

TERMS OF REFERENCE (TORs)

THIRD-PARTY COMPREHENSIVE SECURITY AUDIT OF DATA WAREHOUSE PLATFORM

1. ISSUED BY:

Punjab Information Technology Board (PITB) Lahore.

2. BACKGROUND AND RATIONALE

Online Statistical System in Punjab (OSSP) is a Government-wide enterprise data platform developed with the aim of integrating ICT systems across all Government departments to enable secure integration, management, standardization, and analysis of data. The platform currently integrates 142 ICT systems across 34 government departments, bringing together standardized, non-personal and anonymized datasets to support data-driven governance and evidence-based decision-making.

As part of OSSP, a centralized Data Lake and Data Warehouse environment has been deployed to facilitate the ingestion, storage, processing, transformation, standardization, and analytical use of data received from diverse government systems. The platform also incorporates data integration and API capabilities, Master Data Management (MDM), metadata management, data scheduling and orchestration, Business Intelligence (BI), dashboards, reporting, and analytical tools, providing a unified environment for enterprise-level data management, analytics, and reporting.

OSSP further serves as a foundational data layer for Artificial Intelligence (AI) initiatives and OneMap Punjab, the Government's spatial-visualization platform. These capabilities enable cross-sectoral analytics, data visualization, reporting, intelligent insights, and spatial analysis to support evidence-based planning and decision-making.

Given the Government-wide scope of OSSP and its role in consolidating and processing data from multiple government systems, the security, confidentiality, integrity, availability, and resilience of the platform and its underlying data assets are of strategic importance. The platform encompasses multiple technology and control layers, including infrastructure, networks, data lake, data warehouse, databases, MDM, data integration pipelines, APIs, applications, identity and access management, data protection, and operational security controls.

Accordingly, Punjab IT Board (PITB) intends to engage an independent and qualified consultancy firm to conduct a comprehensive security audit of the OSSP platform, assess its overall security posture and compliance, identify vulnerabilities and control deficiencies, and provide prioritized, risk-based recommendations to strengthen its security and cyber resilience.

3. OBJECTIVE OF THE ASSIGNMENT

The objective of this engagement is to conduct an independent, comprehensive security audit of the on premise Data Lakehouse. The assessment will comprehensively evaluate security architecture, data governance, access management, access controls, data protection mechanisms, operational security, and technical safeguards across all infrastructure, platform, database, and application layers against industry standards to identify security gaps, vulnerabilities risks, control gaps, and non-compliance risks.

4. SCOPE OF WORK

The selected IT Audit Firm shall perform, at a minimum, the following activities:

A. Infrastructure Security

The Auditee is required to perform a security audit covering, but not limited to, the following areas:

- 1) Cloud
- 2) Physical and virtual server
- 3) Hypervisor
- 4) Operating system
- 5) Storage
- 6) Baseline configuration
- 7) Patch management
- 8) High Availability
- 9) Capacity and resilience
- 10) Backup and Disaster Recovery

B. Network Security

The selected audit firm shall perform a security audit covering, but not limited to, the following areas:

- 1) Internal Network
- 2) External Perimeter
- 3) Network Segmentation
- 4) Firewall
- 5) WAF
- 6) Reverse Proxies
- 7) IDS/IPS
- 8) Load Balancers
- 9) VPN
- 10) Router and Switch
- 11) DNS
- 12) Protocols
- 13) NAC
- 14) Wireless (if applicable)

C. Identity & Access Management

The selected audit firm shall perform an Identity and Access Management (IAM) security audit covering, but not limited to, the following areas:

- 1) User Lifecycle management
- 2) Identity Governance
- 3) Authentication
- 4) Authorization (RBAC / ABAC)
- 5) Privileged Access Management
- 6) Service Accounts
- 7) AD (LDAP)
- 8) Administrative Access

D. Application Security

The selected audit firm shall perform an Application Security Audit covering in-scope applications, including but not limited to:

- 1) Web Portals
- 2) APIs
- 3) Reporting Dashboards
- 4) BI Applications

The audit shall cover, but not be limited to, the following areas:

- 1) Secure Tools & Technology
- 2) Secure Design
- 3) Secure Development
- 4) Secure Configuration
- 5) Secure Session management
- 6) Secure Communication
- 7) Secure Data Management
 - a. Structured
 - b. Unstructured
- 8) Exception & Error Management
- 9) Logs & Trails
- 10) Secrets
- 11) Dependencies (Application Composition)

E. Platform Security

The selected audit firm shall perform a Platform Security Audit covering in-scope open-source tools and technologies, including but not limited to:

- 1) Data Lake
- 2) Structured/Unstructured data engines
- 3) Data pipeline orchestrator
- 4) Data streaming engine
- 5) Data visualization tool
- 6) Git repository

The audit shall cover, but not be limited to, the following areas:

- 1) Tools & Technologies
- 2) Data Pipelines
- 3) Distributed Queries
- 4) Message Broker
- 5) Analytics Platform
- 6) Reporting Platform
- 7) CI/CD Pipelines
- 8) Configuration
- 9) Orchestration
- 10) Cluster
- 11) Node
- 12) Services
- 13) Secrets
- 14) Multi-Tenancy
- 15) Platform Resilience

F. Database Security

The selected audit firm shall perform a Database Security Audit covering in-scope databases and data storage technologies, including but not limited to:

- 1) Tools & Technology
- 2) Design
- 3) Development
- 4) Configuration

- 5) Session management
- 6) Data Management
 - a. Structured
 - b. Unstructured
 - c. Meta Data
- 7) Exception & Error Management
- 8) Logs & Trails
- 9) Secrets
- 10) Hardening
- 11) Authentication
- 12) Authorization (RBAC/ABAC)
- 13) Encryption
 - a. In Transit
 - b. At Rest
 - c. Backup
- 14) Data masking
- 15) Critical Data Protection
- 16) Tokenization
- 17) Secure Archival
- 18) Secure Disposal

G. Configuration & Hardening

The selected audit firm shall perform a secure configuration and hardening assessment of all applicable in-scope infrastructure, operating systems, network devices, applications, databases, platforms, services and supporting components.

H. Vulnerability Assessment

The selected audit firm shall perform a Vulnerability Assessment covering all applicable in-scope infrastructure, operating systems, applications, databases, platforms, network components and supporting technologies.

I. Penetration Testing

The selected audit firm shall perform Penetration Testing of applicable in-scope applications, APIs, infrastructure, network-facing services, platforms and other technically testable assets, subject to an agreed scope and Rules of Engagement.

J. Logging, Monitoring & Security Operations

The selected audit firm shall perform a security assessment of Logging, Monitoring and Security Operations across all applicable in-scope infrastructure, applications, platforms, databases, network components and supporting services.

K. Business Continuity & Cyber Resilience

The selected audit firm shall perform a Business Continuity and Cyber Resilience Assessment covering, but not limited to, the following areas:

- 1) Backup strategy
- 2) Backup restoration testing
- 3) Disaster Recovery capability
- 4) High Availability validation
- 5) Recovery objectives (RTO/RPO)
- 6) Cyber resilience
- 7) Business continuity controls

5. AUDIT METHODOLOGY

The selected audit firm shall employ and share a documented audit methodology aligned with industry standards and internationally recognized cybersecurity assessment and auditing practices. The methodology shall be appropriate to the scope of the engagement and shall ensure that all audit activities are evidence-based, repeatable, and independently verified. The audit firm may use its proprietary methodology, provided it meets or exceeds the minimum requirements specified in this ToR.

6. DELIVERABLES

The deliverables shall be based on the Pakistan Information Security Framework (PISF) 2026 format/template (where applicable) and standard industry best practices.

Timeline	Deliverable
Week 1-6	1. Security Assessment of all above in-scope 2. Evidence Repository 3. Final Technical Audit Report 4. Executive Presentation
Week7- 8	Remediation Recommendation Report
Week 9-16	Audit Closure Report

7. DURATION OF THE CONTRACT

Unless otherwise agreed in writing:

1. Total engagement duration shall not exceed Four (4) months.
2. An initial assessment report shall be submitted within the first 6 weeks.
3. The final reports shall be submitted after incorporation of review comments and completion of all agreed activities

8. ESTIMATED COST OF THE ASSIGNMENT:

The total estimated cost for the said assignment is Rs. 9.5 Million.

9. EXECUTION SCHEDULE

The consultant Firm shall complete the deliverables as per scope of work & expected outputs, as per mentioned timelines in deliverables section (section 4) above (from the issuance of the Work Order).

10. ACCEPTANCE CRITERIA

The engagement shall be considered successfully completed only upon fulfillment of all of the following conditions:

- 1) Completion of all agreed audit activities in accordance with the approved scope and methodology.
- 2) Submission of all contractual deliverables in the agreed format.
- 3) Submission of all supporting evidence and audit documentation.
- 4) Delivery of the Final Technical Audit Report and Executive Presentation.
- 5) Presentation of findings to designated Government stakeholders.
- 6) Submission of the Consolidated Risk Register and remediation roadmap.
- 7) Completion of remediation validation activities
- 8) Submission of the Remediation Validation Report
- 9) Resolution of all review comments provided by the procuring agency on submitted reports.
- 10) Audit Closure Report

11. LIQUIDATED DAMAGES

If the Consultant fails / delays in performance of any of the obligations, under the work order / violates any of the provisions of the work order / commits breach of any of the terms and conditions of the work order, the Purchaser may, without prejudice to any other right of action / remedy it may have, deduct from the work order Price, as liquidated damages, a sum of money @0.25% of the total work order Price which is attributable to such part of the Services / the Works, in consequence of the failure / delay, be put to the intended use, for every week between the scheduled delivery date(s), with any extension of time thereof granted by the Purchaser, and the actual delivery date(s). Provided that the amount deducted shall not exceed, in the aggregate, 10% of the work order Price.

12. INTELLECTUAL PROPERTY RIGHTS

All intellectual property rights will rest with PITB/Government of Punjab.

Confidentiality and compliance with government data protection policies are mandatory. All source code, AI/ML models, and documentation must be handed over to the PITB.

13. CONFIDENTIALITY, ETHICS AND PROFESSIONAL CONDUCT

The Consultant firm shall:

A. CONFIDENTIALITY

- i. Execute a Non-Disclosure Agreement (NDA) prior to commencement of the engagement.
- ii. Ensure that all information, records, configurations, source code, credentials, logs, reports, and other sensitive information obtained during the engagement remain confidential.
- iii. Use information obtained during the audit solely for the purposes of the engagement.
- iv. Not disclose, copy, retain, or distribute Government information without prior written authorization.
- v. Securely return or permanently destroy all Government information upon completion of the engagement, if required by the procuring agency.

B. PERSONNEL SECURITY

- i. Ensure that all personnel assigned to the engagement are authorized, suitably qualified, and bound by confidentiality obligations.
- ii. Comply with all applicable Government security clearance, background verification, and access control requirements.
- iii. Ensure that only authorized personnel are granted access to Government facilities, systems, and information.

C. PROFESSIONAL CONDUCT

- i. Perform the engagement independently and objectively.
- ii. Exercise due professional care and professional judgment throughout the engagement.
- iii. Immediately report any critical security vulnerabilities or active security incidents identified during the audit.
- iv. Avoid any activity that could adversely impact the confidentiality, integrity, or availability of production systems.

D. TESTING RESTRICTIONS

- i. Obtain prior written approval before performing intrusive testing, exploitation activities, denial-of-service testing, or any activity that could affect production services.
- ii. All activities must be performed on-premises. Limited remote access may be subjected to approval by senior management. Otherwise, on-premises activities will be performed and

restricted data/information will not be directly accessible but through a designated and authorized staff member.

- iii. Coordinate testing activities with designated Government representatives.
- iv. Conduct testing within approved maintenance windows where applicable.
- v. Immediately suspend testing if instructed by the procuring agency.

E. CONFLICT OF INTEREST

The firm shall disclose any actual, potential, or perceived conflicts of interest prior to commencement of the engagement and throughout the audit.

F. LEGAL AND REGULATORY COMPLIANCE

The firm shall comply with all applicable Government laws, regulations, security policies, privacy requirements, and contractual obligations throughout the engagement.

14. ELIGIBILITY REQUIREMENTS:

CRITERIA FOR SELECTION

Only consultant firms meeting the following technical evaluation criteria would be considered for the financial evaluation:

Category	Requirement
Legal (Mandatory)	1. Firm must be registered with relevant authorities with valid certification for at least 5 years. 2. Valid Provincial Sales Tax (PST) Registration (Status = Active with relevant authority) <u>Single undertaking covering following aspects:</u> 1. Submission of undertaking that the firm is not blacklisted by any of Provincial or Federal Government Department, anywhere in Pakistan. 2. Compliance to the scope of services mentioned under TORs of this document. 3. In full compliance of the Execution Schedule and Delivery Period mentioned in this document. 4. Must have demonstrated experience of delivering similar assignments in global market.

Business Age	Relevant Experience & Value of Projects (Last 3 Years) – Minimum 02 Projects, must be above PKR 250 M (Verifiable through relevant purchase orders / contracts)
Financial	Average Annual Turnover (Last 05 Years), must be above PKR 250 M

Standing	(Verifiable through Audit statement of last three financial years):
Sector Experience	Auditor Qualification and Experience (must provide documentary evidences, verifiable purchase orders, CVs of proposed team along with required certifications etc.) a. General and Domain-Specific Experience 1) Minimum Experience: The auditing firm must possess a minimum of 5 years of demonstrated experience delivering enterprise cybersecurity audits, penetration testing, and architecture reviews. 2) Lead Auditor / Principal Assessor: Must have at least 8 years of dedicated cybersecurity experience, including leading complex data security assessments in enterprise environments. 3) Technical Assessors & Testers: Must have a minimum of 5 years of hands-on experience in penetration testing, infrastructure assessments, and database/platform security reviews. 4) Data Lakehouse Expertise: The proposed team must demonstrate proven expertise (minimum 5 years or 3 completed engagements) auditing on premise Data Lake / Lakehouse architectures and big data ecosystems. b. Mandatory Professional Certifications The assessment team must collectively hold valid, industry-recognized credentials corresponding to their assigned roles on the engagement: 1) Audit Lead & Security Architecture: Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), or equivalent credential. 2) Technical & Penetration Testing Lead: Offensive Security Certified Professional (OSCP), CREST Registered Tester (CRT), GIAC Penetration Tester (GPEN), or equivalent credential. 3) Advanced Technical Assessors (Offensive/Specialized): Offensive Security Experienced Penetration Tester (OSEP), Offensive Security Web Expert (OSWE), GIAC Exploit Researcher and Advanced Penetration Tester (GXPN), or equivalent advanced certifications. c. Compliance & Governance Familiarity 1) The team must demonstrate verifiable experience auditing against major cybersecurity frameworks and compliance standards, including NIST SP 800-53, NIST Cybersecurity Framework (CSF), CIS Benchmarks, ISO/IEC 27001, and applicable regional data privacy regulations (e.g., GDPR, local data protection acts). d. Proof of Capability & Deliverables 1) Case Studies: The vendor must supply at least two (2) anonymized case

	studies or references of similar security audits performed on large-scale, on-premise data platform environments within the past 3 years. 2) Key Personnel Commitment: Named personnel with the required certifications and experience must be explicitly assigned to the project; substitution of key personnel without prior written consent is strictly prohibited.
--	---

15. SCOPE OF FINANCIAL PROPOSAL AND PAYMENT SCHEDULE

Financial proposals of consultants fulfilling the above evaluation criteria will be considered for financial evaluation and the consultant will be selected on least cost selection method as per PPRA Rules, 2014.

16. PAYMENT PLAN

Timeline	Deliverable	Payment
Week 6	1. Security Assessment of all above in-scope 2. Evidence Repository 3. Final Technical Audit Report 4. Executive Presentation	30%
Week 8	Remediation Recommendation Report	20%
Week 16	Audit Closure Report	50%

Payment will be made upon successful delivery of each deliverable as per the schedule detailed above in Section No 4.

- I. The agreed consultancy fee includes all charges and expenses related to the scope and deliverables.
- II. No payment other than the agreed consultancy fee shall be made under this contract. The consultancy firm shall not be entitled to claim any additional charges, reimbursements, or incidental expenses beyond the agreed fee.

17. PROPOSAL SUBMISSION

The firms are required to submit proposals in a single package consisting of two separate envelopes, containing separately the technical and financial proposals, the envelopes shall be marked as ***“Technical Proposal”** and **“Financial Proposal”** – **no later than 16th Oct, 2026 sharp 1100 Hours.** **The proposals shall be opened same day 1130 Hours.** In the first instance, the “Technical Proposal” shall be opened and the envelope marked as “Financial Proposal” shall be retained unopened in the custody of the procuring agency and subsequently, the financial proposals of technically qualified consultants will be opened and considered for financial evaluation.

Note: *firm(s) who participated in establishment of MDM platform (Data Lake and Data Warehouse) are not eligible to participate in the subject Security Audit.*