kolkata.

2.Changes and supplements as well as termination notices need to be made in writing. Side agreements have not been made.

3.Should one or several provisions of this agreement turn out to be invalid, the remainder of this agreement remains valid. In this case, the parties will strive to come to an agreement to their original locations.

4. Issues like Warranty/ Guarantee etc. shall be outside the purview of IEMs.

(For and on behalf of the Principal) (Office Seal)

Place:

Date:

Witness 1: (Name & Address) (For and on behalf of the Bidder/ Contractor) (Office Seal)

Place:

Date:

Witness 1:

(Name & Address)

Witness 2:

(Name & Address)

Witness 2:

(Name & Address)

- **Annexure V: Format for Declaration by Bidder: No Conflict of Interest:**

Sample Format of absence of Conflict of Interest to be submitted by Bidder in their Official Letterhead

To

NATIONAL INSURANCE COMPANY LIMITED
Head Office: Premises No.18-0374, Plot No. CBD-81, New Town, Kolkata-700156 Dear Sir,

Sub.:

Date:

Re: Declaration regarding No Conflict of Interest (COI) in Public Procurement

We, hereby declare that the participation by our bidding firm

… or any of our affiliates that are neither involved in the

consultancy contract to which this procurement is linked; nor we are part of more than one bid in the procurement; nor our bidding firm or our organization personnel have relationships or financial or business transactions with any official of Procuring Entity i.e. M/s National Insurance Company Limited who are directly or indirectly related to the tender or execution process of contract; nor have access to information to gain unfair advantage in the procurement process. We, also confirm that:

1. We, or our constituent do not have common controlling shareholding or other ownership interest

2.Any constituent of us……is not a constituent of another Bidder.

3.We, …… do not have the same legal representation with any other Bidder for the purpose of the bid.

4.We, …… do not have any relationship with any other Bidder that puts us in a position to allow access to each other's information or to influence the bid of any other Bidder.

5. We,……have not participated in preparation of any document, design or technical specification for the project.

Signature of Bidder Dated :

Place :

Seal

- **Annexure VI: Intentionally Kept Blank**
- **Annexure VII: Format for Performance Bank Guarantee**

BANK GUARANTEE FOR PAYMENT (TO BE SUBMITTED IN NON-JUDICIAL STAMP PAPER OF APPROPRIATE VALUE PURCHASED IN THE NAME OF THE ISSUING BANK)

To

NATIONAL INSURANCE COMPANY LIMITED

Head Office: Premises No.18-0374, Plot No. CBD-81, New Town, Kolkata-700156 Dear Sirs,

Sub.: RFPNo. - NICL/IT/RFP/VAPT_Cyber SecurityAudit_RedTeaming/18/2025 Date: ……..

In consideration of your having issued a Purchase Order for the procurement of items as per RFP with M/s.
……
…… (hereinafter referred to as "the Supplier", which expression shall, unless repugnant to the context or meaning thereof, include its successors, legal heirs, and permitted assigns), and your agreement to pay a sum of Rs. …… (Rupees ……) as per the terms of the Contract/Supply Order/Purchase Order No. …… dated …… (hereinafter referred to as "the PO"), and based on your requirement for furnishing a guarantee in the manner hereinafter stated, we, …… (Banker's Name), having our registered office at …… and branch located at ……, hereby issue this guarantee…

DO HEREBY COVENANT AND AGREE AS FOLLOWS:

We, Bank Ltd. having our office located at …… do hereby undertake to indemnify National Insurance Company Limited or their heirs, successors or permitted assigns (hereinafter referred to as 'NICL') and keep indemnified to the extent of the sum of Rs (Rupees

…) from and against all losses and damages that may be caused to NICL in relation to the payment to be made by NICL to the Supplier as aforesaid by reason of any default or defaults on the part of the Supplier in the due supply of services for carrying out any work or discharging supplier's obligation as per the said contract in the observance and performance of any of the terms and conditions relating thereto in accordance with the true intent and meaning thereof and in the event of any default or defaults on the part of the Supplier as aforesaid we shall forthwith on demand and without demur pay to NICL any sum not exceeding in the total the said sum of Rs. …….. (Rupees ……..) As may be claimed by NICL to be due from the Supplier by way of refund of such payment or any portion or otherwise as NICL's losses and / or damages, costs charges or expenses incurred by reason of such default or defaults on the part of the Supplier as aforesaid.

Notwithstanding anything to the contrary, NICL's decision as to whether the Supplier has made any such default or defaults and the amount or amounts to which NICL is entitled by reasons thereof will be binding on us and we shall not be entitled to ask NICL to establish their claim or claims under this guarantee, but will pay the same forthwith on NICL's demand without any protest or demur.

This guarantee shall continue and hold good until it is released by NICL on the applications by the Supplier after completion of delivery of services / terms and conditions at site provided that this guarantee shall in no event remain in force after the day of …….. Without prejudice to NICL's claim or claims arisen and demanded from or otherwise notified to us in writing on or before the seventh day after the said date of expiry of the guarantee which will be enforceable against us notwithstanding that the same is or not enforced after the said date.

Should it be necessary to extend this guarantee on account of any reason whatsoever, we undertake to extend the period of this agreement till such time with the Supplier's consent on the request by NICL, provided the terms and conditions relating to the extension of the Guarantee are satisfied.

NICL will have the fullest liberty without affecting this guarantee, either to vary, or to modify and to revoke any of the terms and conditions of the said PO or to extend the time of performance of the Supplier or to postpone for any time or from time to time any of NICL's rights or powers against the Supplier and either to enforce or to forbear to enforce any of the terms and conditions of the said PO and we shall not be released from our liability under this guarantee by the exercise of NICL's liberty. With reference to matters aforesaid or by reason of any time being given to the Supplier, or any other forbearance, act or omission on NICL's part or any indulgence by NICL to the Supplier or by any variation or modification of the said PO or any other act, matter or things whatsoever, which under the law relating to sureties, would but for the provisions hereof, have the effect of so releasing us from our liability hereunder provided always nothing herein contained will enlarge our liability hereunder beyond the limit of Rs. ..... (Rupees) As aforesaid or extend the period of the guarantee beyond the said day of Unless expressly agreed to by us in writing.

This guarantee shall not in any way be affected by NICL's taking or varying or giving up any securities from the Supplier or any other person, firm or company on their behalf or by winding up, dissolution, insolvency or death as the case may be of the Supplier or his company/firm.

In order to give full effect to the guarantee herein contained, NICL shall be entitled to act as if we were your principal debtors in respect of all NICL's claims against the Supplier hereby guaranteed by us as aforesaid.

Subject to the maximum limit of our liability as aforesaid, this guarantee will cover all NICL's claim or claims against the Supplier from time to time arising out of or in relation to the said PO and in respect of which NICL's claim in writing is lodged on us on or before the seventh day after expiry of this guarantee.

Any notice by way of demand or otherwise hereunder may be sent by special courier, telex, fax, email or registered post to our local address as aforesaid and if sent by post, it shall be deemed to have been lodged / given / submitted when the same is posted.

This guarantee and the powers and provisions herein contained, are in addition to and not by way of limitation of or substitution for any other guarantee or guarantees hereto before given to NICL by us and now existing un-cancelled and that this guarantee is not intended to and shall not revoke or limit such guarantee or guarantees.

This guarantee shall not be affected by any change in the constitution of the Supplier or us nor shall it be affected by any change in your constitution or by amalgamation or absorption thereof or therewith but will ensure to the benefit of and be available to and enforceable by the absorbing or amalgamated company or concern.

This guarantee shall come into force on and shall not be revoked by us whether before it's coming into force or any time during its currency without NICL's prior consent in writing.

We further agree and undertake to pay to NICL the amount demanded by NICL in writing irrespective of any dispute or controversy between NICL and the Supplier

Notwithstanding anything contained hereinabove our liability under this agreement is restricted to Rs …… (Rupees ……..) . Unless a written claim is lodged on us for payment under this guarantee within seven days of the date of expiry of this guarantee i.e. on or before …….. all NICL's rights under this guarantee shall be forfeited and we shall be deemed to have been released and discharged from all liabilities thereunder, irrespective of whether or not the original guarantee is returned to us, discharged.

We have power to issue this guarantee in NICL's favor under the Memorandum and Articles of Association of our Bank and the undersigned has full power to execute this guarantee under the Power of Attorney granted to him by the Bank.

SIGNED AND DELIVERED ON THE DAY OF …… FOR & ONBEHALF OF THE …

BANK LTD.

FOR & ON BEHALF OF (BANKER'S NAME)

Branch Manager

(Banker's seal)

Address……

……

P.S.:The amount referred to above will be as per the terms of payment specified

- **Annexure VIII: Intentionally Kept Blank**

- **Annexure IX: Format for EMD/Bid Security:**

To
NATIONAL INSURANCE COMPANY LIMITED
Head Office: Premises No.18-0374, Plot No. CBD-81, New Town, Kolkata-700156

Sub.: RFP Number - NICL/IT/RFP/VAPT_Cyber SecurityAudit_RedTeaming/18/2025

Date:

Dear Sir,

Whereas **.....** (hereinafter referred to as "the Bidder") has submitted its bid dated **.....** for the **.....** (hereinafter referred to as "the Bid");

NOW, KNOW ALL MEN BY THESE PRESENTS that we, **.....** having our registered office at **.....** (hereinafter referred to as "the Bank"), are firmly bound unto **The National Insurance Company Limited** (hereinafter referred to as "the Purchaser") in the sum of **Rupees .....** (Rs. .....), for the payment of which, the Bank hereby binds itself, its successors and assigns, firmly and irrevocably by these presents.

Sealed with the Common Seal of the said Bank this **..... day of ....., 20.....**.

The Conditions of this obligation are:

If the Bidder withdraws his bid during the period of bid validity specified by the Bidder in the bid; or

If the Bidder, having been notified of the acceptance of its bid by the Purchaser during the period of bid validity

i.Fails or refuses to execute the Contract; or

ii.Fails or refuses to furnish the Performance Security, in accordance with the instructions to Bidder.

We undertake to pay to the Purchaser up to the above amount upon receipt of its first written demand, without the Purchaser having to substantiate its demand, provided that in its demand the Purchaser will note that the amount claimed by it is due to it owing to the occurrence of one or both of the two conditions, specifying the occurred condition or conditions.

This guarantee will remain in force up to and including 45 days after the period of bid validity, and any demand in respect thereof should reach the Bank not later than the above date.

Signature of Bidder Dated :

Place :

Seal

- **Annexure X: Undertaking for providing authorized representatives of IRDAI the right to inspection, investigation, obtaining information:**

To
NATIONAL INSURANCE COMPANY LIMITED
Head Office: Premises No.18-0374, Plot No. CBD-81, New Town, Kolkata-700156

Sub.: RFP Number - NICL/IT/RFP/VAPT_Cyber SecurityAudit_RedTeaming/18/2025

Date:

Dear Sir,

Undertaking from the Bidder for providing authorized representatives of the IRDAI the right to inspection, investigation, obtaining information for Tender Ref No: NICL/IT/RFP/MANPOWER/14/2025

We hereby undertake to provide authorized representatives of Insurance Regulatory Development Authority of India (IRDAI) right to:

(a)examine the books, records, information, systems and the internal control environment to the extent that they relate to the service being performed for the company for NICL under this contract and

(b)access to any internal audit reports or external audit findings for the service being performed for the company for NICL under this contract.

Signature of Bidder Dated :

Place :

Seal :

- **Annexure XI: Format of Certificate for Tenders for Works under Rule 144 (xi) in the General Financial Rules (GFRs), 2017**

To
NATIONAL INSURANCE COMPANY LIMITED
Head Office: Premises No.18-0374, Plot No. CBD-81, New Town, Kolkata-700156

Sub.: RFP Number - NICL/IT/RFP/VAPT_Cyber SecurityAudit_RedTeaming/18/2025

Date:

Dear Sir,

Bidder Name:

We, M/s are a private/public limited company/LLP/Firm incorporated under the provisions of the

Companies Act, 1956/2013 Limited Liability Partnership Act 2008/ Indian Partnership Act 1932, having our registered office at ----------(referred to as the "Bidder") are desirous of participating in the Tender Process in response to your captioned RFP and in this connection we hereby declare, confirm and agree as under:

a)We, the Bidder have read and understood the contents of the Office Memorandum & the Order (Public Procurement No.1) both bearing no. F.No.6/18/2019/PPD of 23rd July 2020 issued by Ministry of Finance, Government of India on insertion of Rule 144 (xi) in the General Financial Rules (GFRs) 2017 and the amendments & clarifications thereto, regarding restrictions on availing/procurement of goods and services, of any Bidder from a country which shares a land border with India and / or sub-contracting to contractors from such countries.

b)In terms of the above and after having gone through the said amendments including in particular the words defined therein (which shall have the same meaning for the purpose of this Declaration cum Undertaking), we the Bidder hereby declare and confirm that:

* We, the Bidder are not from such a country which shares a land border with India, in terms of the said amendments to GFR, 2017. or *We, the Bidder are from such a country and has been registered with the Competent Authority i.e. the Registration Committee constituted by the Department for Promotion of Industry and Internal Trade, as stated under Annexure I to the said Office Memorandum / Order and we submit the proof of registration herewith. (*Delete whichever is not applicable)

c)We, the Bidders agree and undertake that if the contract is awarded to us, we will not sub-contract or outsource the contract and / or any part thereof unless such subcontract/ outsourcing is permitted by NICL in writing, in which case we shall not subcontract or outsource the work to a contractor from such countries, unless such contractor is registered with the Competent Authority and proof of same is obtained.

2.We, the Bidders hereby confirm that we fulfill all the eligibility criteria as per RFP and are not ineligible from participating in the Tender in view of the above Office Memorandum and Order. We also agree and accept that if our declaration and confirmation is found to be false at any point of time including after awarding the contract, NICL shall be within its right to forthwith terminate the contract/ bid without notice to us and initiate such action including legal action against us. NICL shall also be within its right to forfeit the security deposits provided by us and also recover from us the loss and damages sustained by NICL on account of the above.

3.This declaration cum undertaking is executed by us through our Authorized signatory/ies after having read and understood the Office Memorandum and Order (Public Procurement No.1) both bearing F.No.6/18/2019/PPD of 23rd July 2020 of Ministry of Finance, Department of Expenditure, Public Procurement Division, Government of India including the words defined in the said order (reproduced hereunder) which shall have the same meaning for the purpose of this Declaration cum Undertaking.

Definitions:

"Bidder from a country which shares a land border with India" for the purpose of this Order means:

a)An entity incorporated, established or registered in such a country; or

b)A subsidiary of an entity incorporated, established or registered in such a country; or

c)An entity substantially controlled through entities incorporated, established or registered in such a country; or

d)An entity whose beneficial owner is situated in such a country; or

e)An Indian (or other) agent of such an entity; or

f)A natural person who is a citizen of such a country; or

g)A consortium or joint venture where any member of the consortium or joint venture falls under any of the above

"Beneficial owner" for the purpose of above will be as under:

(i)In case of a company or Limited Liability Partnership, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person(s), has a controlling ownership interest or who exercises control through other means. Explanation—

a."Controlling ownership interest" means ownership of, or entitlement to, more than twenty-five per cent of shares or capital or profits of the company;

b."Control" shall include the right to appoint the majority of the directors or to control the management or policy decisions, including by virtue of their shareholding or management rights or shareholders agreements or voting agreements;

(i)In case of a partnership firm, the beneficial owner is the natural person(s)who, whether acting alone or together, or through one or more juridical person, has ownership of entitlement to more than fifteen percent of capital or profits of the partnership;

(ii)In case of an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has ownership of or entitlement to more than fifteen percent of the property or capital or profits of such association or body of individuals;

(iii)Where no natural person is identified under (i) or (ii) or (iii) above, the beneficial owner is the relevant natural person who holds the position of senior managing official;

(iv)In case of a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with fifteen percent or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

"Agent" for the purpose of this Order is a person employed to do any act for another, or to represent another in dealings with third persons."

Dated this, the day of 20

Signature: .....

Name of the authorized signatory .....

Designation .....

Duly authorized to sign the RFP Response for and on behalf of: (Name and Address

of Company) Company Seal:

*Note: Where applicable, evidence of valid registration by the Competent Authority shall be attached.

-
-

- **Annexure XII: Format for CV Submission, including:**

  All proposed personnel must have the relevant qualifications and certifications as mentioned in Section 3.4 and a minimum of **5 years of experience in BFSI or relevant Cyber Security domains**. All certifications must be active at the time of proposal submission.

  a. Cover Page for Each CV

Field	Details
Name of Resource	
Proposed Role	
Employment Status	(Permanent / Contract / Sub-contracted)
Proposed Duration of Deployment	From DD/MM/YYYY to DD/MM/YYYY
Contact Email	

Mobile Number	
Reporting Manager (at Vendor)	
Assigned Project(s)	VAPT / Audit / Forensics / Red Teaming
Summary of Experience	XX Years

b. Educational Qualifications

Degree	University/ Institute	Year of Completion	Percentage/CGPA

c. Professional Certifications

Certification	Issuing Authority	Certification ID	Valid Till	Attached Copy (Yes/No)
OSCP, CEH, CISA, etc.	Offensive Security / ISC² / ISACA / etc.			

d. Domain Expertise (Mark Applicable)

Domain	Relevance	Years of Experience	Example Projects

Network VAPT	Yes/ No		
Web & API VAPT	Yes/ No		
Cloud Security	Yes/ No		
Cyber Security Audit (IRDAI/ISO)	Yes/ No		
Digital Forensics	Yes/ No		
Malware Analysis	Yes/ No		
Red Teaming / Adversary Simulation	Yes/ No		

e. Relevant Project Experience Summary (Minimum 3 Projects)

Project Title	
Client Name	(BFSI preferred)
Engagement Duration	From DD/MM/YYYY to DD/MM/YYYY

Project Type	VAPT / Audit / Forensics / Red Team / Other
Tools Used	Burp Suite, Nmap, Splunk, MISP, etc.
Scope	e.g., 500 IPs, 15 Apps, 3 Cloud Environments
Key Contributions	
Reporting Output	Executive Summary, Detailed Findings, etc.

f. Declaration

I hereby declare that the above information is true and correct to the best of my knowledge. Copies of relevant documents are enclosed.

Signature of Candidate
Date: DD/MM/YYYY
Authorized Signatory (Vendor HR/Manager):
Company Stamp (with date):

- **Annexure XIII: Sample Consent Form for Social Engineering Testing**

To: [Vendor Name]
From: [Employee Name], [Designation], National Insurance Company Limited
Date: [Insert Date]

I, [Employee Name], voluntarily provide my informed consent to participate in social engineering testing activities (including but not limited to phishing simulations, vishing calls, or other authorized awareness assessments) conducted by [Vendor Name] as part of the Cyber Security assessment under RFP No. NICL/IT/RFP/VAPT_Cyber SecurityAudit_RedTeaming/18/2025.

I acknowledge and understand the following:

- The tests will simulate real-world social engineering tactics strictly for the purpose of assessing and enhancing NICL's Cyber Security awareness and resilience.
- These activities shall not involve any unauthorized access, harm, or misuse of personal or confidential information.

- All tests shall be conducted in accordance with applicable laws and regulations, including the Information Technology Act, 2000, the Digital Personal Data Protection (DPDP) Act, 2023, and relevant IRDAI Information and Cyber Security Guidelines, 2023 (as updated March 24, 2025).
- Results from these assessments will be anonymized, used solely for internal security posture improvement, and will not be used for any disciplinary or punitive action without due process.
- I have the right to seek clarification from NICL's Information Security Team before signing this form.

Signature of Employee: _____
Date: _____
Approved by (NICL CISO): Name: [Insert Name]
Signature: _____
Date: _____

***Note**:*
*The selected vendor shall **collect and submit signed consent forms for all participating employees** to the office of the **CISO, NICL**, before the commencement of any social engineering activity. Testing must not begin unless such consent documentation is in place.*

- Intentionally Kept Blank

12. Format for Queries from Bidders

Bidders have to provide their queries on scope of work, terms & conditions etc. in the below format in excel file only (xlsx). Bidders should **NOT MERGE ROWS OR COLUMNS**. Bidders should provide a reference of the page number, state the clarification point and the queries/suggestion/modification that they propose as shown below

Sl. No.	RFP Document Page No.	Point/ Section No.	Term stated in RFP document	Bidder's Query/Suggestion /Modification

***** End of Document *****