

INVITATION TO QUOTE

Dear Sir/Madam,

1. You are invited to present your technical offer & price quotation(s) for new solution that include following modules :

- IT Service Management (ITSM) that supports Enterprise Service Management through customized workflows for multiple business departments,
- Change Management module
- IT Asset Management (ITAM) and
- Software License Management capabilities.

The platform must support deployment as SaaS (cloud) or on-premises; however, EU/EEA data residency is mandatory for all data, including backups and disaster recovery. as described below on point 5 (Details & Technical Specifications) and Annex B.

2. You can provide to us your offer (Technical Offer and estimations cost for the mentioned services and other requested documentation) which will be subject of a separate review procedure and signature of the respective contract by parties included, for the best offer.
{Based on the "Invitation to Quote" you should present your offer, after you have read carefully each articles specified, as parts of your assessment}.

3. **ADDRESS FOR QUOTATION**

Your quotation(s) should be addressed in a closed envelope, superscribed "Quotation for Bid" and submitted to:

Procurement Unit

**Tirana Bank, Head Office, "Bulevardi "Zhan D'Ark, Njesia Administrative nr. 2, MET Tirana Building
Tirane, Albania**

4. **THE DEADLINE**

The deadline for receipt your quotation (s) by the Purchaser at the address indicated above is:

27.04.2026

5. **DETAILS & TECHNICAL SPECIFICATIONS**

A) Key Objectives

- Consolidate service delivery processes on a single platform.
- Deliver department-specific service catalogs, forms, approvals, SLAs, and routing.
- Improve service quality via automation, knowledge, and standardized governance.
- Strengthen governance and compliance via audit trails, security controls, and reporting.
- Gain full visibility into assets and software usage with ITAM & License Management.
- Integrate with SAP and Microsoft 365 (M365) as mandatory systems.
- Meet mandatory EU/EEA data residency and applicable security/compliance expectations.

B) Project Scope

B.1 Phase 1 Departments (Mandatory)



- IT Department — Incident, Service Request, Problem, Change, Knowledge, Service Catalog.
- ISO — Security service request workflows, risk & exception requests, access governance requests; audit ready logging and approvals.
- Organization — Internal service requests and operational workflows with department specific approvals/SLAs.
- MIS — Data/reporting requests, system configuration requests, cross functional workflows.

B.2 Phase 2+ Expansion (Mandatory Capability)

The platform must support progressive onboarding of additional departments (e.g., HR, Finance, Procurement, Facilities, Legal, Commercial) through configuration/low code rather than heavy custom development.

B.3 Users, Agents & Scale

- Agents (fulfillers): ~100.
- End users (requesters): ~650.
- Vendors must describe scalability to support growth (e.g., up to 150 agents and 1,500+ users) without major redesign.

C) Deployment Model & Data Residency

C.1 Deployment Options

Vendors may propose SaaS (Cloud), On Premises, and/or Private Cloud. Vendors must clearly outline architecture, sizing assumptions (on prem), environment strategy (dev/test/prod), upgrade/patching model, HA/backup/restore/DR, and support responsibilities.

C.2 EU/EEA Data Residency — Mandatory, Non-Negotiable

- All data must reside within the EU/EEA, including production data, audit logs/telemetry related to the platform, backups, replicas, and DR/failover.
- No data may be transferred, mirrored, cached, or processed outside the EU/EEA at any time, including by subcontractors or sub processors.
- Vendors must provide: primary and DR data center locations (country + region), backup locations, sub processor list and locations, contractual assurance, and a data flow diagram proving no out of region processing/storage.

The Service providers might provide a platform for all the required requests, or a solution for each of the requests. The Bank reserves the right to choose the best solution or platform offered by the providers. Might be one or several providers for each solution.

D) Functional requirements

1. Functional Requirements

1.1 Core ITSM Capabilities (Mandatory)

1.2 Departmental Workflow Customization (Enterprise Service Management) — Mandatory
Demo-ready example workflows

2. Change Management Capabilities (Mandatory)

3. IT Asset Management (ITAM) — Mandatory

3.1 Asset Lifecycle Management

4. Software License Management — Mandatory

5. Mandatory Integrations

5.1 Microsoft 365 (Mandatory)

5.2 SAP (Optional)

6. Security, Privacy & Compliance Requirements

6.1 Core Security Requirements

6.2 Compliance Expectations



6.3 Data Protection Requirements
7. Reporting, Analytics & Dashboards
8. User Experience Requirements

E) Security requirements:

Please fill the below questionnaire attached email:

- Information Security Technical Requirements 2025_New Website
- Third-Party Security Risk Assessment QuestionnaireTirana Bankform

F) Service Level Agreement (SLA) & Incident handling

Please provide:

- An example Service Level Agreement (SLA).
- Which service levels are available?
- Process of incident handling

G) Implementation

Providers are required to quote for the following:

- Implementation Plan
- Detailed deliverables
- Custom Development

+ All above points from A to G are detailed as per Annex B

6. PRICE

Your financial offer should provide:

The financial offer for 2 years followed by an automatic renewal for an additional one (1) year, unless either party provides written notice of termination no later than thirty (30) days prior to the expiration of the contract for:

1. Licensing

- License model (named agent, concurrent agent, requester, asset-based, etc.).
- Costs for 100 agents and 650 users, plus growth tiers.
- Module pricing: ITSM, ITAM, License Management (and CMDB/discovery if separate).
- Non-production environments.
- API limits and any extra charges.

2. Implementation Services

- Itemized services estimate: workshops, configuration, SAP/M365 integration, migration, testing, training, go-live.
- Optional services: additional department onboarding, advanced reporting.

3. Ongoing Costs

- Annual subscription/support and maintenance.
- Hosting costs (if SaaS).
- DR/HA costs (if applicable).
- Professional services retainers (if proposed).

+ Detailed Price requirements are given in Annex A

7. SERVICE DURATION:

- 2-years followed by an automatic renewal for an additional one (1) year, unless either party

provides written notice of termination no later than thirty (30) days prior to the expiration of the contract.

8. DOCUMENTATIONS

The following documentations should be parts of your offer:

- Financial offer (including all requirement in Annex A and Annex B).
- Technical offer, including all requirement mentioned in point 5 above and Annex B
- Extract printed from e-albania (valid for Albanian registered companies) of the Commercial Register from the within the last month
- Copy of the certificate of Registrations as a taxable person.
- "Third-Party Security Risk Assessment Questionnaire_Tirana Bank_form" questionnaire (to be completed by all tender's participants)
- "Information Security Technical Requirements 2025_New Website" questionnaire (to be completed by all tender's participants)
- Signed "Vigilance Form" attached (to be completed only from Albanian companies)
- CV of the Company, a general presentation of your company. Company profile and financial stability overview.
- Relevant experience implementing ITSM/ESM with ITAM and license management.
- Experience integrating with SAP and Microsoft 365.
- At least 3 references of comparable size/complexity (preferably with EU/EEA residency requirements), List of Clients for respective similar services or equal to the one requested above

9. CONTACT

For further information you should contact at:

e-mail: procurement@tiranabank.al

- 10. In your attention:** Payments to the winning company/ies for the procurement process will be done through Tirana Bank account and in the case that there is no chance to open an account at Tirana Bank, the transfer commissions will be charged to the company.
- 11.** Please confirm in the above-mentioned email contact, that you receive this invitation of quote as well as your consent for participants in this procurement procedure.

Sincerely
TIRANA BANK



ANNEX A- FINANCIAL OFFER

The financial offer should be provided for the following periods: 2-years +1-year automatic renewal unless either party provides written notice of termination at least 30 days before the contract's expiration date. In addition, bidders shall specify financial offer, as detailed in the table below

Modules	NO	Description	Define Unit / frequency	Unit price	Value	-Payment terms: Days after invoice issued -Invoicing: upfront or not annually or monthly or other
<ul style="list-style-type: none"> • ITSM • ITAM • Change management module • Software license management 	1	Licensing				
	1.1	License model (named agent, concurrent agent, requester, asset-based, etc.).				
	1.2	Costs for 100 agents and 650 users, plus growth tiers.				
	1.3	Module pricing: ITSM, ITAM, License Management (and CMDB/discovery if separate).				
	1.4	Non-production environments.				
	1.5	API limits and any extra charges.				
	2	Implementation Services				
	2.1	Itemized services estimate workshops, configuration, SAP/M365 integration, migration, testing, training, go-live.				
	2.2	Optional services: additional department onboarding, advanced reporting.				
	3	Ongoing Costs				
	3.1	Annual subscription/support and maintenance.				
	3.2	Hosting costs (if SaaS).				
	3.3	DR/HA costs (if applicable).				
	3.4	Professional services retainers (if proposed).				
	Total Value including VAT					

Prices should include all taxes and expenses: VAT.

A. Important note: Bidders may offer either a comprehensive platform covering all required modules: ITSM, ITAM, Change management module, Software license management or individual solutions addressing specific modules. The Bank reserves the right to select the most suitable option, whether from a single provider or multiple providers

B. Terms of payments: Tirana Bank standard payment terms 30 days after delivery of service and invoice issuance. Invoice to be issued after service is delivered and accepted.

C. Note for foreign companies for Withholding tax:

c1 Please define country that will issue the invoice

c2 In case exist the Double taxation Agreement between Albania and your Company's country for avoidance of double taxation, your Company will fulfill and duly sign Tax residence certificate for the year (i.e.2026) and the Claims for double taxation avoidance for the invoices paid. Please note that If you do not agree for application of double taxation treatment, withholding tax will be applied at the standard rate of 15% on every payment (will be deducted from the amount stated in the invoice).

D. Price changing

d1 Prices should be unchanged during contract duration. Please your comment if it is different

d2 CPI rules. Please define CPI after contract duration



ANNEX B REQUIREMENTS

1. Executive Summary / Purpose

Tirana Bank invites qualified vendors to propose a solution that includes the following modules:

- IT Service Management (ITSM) that supports Enterprise Service Management through customized workflows for multiple business departments,
- Change Management module
- IT Asset Management (ITAM) and
- Software License Management capabilities.

The platform must support deployment as SaaS (cloud) or on premises; however, EU/EEA data residency is mandatory for all data, including backups and disaster recovery.

2. Key Objectives

- Consolidate service delivery processes on a single platform.
- Deliver department specific service catalogs, forms, approvals, SLAs, and routing.
- Improve service quality via automation, knowledge, and standardized governance.
- Strengthen governance and compliance via audit trails, security controls, and reporting.
- Gain full visibility into assets and software usage with ITAM & License Management.
- Integrate with SAP and Microsoft 365 (M365) as mandatory systems.
- Meet mandatory EU/EEA data residency and applicable security/compliance expectations.

3. Project Scope

3.1 Phase 1 Departments (Mandatory)

- IT Department — Incident, Service Request, Problem, Change, Knowledge, Service Catalog.
- ISO — Security service request workflows, risk & exception requests, access governance requests; audit ready logging and approvals.
- Organization — Internal service requests and operational workflows with department specific approvals/SLAs.
- MIS — Data/reporting requests, system configuration requests, cross functional workflows.

3.2 Phase 2+ Expansion (Mandatory Capability)

The platform must support progressive onboarding of additional departments (e.g., HR, Finance, Procurement, Facilities, Legal, Commercial) through configuration/low code rather than heavy custom development.

3.3 Users, Agents & Scale

- Agents (fulfillers): ~100.
- End users (requesters): ~650.
- Vendors must describe scalability to support growth (e.g., up to 150 agents and 1,500+ users) without major redesign.

4. Deployment Model & Data Residency

4.1 Deployment Options

Vendors may propose SaaS (Cloud), On Premises, and/or Private Cloud. Vendors must clearly outline architecture, sizing assumptions (on prem), environment strategy (dev/test/prod), upgrade/patching model, HA/backup/restore/DR, and support responsibilities.

4.2 EU/EEA Data Residency — Mandatory, Non-Negotiable

- All data must reside within the EU/EEA, including production data, audit logs/telemetry related to the platform, backups, replicas, and DR/failover.
- No data may be transferred, mirrored, cached, or processed outside the EU/EEA at any time, including by subcontractors or sub processors.



- Vendors must provide: primary and DR data center locations (country + region), backup locations, sub processor list and locations, contractual assurance, and a data flow diagram proving no out of region processing/storage.

The Service providers might provide a platform for all the required requests, or a solution for each of the requests. The Bank reserves the right to choose the best solution or platform offered by the providers. Might be one or several providers for each solution.

FUNCTIONAL REQUIREMENTS

1. Functional Requirements

1.1 Core ITSM Capabilities (Mandatory)

- Incident Management — multi-channel intake (portal/email/API), categorization/priority, SLA, escalation, major incident handling, assignment rules, linking to problems/changes/knowledge/assets.
- Service Request & Catalog — multi-department catalogs, dynamic forms, multi-step approvals, fulfillment tasks/orchestration.
- Problem Management — RCA, known errors, workarounds, trend analysis.
- Knowledge Management — lifecycle (draft/review/publish/archive), permissions, feedback, search, optional knowledge suggestion.
- SLAs/OLAs — per department/service/category/priority; pause rules; breach alerts; reporting.

1.2 Departmental Workflow Customization (Enterprise Service Management) — Mandatory

- Separate departmental workspaces/queues/catalog views as needed.
- Configurable workflows per department (routing, approvals, tasks).
- Department-specific SLAs, notifications, templates, dashboards.
- Role-based access control and data segregation.
- Reusable workflow components/shared services.
- Ability to add new departmental services without coding (low-code acceptable).

Demo-ready example workflows

- ISO: security exception request with risk approval chain and audit trail.
- Organization: departmental request with approvals and SLA.
- MIS: reporting/data request flow with intake form, approval, delivery tasks.

2. Change Management Capabilities (Mandatory)

- Ability to create, submit, and track change requests.
- Customizable forms and fields for different types of changes (standard, normal, emergency).
- Automated workflows for review, approval, and implementation.
- SLA tracking for each stage of the change process.
- CAB, Role-based approval matrices
- Built-in templates for risk scoring / impact analysis.
- Tools to assess technical, operational, financial, and risk impacts.
- Ability to link changes to incidents or problems, projects etc
- Post-implementation review templates.
- Automated reminders for pending reviews.
- Lessons-learned documentation functionality
- Integration with organizational calendars (Microsoft Outlook, Teams, etc.).
- Ability to categorize blackout periods, maintenance windows, and high-risk intervals.

3. IT Asset Management (ITAM) — Mandatory



3.1 Asset Lifecycle Management

- Asset types: endpoints, servers, network devices, peripherals; optional non-IT assets.
- Lifecycle: procurement → receiving → stock → deployment → assignment → maintenance → retirement/disposal.
- Ownership/assignment to user/location/cost center/department; warranty/maintenance/contracts; full audit trail.

4. Software License Management — Mandatory

- License entitlements and contract tracking (purchase, renewal dates, terms).
- Installed software evidence collection (from inventory/discovery sources).
- Compliance reporting (installed/used vs entitled).
- Alerts for non-compliance and renewals.
- Optimization/reclamation workflows and audit readiness.
- Support for key license models (named user, device, subscription, etc.).
- Vendors must detail limitations and compliance calculation methods.

5. Mandatory Integrations

5.1 Microsoft 365 (Mandatory)

- Azure AD / Microsoft Entra ID — SSO via SAML 2.0 or OIDC, group/role mapping for RBAC, MFA compatibility.
- Exchange Online — email ticket creation/updates; modern auth (OAuth 2.0).
- Microsoft Teams — notifications and (preferably) ticket actions/approvals.

5.2 SAP (Optional)

- Integrate with SAP S/4HANA via REST/SOAP/OData or files.
- Use cases: Asset Management lifecycle integration.
- Provide supported SAP versions, integration patterns, mapping, sync frequency, and error handling.

6. Security, Privacy & Compliance Requirements

6.1 Core Security Requirements

- Encryption in transit (TLS 1.2+) and at rest (AES-256 or equivalent).
- RBAC, least privilege, segregation of duties.
- Audit logging for admin and user actions; exportable logs.
- Secure API access (OAuth tokens/keys), rate limiting and monitoring.
- Vulnerability management and patching model (SaaS vendor-managed; on-prem vendor guidance).
- Configurable retention policies for tickets, logs, knowledge, and attachments

6.2 Compliance Expectations

Vendor must describe alignment with GDPR and provide security management certifications/attestations (e.g., ISO 27001 and/or SOC 2 Type II where applicable), including scope.

6.3 Data Protection Requirements

- EU/EEA residency assurance (Section 4.2).
- Ability to export data in standard formats.
- Retention/archival and secure deletion processes.
- Customer ownership of data and export at termination.

7. Reporting, Analytics & Dashboards

- Real-time operational dashboards for IT and each onboarded department.
- SLA compliance dashboards (by department/service/priority).
- Backlog aging, volume trends, resolution times, FCR (if applicable).
- Custom report builder and scheduled reports.



- Export: CSV/Excel/PDF (as available).
- API access to reporting data (or DWH integration options).

8. User Experience Requirements

- End User Portal
- Simple request submission and tracking.
- Department-specific catalogs and knowledge visibility.
- Mobile-friendly UI.
- Agent Experience
- Unified agent workspace and queue management.
- Configurable views, templates, macros, automation/assignment rules.
- Linking between tickets, assets, changes, knowledge.
- Documentation and knowledge transfer.

9. Vendor Qualifications

- Company profile and financial stability overview.
- Relevant experience implementing ITSM/ESM with ITAM and license management.
- Experience integrating with SAP and Microsoft 365.
- At least 3 references of comparable size/complexity (preferably with EU/EEA residency requirements)

B. SECURITY REQUIREMENTS:

Please fill the “**Information Security Technical Requirements**” questionnaire and “**Third-Party Security Risk Assessment Questionnaire Tirana Bankform**”

C. SERVICE LEVEL AGREEMENT (SLA) & Incident handling

- Please provide Service Level Agreement (SLA).
- Which service levels are available? Describe those in detail, especially regarding the availability of company customer support (Mo - So, bank holidays, weekends, etc.) and how customer support can be reached (email, mobile, etc.).
- Please describe the process of incident handling, dedicated portal for reporting, time frames of resolution, etc.

D. SERVICE DURATION:

- 2-year maintenance followed by an automatic renewal for an additional one (1) year, unless the Bank provides written notice of termination no later than thirty (30) days prior to the expiration of the contract."

E. YOUR OFFER SHOULD CONTAIN:

- **Financial offer**
 - Financial offer should be provided for the following modules:
 - ITSM
 - ITAM



- Change management module
- Software license management

And should cover the following:

- Licensing
- Implementation Services
- Ongoing Costs

- **Technical offer:**

- Presentation of system functionalities
- Presentation of system technical architecture
- Presentation of security features
- Implementation plan

- **Service Level Agreement (SLA)**

- **Delivery terms**

- **Warranty**

- **Payment terms related to service delivery.**

- **List of Clients for respective similar services or equal to the one requested above**