



REQUEST FOR PROPOSAL NUMBER: AF/AP/RFP26007/2026

Date: September 10, 2026

RFP Deadline: September 30, 2026

REQUEST FOR PROPOSAL

NAME: RFP for L1 & L2 MANAGED SUPPORT SERVICES

CONFIDENTIALITY

No part of this document may be disclosed verbally or in writing, including by reproduction, to any third party without the prior written consent of ATOMA Pay. This document, its associated appendices and any attachments remain the property of ATOMA Pay and shall be returned upon request.

ATOMA PAY

L1 & L2 MANAGED SUPPORT SERVICES

Requirements and Statement of Work

Vendor-Neutral Solicitation Document

Huawei Mobile Money Platform and Connected ATOMA Pay Services

Document Owner	ATOMA Pay - IT Product and Service Delivery
Version	1.1
Issue Date	10 September 2026
Purpose	Request technical and commercial proposals from qualified managed-service providers

This document contains confidential operational requirements and shall only be used for proposal preparation.

TENDERER'S ACKNOWLEDGEMENT/ PRELIMINARY NON-DISCLOSURE AGREEMENT.**Tender's Acknowledgment: Please mark as appropriate:**

We acknowledge receipt and acceptance of the RFP and intend to submit a tender as required ☐

We acknowledge receipt of the RFP but decline to tender for the following reasons: ☐
Please write your reason here: _____

- We undertake to return to ATOMA Pay within the below-mentioned deadline from receipt of the complete RFP package with all attachments, information and documents related thereto as provided by ATOMA Pay and any copies made thereof.
- The complete tender documents along with the Proposal to be submitted in a SEALED envelope addressed to the Supply Chain Department of ATOMA Pay and to be physically submitted in the tender box located in ATOMA Pay Head Office, Reception, located in Shar-E-Naw Kabul not later than **Dated 24/September/2026**.
- Bidders are requested to do the registration at ATOMA Pay at the time of obtaining the RFP from ATOMA Pay reception.
- Bidders should ensure that they provide accurate email addresses and contact numbers at the time of registration.
- Bids are invited from reputable companies for **"Request for Proposal for L1 & L2 MANAGED SUPPORT SERVICES"** according to ATOMA Pay requirements and Technical Specifications as per RFP.
- Bid received after the mentioned deadline shall not be accepted.
- ATOMA Pay reserves the right to accept or reject any or all bids and to annul the bidding at any time, without thereby incurring any liability to the affected supplier(s) or any obligations to inform the affected supplier(s) on the grounds of ATOMA Pay's action.

12: Preliminary Non-Disclosure Agreement:

We agree that all information and documents contained in or related to this RFP as provided by ATOMA pay is proprietary information and shall be treated as confidential. We undertake that all such information and documents, as described above, shall not be divulged to any other party (such prohibition applies to any further release of information regarding this RFP by ATOMA Pay) without the prior written permission from ATOMA Pay to do so. We agree that this RFP and all information and documents relating to it and provided hereunder by ATOMA Pay are not to be used for any purpose other than for the preparation of our tender submission. This undertaking will also apply to any subsequent contract resulting from this RFP.

Name: _____

Designation: _____

Signed / Date / Stamped: _____

Document Control

Field	Details
Document title	L1 & L2 Managed Support Services Requirements
Service owner	ATOMA Pay - IT Product and Service Delivery
Intended recipients	Invited managed-service providers and approved subcontractors
Contract term	Vendor to propose for an initial 12-month term, renewable subject to performance
Commercial status	No pricing is prescribed in this document; suppliers shall submit a separate commercial response
Confidentiality	All platform, customer, transaction, network, integration and security information is confidential
Revision note	Version 1.1 strengthens financial-integrity monitoring, operational readiness, lifecycle management, ticket quality and configuration-drift controls.

Document Structure

- 1. Purpose and objectives
- 2. Service environment
- 3. Scope of services
- 4. Coverage and operating model
- 5. Incident severity and service levels
- 6. IT service management requirements
- 7. Monitoring and support tools
- 8. Staffing and competency requirements
- 9. Deliverables and reporting
- 10. Governance and escalation
- 11. Security, compliance and access control
- 12. Transition, knowledge transfer and exit
- 13. Service continuity and disaster recovery
- 14. Vendor proposal response requirements
- 15. Acceptance and performance management
- Appendices: RACI, compliance checklist and commercial response template
-

Mandatory response rule: The supplier shall answer every requirement as Comply, Partially Comply, or Do Not Comply and shall explain any assumptions, dependencies or exclusions. Silence will be treated as non-compliance.

1. Purpose and Objectives

ATOMA Pay intends to appoint a qualified managed-service provider to deliver Level 1 (L1) and Level 2 (L2) operational and application support for the Huawei Mobile Money platform and its connected channels, integrations and supporting components. The selected supplier will be responsible for stable daily operation, rapid incident restoration, proactive monitoring, technical troubleshooting, controlled configuration activities and continuous service improvement.

The primary objectives are to:

- Provide a single, accountable support function for all production and non-production platform incidents and service requests.
- Maintain 24x7 visibility of platform health, transaction processing, interfaces, batch jobs, alarms, capacity and service availability.
- Reduce service disruption through preventive maintenance, proactive detection, clear escalation and timely coordination with Huawei/OEM Level 3 and third parties.
- Apply consistent ITSM processes for incident, problem, change, request, access, release, configuration and knowledge management.
- Maintain complete operational documentation, shift handover records, knowledge articles, runbooks and auditable support evidence.
- Provide transparent SLA, KPI, trend and capacity reporting to ATOMA Pay management.

2. Service Environment

The managed-service scope covers the Huawei Mobile Money platform and all technical dependencies required to provide ATOMA Pay services. The final component inventory will be confirmed during transition and shall be maintained in a controlled configuration register.

- Huawei Mobile Money application components, portals, webcare functions and platform services.
- Customer, agent, merchant and administrative channels, including mobile applications, USSD, web interfaces and APIs where applicable.
- Integrations with billing/OCS, CBS, SMS/OTP, identity/KYC systems, payment systems, banks, external wallets, card/payment gateways and third-party service providers.
- Application servers, middleware, databases, schedulers, file transfers, certificates, queues, interfaces, logs and platform-specific utilities within the agreed responsibility boundary.
- Production, disaster-recovery, UAT, staging and test environments included in the approved support inventory.
- Monitoring, ticketing, reporting and operational tools used to manage the service.

Scope confirmation: The supplier shall perform a discovery exercise and submit a detailed service inventory, dependency map, support boundary and responsibility matrix within the transition period.

3. Scope of Services

3.1 Level 1 Support Requirements

L1 support shall be the first operational point of contact and shall continuously monitor the platform, receive alerts and requests, perform approved initial recovery actions and maintain communication until closure or escalation.

- Operate a 24x7x365 service desk and surveillance function for the agreed production services.
- Monitor alarms, dashboards, service KPIs, transaction success rates, interface status, batch jobs, queues, resource utilization and critical log events.

- Receive incidents and requests through the approved ticketing system, telephone, email and authorized operational channels.
- Record complete ticket information including detection time, affected service, business impact, symptoms, evidence, actions, owner and next update time.
- Perform first-level validation and approved troubleshooting using runbooks, knowledge articles, health checks and standard operating procedures.
- Execute safe, pre-approved restoration actions such as service checks, controlled restarts, queue validation, job reruns and connectivity verification, subject to access and change controls.
- Handle standard service requests, account support, password reset coordination, user guidance and basic configuration tasks approved for L1.
- Validate whether an issue is platform-related, network-related, integration-related, data-related or third-party-related and route it to the correct owner.
- Escalate incidents to L2 without delay when the issue exceeds L1 authority, knowledge, access or SLA limits.
- Maintain regular customer/stakeholder communication in accordance with incident severity update intervals.
- Prepare shift handover records and ensure no open incident, alarm, change or risk is lost between shifts.
- Create and update knowledge-base articles for recurring issues, standard checks and approved solutions.
- Support planned activities, post-change verification, production smoke tests and post-go-live monitoring.
- Provide daily platform health and operations reports.
- Perform scheduled end-to-end synthetic transaction checks for agreed critical customer, agent and merchant journeys, and retain evidence of the results.
- Complete start-of-day, end-of-day and business-cycle checklists covering critical jobs, settlement files, reconciliations, scheduled processes and interface acknowledgements.
- Detect, record and escalate financial transaction exceptions including pending, duplicate, timed-out, partially completed, orphaned, failed and unreconciled transactions.
- Maintain ticket-queue hygiene by ensuring correct ownership, priority, categorization, aging control, duplicate linkage, action history and closure validation for every ticket.
- Verify restoration through actual service and transaction-flow testing, and obtain business confirmation for high-impact incidents where required before closure.
- Identify any monitoring gap, undocumented dependency or missing runbook discovered during operations and ensure it is assigned for correction and tracked to closure.

3.2 Level 2 Support Requirements

L2 support shall provide in-depth technical analysis and restoration for incidents escalated by L1. L2 remains responsible for technical ownership, coordination and closure even where Huawei/OEM L3 or another third party is engaged.

- Analyze application, middleware, database, API, integration, transaction, system and security logs to isolate faults and identify root cause.
- Reproduce issues in controlled environments where feasible and compare successful and failed transaction flows.
- Perform advanced troubleshooting of interfaces, service endpoints, certificates, schedulers, queues, files, database sessions, application processes and platform configurations.
- Implement approved intermediate fixes, configuration corrections and controlled operational workarounds.
- Prepare technical change plans, methods of procedure (MOP), implementation steps, rollback plans, verification plans and activity reports.
- Coordinate patches, releases, hotfixes and vendor recommendations with ATOMA Pay, Huawei/OEM L3, infrastructure, network, security and business teams.
- Own incident bridges for major incidents and provide structured technical updates, decisions, risks and action tracking.
- Perform problem management, recurring-incident trend analysis, known-error recording and permanent corrective-action tracking.

- Produce formal root-cause analysis (RCA) reports for P1 incidents, repeated P2 incidents and any incident requested by ATOMA Pay.
- Support database, backup, restore, archival, reconciliation and data-correction activities within approved procedures and segregation-of-duty controls.
- Support access management, privilege review, audit evidence, service-account maintenance and certificate/credential expiry tracking.
- Coordinate with Huawei/OEM L3 for product defects, source-code issues and changes outside standard tools; track vendor cases until final closure.
- Maintain technical documentation, dependency diagrams, configuration baselines, runbooks and troubleshooting guides.
- Perform proactive performance tuning, capacity analysis and recommendations before resource thresholds are breached.
- Investigate and reconcile discrepancies across the wallet ledger, CBS/OCS, banks, payment gateways, partner wallets and external service providers, with full evidence and ownership until resolution.
- Perform any production data correction only through an approved, auditable procedure with maker-checker authorization, backup/rollback protection and post-correction reconciliation; unauthorized direct database updates are prohibited.
- Maintain and periodically verify configuration baselines across production, DR, UAT and test environments, identify configuration drift and document approved differences.
- Manage the technical lifecycle of certificates, licenses, service accounts, keys, supported software versions and OEM end-of-support dates, with formal 90/60/30-day expiry or obsolescence alerts.
- Perform operational-readiness assessments for new services, integrations, releases and major changes, confirming monitoring, support ownership, capacity, security, runbooks, rollback and escalation readiness before production acceptance.
- Prepare complete diagnostic evidence packages for Huawei/OEM L3 and third parties, including timestamps, transaction/reference IDs, logs, traces, request/response samples, topology context and reproduction steps.
- Support vulnerability remediation, security patch validation and emergency technical changes in coordination with ATOMA Pay security and change-management teams.
- Identify and propose safe automation for repetitive health checks, alert correlation, evidence collection and reporting, subject to ATOMA Pay approval and security review.

3.3 Business Configuration and Integration Support

Although the primary engagement is for L1 and L2 support, the supplier shall provide operational business-configuration and integration support where the change can be completed using standard platform tools and approved procedures.

- Gather, analyze and clarify configuration requests from ATOMA Pay IT Product and Service Delivery.
- Assess impact, dependencies, security, rollback and testing requirements before implementation.
- Configure approved products, fees, limits, rules, menus, user profiles, notifications, service parameters and channel settings using standard tools.
- Support API and interface configuration, connectivity validation, test execution and issue analysis for approved integrations.
- Prepare a change request specification for any requirement that requires Huawei/OEM product development or non-standard modification.
- Execute changes only after formal approval and within agreed maintenance windows.
- Provide implementation evidence, test results, updated documentation and post-change monitoring.

3.4 Exclusions Unless Separately Agreed

- New product development or source-code modification by the Huawei/OEM vendor.
- Major platform upgrades, migrations or expansion projects not included in the agreed annual plan.

- Infrastructure, network or security engineering outside the agreed support boundary, while coordination and evidence collection remain in scope.
- Commercial operations, customer call-center services and field-agent support unless explicitly included in the final contract.

4. Coverage and Operating Model

Service Function	Minimum Coverage Requirement
L1 monitoring and service desk	24x7x365, including public holidays, with continuous shift handover.
L2 technical support	Business-hours presence plus 24x7 on-call coverage for P1/P2 incidents and approved critical activities.
On-site support	At least one named L2 application/integration resource on-site during agreed business hours; exceptions require ATOMA Pay approval.
Planned activities	Support during approved maintenance windows, including nights and weekends, without additional charge where included in the agreed service calendar.
Major incident support	Immediate bridge participation and continuous technical ownership until service restoration and formal handover.
Language	Operational communication and reports in English; supplier should provide local-language support where operationally necessary.
Location and remote access	Remote access only through ATOMA Pay-approved secure channels; supplier shall maintain local capability for urgent on-site intervention.

The supplier shall submit a detailed shift plan, backup roster, leave-coverage plan and on-call schedule. Resource shortages, annual leave, sickness or resignation shall not reduce contracted coverage or SLA performance.

5. Incident Severity and Service Levels

The following are minimum service levels. The supplier may propose improved targets but may not weaken them without explicit written agreement. SLA timing begins at the earliest of monitoring detection, ticket creation or notification to the supplier.

Priority	Business Impact / Example	Acknowledgement	Technical Engagement	Workaround / Restore Target	Update Frequency	RCA
P1 - Critical	Total service outage; widespread transaction failure; data integrity or security risk; critical integration unavailable with no workaround.	10 min	15 min	Workaround 30 min; service restoration 2 hours	Every 30 min	Draft within 1 business day; final within 2 business days
P2 - High	Major degradation; important service or channel unavailable; significant user impact; workaround limited.	15 min	30 min	Workaround 2 hours; service restoration 4 hours	Every 60 min	Within 3 business days when requested or recurring
P3 - Medium	Limited impact; non-critical function unavailable; workaround available; isolated users or transactions.	1 hour	4 hours	Resolution within 2 business days or agreed plan	Daily	Problem record if recurring
P4 - Low / Request	Information request, cosmetic issue, planned configuration or low-impact service request.	4 business hours	1 business day	Resolution within 5 business days or agreed schedule	As agreed	Not normally required

SLA exclusions apply only where the supplier proves that delay was caused solely by an approved dependency outside its control and that escalation, evidence, follow-up and stakeholder communication were performed on time. Waiting for a third party does not remove ticket ownership or reporting obligations.

5.1 Key Service KPIs

KPI	Minimum Target
Platform/service availability	99.95% monthly for in-scope critical services, excluding approved maintenance.
P1/P2 acknowledgement compliance	At least 98% monthly.
P1/P2 technical engagement compliance	At least 98% monthly.
Incident update compliance	At least 98% of required updates issued on time.
Repeat incident reduction	Month-on-month reduction plan for recurring incidents; zero overdue high-risk permanent actions without approved exception.
Monitoring coverage	100% of agreed critical components, interfaces, jobs and service KPIs.
Shift handover compliance	100% of shifts with documented and acknowledged handover.
Change success rate	At least 98% successful changes without unplanned rollback or service impact.
RCA quality and timeliness	100% of required RCAs delivered on time and accepted after no more than one revision cycle.
Knowledge base currency	All recurring/major issues documented within five business days of closure.
Financial exception control	100% of critical pending, duplicate, failed or unreconciled transaction exceptions ticketed, owned and tracked within the agreed incident target.
Ticket backlog and ownership	Zero unassigned P1/P2 tickets; no overdue ticket without a documented action, owner and next-update date.
Expiry and lifecycle prevention	Zero avoidable service outage caused by expired certificates, licenses, credentials or unsupported components.
Operational readiness compliance	100% of agreed production releases and new services supported by approved monitoring, runbooks, rollback and support-acceptance evidence.

6. IT Service Management Requirements

The supplier shall operate processes aligned with recognized ITSM practices and ATOMA Pay procedures. The supplier shall use ATOMA Pay-approved workflows, forms and authorization controls.

Process	Supplier Requirement
Event and Alarm Management	Validate, correlate, prioritize and act on alarms; remove false positives; ensure critical events create tickets automatically where technically possible.
Incident Management	Restore service quickly, assign ownership, maintain business communication, preserve evidence and formally close only after verification.
Major Incident Management	Open an incident bridge, identify technical and business leads, maintain timeline/action log and issue an incident summary immediately after restoration.
Problem Management	Identify recurring causes, maintain known errors, perform trend analysis and track permanent corrective actions to closure.

Process	Supplier Requirement
Change Management	Use approved MOP, risk/impact, test, rollback, approval, implementation and post-implementation review processes.
Release and Deployment Management	Coordinate release calendars, readiness checks, deployment support, smoke testing, rollback and enhanced post-release monitoring.
Request Fulfilment	Process approved standard requests against documented fulfilment targets and authorization rules.
Access Management	Use named accounts, least privilege, approvals, periodic review, timely revocation and complete audit trails.
Configuration Management	Maintain accurate service inventory, dependencies, versions, certificates, endpoints, owners and configuration baselines.
Knowledge Management	Maintain searchable runbooks, SOPs, FAQs, known errors and troubleshooting procedures owned by ATOMA Pay.
Capacity and Performance Management	Track utilization, growth, transaction load, latency, database and middleware health; forecast constraints and recommend action.
Availability and Continuity Management	Track availability, single points of failure, recovery capability, backup status and resilience improvements.
Financial Operations and Reconciliation Management	Monitor transaction completion, settlement and reconciliation exceptions; preserve financial integrity; coordinate correction and closure using approved maker-checker controls.
Service Validation and Operational Readiness	Confirm support ownership, monitoring, capacity, security, documentation, rollback and escalation readiness before a new or changed service enters production.
Lifecycle and Obsolescence Management	Track certificates, licenses, software support status, service accounts, keys and OEM end-of-support dates; issue timely alerts and remediation plans.
Ticket Quality and Backlog Management	Control assignment, categorization, aging, duplicate records, stale tickets, reopen rates, closure evidence and backlog reduction.

7. Monitoring and Support Tools

The supplier shall use ATOMA Pay-approved monitoring and ticketing tools. Where the supplier proposes its own tool, it must be integrated with ATOMA Pay systems and provided without restricting ATOMA Pay visibility, data ownership or access.

- Real-time dashboards for service availability, transaction success/failure, latency, throughput, error codes, interfaces, resources and critical jobs.
- Threshold-based and anomaly-based alerting with severity mapping, suppression rules and escalation workflows.
- Centralized collection/search of application, integration and system logs where permitted.
- Ticketing integration with automatic incident creation for critical alarms and traceable linkage between alert, ticket, change, problem and RCA.
- Role-based access for ATOMA Pay users to view dashboards, tickets, reports, alerts and SLA status.
- Retention of monitoring and ticket evidence in accordance with ATOMA Pay policy and regulatory requirements.
- Automated daily, weekly and monthly reports, with export capability to common formats.
- No supplier lock-in: all configuration, data, dashboards, rules, scripts and documentation created for the service shall be transferred at contract end.

7.1 Minimum Monitoring Catalogue

Category	Minimum Items
Service health	Application processes, URLs/APIs, service ports, login/transaction probes, critical business flows.
Transactions	Volume, success rate, failure rate, pending/reversed transactions, response time, top error codes and channel/service breakdown.
Interfaces	Connectivity, authentication, certificate validity, request/response latency, queue/backlog, file arrival and acknowledgement.
Application and middleware	Process status, threads, memory, CPU, sessions, queue depth, connection pools, job/scheduler status and error logs.
Database	Availability, sessions, locks, replication, tablespace/storage, slow queries, backup status and growth trends.
Infrastructure dependencies	Server health, disk, memory, CPU, time sync, network reachability and relevant load-balancer status.
Security and access	Failed logins, account lockouts, privileged access events, certificate/credential expiry and suspicious system events.
Financial integrity and reconciliation	Pending, duplicate, orphaned, timed-out, reversed and unreconciled transactions; settlement files; ledger/interface mismatch; exception aging and ownership.
Lifecycle and expiry	Certificates, licenses, keys, credentials, service accounts, software support dates and vendor/OEM support entitlement.
Operational readiness	Monitoring coverage, runbook availability, rollback readiness, support ownership and post-release enhanced monitoring for new or changed services.

8. Staffing and Competency Requirements

The supplier shall provide a stable, named and dedicated team of four (4) resources in the role structure below. Interns, trainees or shared resources shall not be counted toward the committed staffing unless expressly approved in writing by ATOMA Pay.

Role	Minimum Quantity	Location / Coverage	Core Responsibilities
Operations Support Engineer (L1/L2)	3	Shift-based coverage; local/on-site availability	24x7 monitoring, ticket handling, first-line troubleshooting, approved recovery, handover, reporting and activity support.
Application & Integration Engineer (L2)	1	On-site during business hours; 24x7 on-call	Advanced application/API/integration troubleshooting, technical changes, RCA, vendor coordination, permanent fixes, business configuration, testing, documentation and CR preparation.

The committed operational team shall consist of four (4) named resources. The supplier remains responsible for backup, leave and absence coverage without reducing the agreed service coverage or SLA performance. ATOMA Pay reserves the right to interview, approve or reject proposed resources and replacements.

8.1 Minimum Qualifications

- Relevant degree or recognized technical qualification in computer science, information systems, telecommunications or a related discipline.

- Demonstrated experience supporting mobile money, fintech, payment, billing or other high-availability transaction platforms.
- Hands-on capability in Linux, SQL, databases, APIs, web services, middleware, logs, network fundamentals and production troubleshooting.
- Experience with Huawei Mobile Money is strongly preferred for the L2 application/integration role and resources performing business configuration activities.
- Knowledge of ITSM/ITIL processes and major-incident management.
- Ability to prepare clear MOPs, RCAs, reports, diagrams and technical documentation in English.
- Security awareness, confidentiality commitment and successful background/identity verification as required by ATOMA Pay.

8.2 Resource Continuity

- No resource may be removed or reassigned without at least 30 days written notice and ATOMA Pay approval, except in genuine emergencies.
- Replacement resources must have equal or higher competency and complete overlap/knowledge transfer before taking responsibility.
- Vacancies must be filled within 15 calendar days; the supplier must provide temporary qualified coverage immediately.
- The supplier shall maintain a skills matrix, training plan and backup resource for every critical role.

9. Deliverables and Reporting

Deliverable	Frequency / Due Date	Minimum Content
Shift handover report	Every shift	Open incidents, alarms, changes, pending jobs, risks, actions, owners and next update.
Daily health report	Daily by agreed time	Platform health, service availability, transaction KPIs, incidents, failures, backups, capacity alerts and planned activities.
Weekly operations report	Weekly	Incident/problem/change summary, SLA status, recurring errors, risks, action tracker and upcoming activities.
Monthly service report	Within 5 business days after month-end	SLA/KPI performance, availability, incident trends, problem status, change success, capacity, security/access, knowledge and improvement plan.
RCA report	Per SLA	Timeline, impact, detection, technical root cause, contributing factors, recovery, corrective/preventive actions, owners and deadlines.
Capacity and performance report	Monthly	Growth trends, utilization, bottlenecks, thresholds, forecast and recommendations.
Access review report	Monthly or as requested	Active privileged/operational accounts, changes, exceptions, expired access and actions.
Backup and restore report	Daily backup status; restore test at agreed frequency	Backup success, failures, retention, recovery test evidence and gaps.
Knowledge-base update	Continuous; monthly summary	New/updated SOPs, runbooks, known errors, troubleshooting and ownership.
Quarterly service review pack	Quarterly	Executive KPIs, service risks, improvement roadmap, resource performance and strategic recommendations.
Financial exception and reconciliation report	Daily summary; immediate escalation for critical items	Pending/duplicate/failed/reversed/unreconciled exceptions, aging, value/volume, owners, corrective actions and closure evidence.
Certificate, license and lifecycle register	Monthly; 90/60/30-day alerts	Expiry dates, support status, responsible owner, renewal/remediation plan, risks and escalation status.

Deliverable	Frequency / Due Date	Minimum Content
Operational readiness assessment	Before every agreed major release, integration or new service	Support boundary, monitoring, capacity, security, runbooks, rollback, escalation, known risks and acceptance decision.

10. Governance and Escalation

The supplier shall operate a transparent governance model with operational, management, security and change-control forums. Meeting minutes and action trackers shall be issued within one business day.

Forum	Frequency	Participants	Purpose
Operations review	Daily during transition / as needed thereafter	ATOMA operations and supplier team	Review service health, incidents, risks and daily activities.
Weekly service meeting	Weekly	Service owners, designated supplier contact, technical leads	Review SLA, open problems, changes, actions, staffing and upcoming work.
Monthly service review	Monthly	ATOMA management and designated supplier representative	Approve service report, discuss trends, risks, improvements and contractual performance.
Change Advisory Board	As scheduled / emergency as required	Change owners, IT, security, business and supplier	Review risk, implementation, rollback and approvals.
Security working session	Monthly or incident-driven	ATOMA security and supplier representatives	Review access, vulnerabilities, audit actions and security incidents.
Quarterly executive review	Quarterly	Senior management from both parties	Review strategic performance, capacity, roadmap and commercial/service issues.

10.1 Escalation Requirements

- The supplier shall provide a named operational, technical and executive escalation matrix with 24x7 contact details. A designated escalation contact may be selected from the four committed resources.
- P1 incidents shall be escalated to the designated supplier escalation contact and ATOMA Pay management immediately after validation.
- Any risk of SLA breach shall be escalated before the breach, with recovery plan and required decisions clearly stated.
- Unresolved OEM/third-party cases shall be escalated through vendor management channels and reviewed during service meetings.

11. Security, Compliance and Access Control

- Comply with ATOMA Pay information-security policies, access procedures, change controls, data-handling requirements and applicable laws/regulations.
- Use only named user accounts with multi-factor authentication where supported; shared accounts are prohibited except approved technical service accounts.
- Apply least privilege, segregation of duties and formal approval for production, database, operating-system and application access.

- Connect only through ATOMA Pay-approved VPN, bastion, PAM or secure remote-access solutions; direct internet exposure is prohibited.
- Do not copy production data, logs containing sensitive customer information or credentials outside approved ATOMA Pay environments.
- Maintain complete audit trails of access, commands, configuration changes and privileged activities.
- Immediately report suspected security incidents, data exposure, unauthorized access or policy violations through the approved incident channel.
- Support periodic access reviews, internal/external audits, vulnerability remediation and evidence requests.
- Ensure all supplier personnel sign confidentiality obligations and complete required security awareness before access is granted.
- Return or securely destroy ATOMA Pay information and revoke all access upon role change or contract termination.

12. Transition, Knowledge Transfer and Exit

The supplier shall deliver a controlled transition without service interruption. A detailed transition plan shall be submitted with the proposal and finalized within five business days of contract award.

Phase	Indicative Duration	Required Outputs
Initiation and discovery	Week 1	Confirmed scope, stakeholder map, access plan, asset/service inventory and transition risks.
Knowledge acquisition and shadowing	Weeks 1-2	Document review, platform walkthroughs, process training, ticket/history review and monitoring familiarization.
Reverse shadowing and readiness	Weeks 3-4	Supplier-led operation under observation, simulated incidents, shift handover, escalation test and readiness assessment.
Service acceptance	End of Week 4 or agreed date	Approved staffing, access, runbooks, monitoring, reporting, contact matrix and signed transition acceptance.

Transition duration may be adjusted based on platform complexity, but all critical controls must be operational before the supplier assumes sole responsibility.

12.1 Mandatory Transition Deliverables

- Current-state architecture and dependency diagrams.
- Service inventory and ownership/support boundary.
- Monitoring catalogue and alarm-to-ticket mapping.
- Incident, change, access, backup, release and escalation procedures.
- Platform health-check and daily operations runbooks.
- Known issue, risk, open incident/problem and pending change register.
- Shift roster, on-call schedule and contact matrix.
- Knowledge-transfer completion and competency evidence.

12.2 Exit Assistance

At contract expiry or termination, the supplier shall provide orderly exit assistance for at least 30 days, including documentation refresh, data/tool export, access handover, knowledge transfer, open-ticket transfer and cooperation with ATOMA Pay or a replacement supplier. No supplier-owned password, tool restriction or proprietary format may prevent transition.

13. Service Continuity and Disaster Recovery

- Support the approved ATOMA Pay business continuity and disaster-recovery plans for the in-scope platform.
- Maintain current DR contact lists, technical runbooks, dependency checks and recovery verification steps.

- Participate in scheduled DR exercises, switchover/switchback activities and post-test reviews.
- Monitor backup completion, replication, recovery-point risks and critical recovery dependencies.
- Document all findings and track remediation actions to closure.
- Maintain supplier continuity for staff, communications and remote/on-site support during emergencies.

14. Vendor Proposal Response Requirements

The supplier shall submit separate technical and commercial proposals. The technical proposal should follow the structure below and must clearly identify any deviation from these requirements.

1. Executive summary and understanding of the requirement.
2. Detailed service-delivery approach for L1, L2, configuration and integration support.
3. Proposed organization structure, named resources, CVs, location, shift roster and backup coverage.
4. Relevant Huawei Mobile Money, fintech/payment and managed-service references.
5. Transition plan with timeline, activities, dependencies, risks and deliverables.
6. Monitoring/ticketing tool approach and integration capabilities.
7. ITSM processes, major-incident method, RCA method and sample report formats.
8. Security and compliance approach.
9. SLA compliance statement and any proposed improvements.
10. Assumptions, dependencies, exclusions and required ATOMA Pay support.
11. Completed mandatory compliance checklist in Appendix B.
12. Commercial response using Appendix C, with all taxes, travel, on-call, planned activities, licenses and other charges clearly identified.

14.1 Evaluation Considerations

Technical Evaluation Area	
Technical compliance and quality of support model, SLA, monitoring, ITSM and governance approach	
Team competency, Transition plan and service continuity	
Huawei/mobile-money experience	
Local presence	
Commercial competitiveness and transparency	

ATOMA Pay may adjust evaluation weights in the final procurement process and may request presentations, interviews, reference checks, demonstrations or clarification sessions.

15. Acceptance and Performance Management

15.1 Service Acceptance Criteria

- All approved resources are onboarded, trained, available and working according to the accepted roster.
- Access, monitoring, ticketing, reporting and escalation channels are operational and tested.
- The service inventory, support boundary, runbooks, known issues and transition documents are accepted by ATOMA Pay.
- Supplier demonstrates successful handling of test alarms, incidents, escalations, changes and shift handover.
- No critical transition risk remains without an approved mitigation and owner.

15.2 Performance Remedies

The final contract shall include service credits or other remedies for repeated SLA failure, resource shortfall, unauthorized replacement, missed coverage, delayed reporting, security non-compliance or failure to implement agreed corrective actions. Repeated material failure may trigger a formal improvement plan or contract termination rights.

Appendix A - Responsibility Matrix (RACI)

Activity	ATOMA Pay	Supplier L1	Supplier L2 / Config	Huawei/OEM L3 / Third Party
24x7 monitoring and alarm handling	I/A	R	C	I
Incident logging and initial triage	I/A	R	C	I
Advanced diagnosis and workaround	C/A	C	R	C
Major incident coordination	A	R/C	R	C
Root-cause analysis	A/C	C	R	C/R for product defects
Standard configuration change	A	C	R	C
Product/code change	A	I	C	R
Change approval	A/R	I	C	I
Backup monitoring and recovery support	A	R	R	C
Access approval	A/R	I	C	I
Service reporting and SLA	A/C	C	R	I
Knowledge-base maintenance	A	R	R	C
Financial reconciliation exception handling	A/C	R	R	C/R for external-system discrepancies
Operational readiness and support acceptance	A/R	C	R	C
Certificate/license/EOL tracking	A	R	R	C

R = Responsible, A = Accountable, C = Consulted, I = Informed. The final RACI shall be refined during transition for each platform component and dependency.

Appendix B - Mandatory Compliance Checklist

ID	Requirement	Compliance	Comments / Proposal Reference
B1	24x7x365 L1 monitoring and service desk.	Comply / Partial / No	Supplier response / reference
B2	24x7 on-call L2 coverage for P1/P2 incidents.	Comply / Partial / No	Supplier response / reference
B3	Four (4) dedicated resources in the stated role structure.	Comply / Partial / No	Supplier response / reference
B4	Named operational/technical escalation contacts and escalation matrix, with no separate manager role required.	Comply / Partial / No	Supplier response / reference
B5	On-site L2 application/integration capability.	Comply / Partial / No	Supplier response / reference
B6	Huawei Mobile Money or comparable transaction-platform support experience.	Comply / Partial / No	Supplier response / reference

ID	Requirement	Compliance	Comments / Proposal Reference
B7	ATOMA Pay access to monitoring dashboards, tickets and SLA reports.	Comply / Partial / No	Supplier response / reference
B8	ITSM incident, problem, change, release, request, access and knowledge processes.	Comply / Partial / No	Supplier response / reference
B9	Formal P1 RCA and permanent corrective-action tracking.	Comply / Partial / No	Supplier response / reference
B10	No interns or unapproved shared resources counted toward minimum staffing.	Comply / Partial / No	Supplier response / reference
B11	Secure named access, least privilege and full auditability.	Comply / Partial / No	Supplier response / reference
B12	Transition and exit assistance without service interruption or supplier lock-in.	Comply / Partial / No	Supplier response / reference
B13	Separate technical and commercial response with all assumptions disclosed.	Comply / Partial / No	Supplier response / reference
B14	Acceptance of SLA/KPI reporting and contractual service remedies.	Comply / Partial / No	Supplier response / reference
B15	End-to-end synthetic transaction monitoring and business-flow verification for critical services.	Comply / Partial / No	Supplier response / reference
B16	Financial exception, settlement and reconciliation monitoring with auditable maker-checker correction controls.	Comply / Partial / No	Supplier response / reference
B17	Certificate, license, credential and OEM end-of-support lifecycle management with 90/60/30-day alerts.	Comply / Partial / No	Supplier response / reference
B18	Operational-readiness assessment and formal support acceptance before new services or major releases enter production.	Comply / Partial / No	Supplier response / reference
B19	Ticket backlog, aging, ownership, reopen and closure-quality controls with transparent reporting.	Comply / Partial / No	Supplier response / reference
B20	Configuration baseline and drift management across production, DR and non-production environments.	Comply / Partial / No	Supplier response / reference

Appendix C - Commercial Response Template

Suppliers shall provide a transparent, all-inclusive commercial proposal. Any item not explicitly priced shall be considered included in the managed-service fee unless clearly stated otherwise and accepted by ATOMA Pay.

Cost Item	Unit	Quantity	Unit Price	Total Price	Notes / Inclusions
L1 & L2 managed support service	Monthly	12			Include staffing, shift coverage, on-call, reporting and governance.
Transition and knowledge transfer	One-time	1			State whether included in annual fee.
Monitoring/ticketing tools and licenses	Annual	1			Identify all licenses and integration costs.
Planned after-hours activities	Annual allowance				State included hours/activities and overtime conditions.
Change request / project day rate	Person-day				Only for agreed out-of-scope work.
Travel and local expenses	Annual				State whether included.
Taxes and statutory charges	As applicable				Show tax basis separately.
Total annual contract value	Annual	1			Provide currency and payment schedule.

Appendix D - Supplier Assumptions and Deviations

Reference	Assumption / Deviation	Impact on Scope, SLA or Price	Proposed Resolution

The final scope, resource plan, SLA, RACI, pricing and contract terms will be agreed through the procurement and contract-negotiation process. The supplier shall not rely on verbal assumptions or undocumented exclusions.

PROPOSAL REQUIRED DOCUMENTS

The following documents are required to be submitted along with Sealed Proposal to be submitted in Tender Box Located in reception of ATOMA-Head Office.

- **Technical Proposal** Detailed technical approach and demonstrating compliance with the RFP requirements.
- **Commercial Proposal** Detailed financial proposal and breakdown, covering all applicable costs, rates, fees, and other commercial terms related to the required services.
- **Company Profile** (Company Background, Staff Availability, Office location, Tangible Assets)
- **Valid License from Government** of Afghanistan (Relevant License duration should be not less than three years)
- **At least 3 references** of reputable and well-known organizations along with their names and contact numbers where the company has provided or providing the same services to.
- **Experience in relevant** field minimum 3 years and (Relevant Experience, Client References, Projects Values and Turners)
- **Financial Stability** (Bank Statement for last Six Months, (All bank accounts should be in the name of the company stamped by Authorized Bank.)
- **Team Composition** Details of the proposed team, including key personnel, qualifications, roles, responsibilities, and relevant experience.

Evaluation Criteria:

- Technical capabilities and experience
- Price and commercial terms
- Financial stability and references
- Compliance with Documentation Requirements (Pass/Fail)

The Evaluation Committee shall assign the percentage weight for each evaluation criterion prior to the opening and evaluation of proposals. The weighting shall reflect the importance of each criterion in achieving the objectives of this procurement and shall remain unchanged throughout the evaluation process.

Only proposals that satisfy the mandatory compliance requirements shall be considered for detailed technical and commercial evaluation.

Submission Instructions:

- All proposals must be submitted electronically to:
Temp_ismail.safi1@atoma.com.af, sadeequllah@atoma.com.af
- All commercial proposal which are submitted electronically must be **password protected**. Unprotected proposal will not be considered for further evaluation.
- The sealed envelope should be submitted at:
ATOMA Head Office, Reception Shar-E Naw Kabul, Afghanistan.
- The sealed envelope must be placed in ATOMA tender box, located in ATOMA main office reception.
- All questions regarding this RFP must be submitted in writing.
- Responses will be provided to all potential bidders.
- Bids must remain valid for 120 days from the submission deadline.
- The bid must be submitted in English.
- ATOMA reserves the right to reject any or all proposals.

General Requirements and Compliance

- The supplier must have and always maintain and all the time, at its own cost and expense, all permits, licenses, authorization, and approval from relevant government entities necessary for the service provided under this RFP/Agreement.

All foreign companies are therefore required to ensure that all corporate documents are:

- Officially translated into English, if not already in English
- Notarized or certified by an appropriate authority in the country of origin (e.g., notary public, apostil, Ministry of foreign Affairs, or embassy) such as Business Licenses, Incorporation Certificates, Tax Certificates, Bank Reference Letters, ISO Certifications properly stamped, signed, and dated
Failure to submit properly certified and verifiable documentation may result in disqualification or reduced eligibility.
- The top three suppliers shall present slide presentations to the cross-functional team comprised of technical IT and Network, legal and compliance, procurement and ATOMA Pay Business team).

Queries and Submissions:

All queries related to this document should be addressed to:

Procurement department of ATOMA

Email: Temp_ismail.safi1@atoma.com.af, sadeequllah@atoma.com.af. Phone# 0772227050, 0772222021