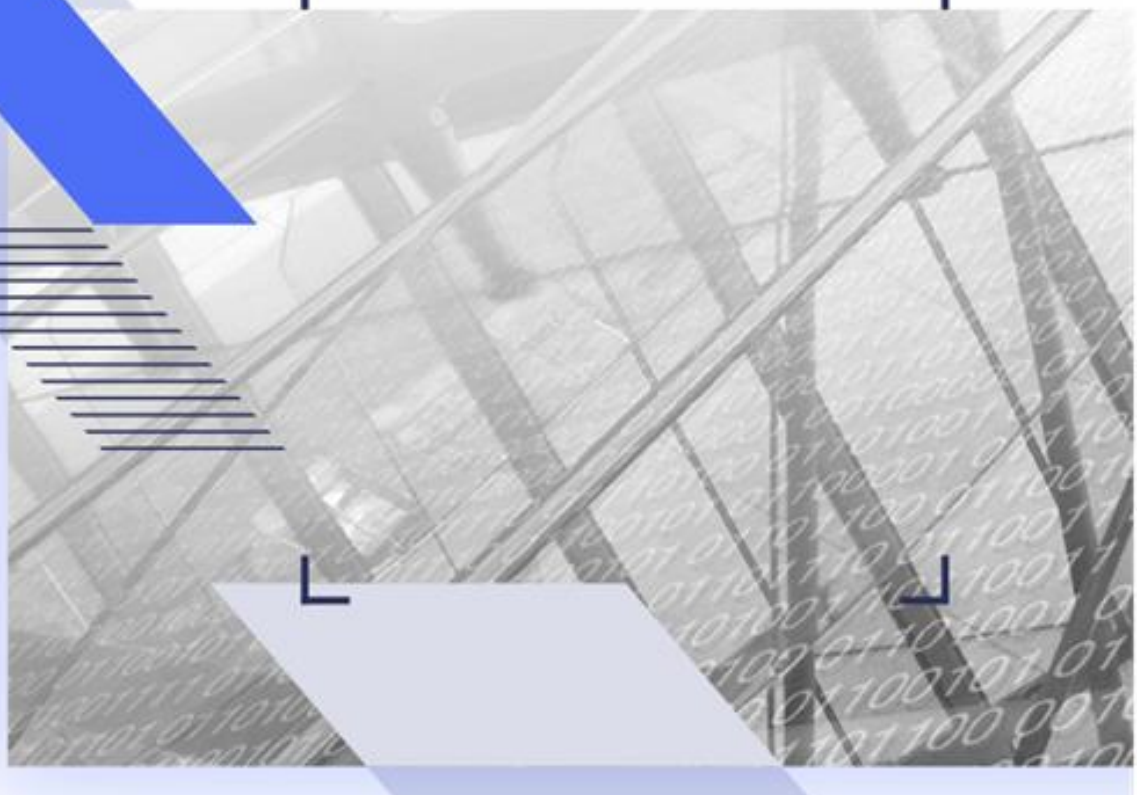


Forbis services

COMMERCIAL IN CONFIDENCE

Table of Content

1. Introduction

Forbis fully complies with the National Bank of Moldova's requirements by delivering a Core Banking System and implementation approach that aligns with all defined functional, technical, and methodological criteria.

The proposed solution covers all required banking operations, while our implementation framework ensures strict adherence to quality, efficiency, and structured delivery, including comprehensive training, documentation, and knowledge transfer.

Forbis is a leading developer of banking software in the Baltics. Established since 1990, the Forbis group has always offered cutting-edge technology and innovative financial products and solutions to its clients, which range from state enterprises to large banks and small payment service providers. Business: Financial software development and IT services for financial institutions. Banking software as a service (SaaS), IT infrastructure support and maintenance.

1.1 Competence

Our team consists of highly skilled individuals with a wide range of skills and experience.

- 100+ staff.
- Multi-language and diverse team. English is the main language of the project.
- Competitive benefit package attracts and retains highly qualified and motivated specialists.
- Aim at long-lasting work relationships – 60% of the personnel have been working for the company for more than 5 years.

Team members are specialists in the IT and banking areas, including:

- Developers and architects
- Hardware and database administrators
- Payment business analysts.
- Project managers with experience in system implementation
- Business and legal consultants in the area of financial regulation and the payment market

1.2 Certification

Forbis delivers a wide range of software development, implementation, and support services for the banking and finance sectors. Information security requirements are also set out in accordance with international legal acts related to information security, including:

- General Data Protection Regulation (EU) 2016/679 (EU GDPR).
- EBA guidelines regarding outsourcing delivery to cloud providers EBA/REC/2017/03

Forbis information security management is based on the operational and security risk management pursuant to the requirements of international standard LST EN ISO/IEC 27001:2017 (ISO/IEC 27001:2013). Our company ensures the provision of the services and their continuous improvement in compliance with:

- ISO 27001 Information Security Certificate
- ISO 20000 IT Service Management Certificate
- ISO 9001 Quality Management Certificate

Quality assurance goals of Forbis are as follows:

- To strive to understand the customer expectations as best as possible and to precisely follow their requirements when implementing new technologies.
- To continuously monitor and assess the quality planning and implementing process, to increase its efficiency and outcome to avoid failures as well as to effectively remedy consequences of such failures, if any.
- To select those service providers who follow both quality and security requirements in the best possible manner.
- Train competent employees to help the company attain the goals of the quality management system.
- To analyse the worldwide technological progress in the area of company activity and to implement up-to-date solutions in the products developed by Forbis.

2. Proposed licensing model

Main notions

- Licensee – contracting authority, National Bank of Moldova, hereafter referred to as Bank or NBM or Licensee.
- Licensor – Forbis UAB.
- Forbis Banking Information System (hereafter referred to as FBS or BIS) – a set of applications and information means and methods, designed for management of information flows, record keeping, preparation of accounting and analysis of activity of the bank.
- BIS product (hereafter referred to as the Product) – a product, subsystem or a software module making a compositional part of Forbis BIS.
- Forbis BIS license – non-exclusive right of the National Bank of Moldova (NBM) to compensated use of Forbis BIS with all its functions on server equipment.
- Forbis BIS product license – non-exclusive right of the NBM to compensated use of the Product.

- Environment – integrity of hardware, general software and the executed components of BIS.
- Licenses Acceptance Note – a document signed by the Parties, confirming transference of BIS license and BIS product licenses, if applicable.

The proposed licensing model consists of:

- Solution licenses: a perpetual, non-exclusive license covering the full functionality of the Forbis BIS platform, including all required modules to meet functional requirements.
- Complementary licenses: third-party components (e.g., DBMS) sublicensed to the Bank under standard vendor terms, fully included where required for system operation.

Justification of optimality

This model is optimal for the NBM because it:

- Ensures a “turn-key” solution, with all necessary licenses included and no need for additional purchases to meet functional requirements
- Provides cost predictability through perpetual licensing (no recurring base license fees)
- Enables controlled scalability, allowing incremental expansion via additional product licenses
- Guarantees operational continuity, with all dependencies covered through sublicensed complementary components.

A comparative table with Forbis other options

Compared to typical licensing models used in similar tenders, such as subscription-based approach, the proposed model offers lower long-term costs, reduced vendor dependency, and greater transparency, making it particularly suitable for a central bank environment that requires stability, control, and long-term planning.

Model Type	Forbis Proposed Model for NBM	SaaS Alternative
License Type	Perpetual	Subscription
User Licensing	Named, reusable	Concurrent
Cost Structure	One-time with optional add-ons	Hybrid, Recurring (annual) with optional add-ons
Scalability	Incremental (product-based)	Incremental (product-based)
3rd Party Licenses	Included/sublicensed	Included/sublicensed

Model Type	Forbis Proposed Model for NBM	SaaS Alternative
Vendor Dependency	Low	High

3. Training

Forbis provides a comprehensive, structured, and results-oriented training methodology, aligned with the project's objectives and implementation phases. Our approach ensures that our customers' personnel acquire both functional proficiency and technical understanding of the Core banking solutions, enabling sustainable internal use and long-term independence.

In line with the requirements, Forbis applies internationally recognized methodologies and best practices, ensuring high levels of quality, professionalism, and effectiveness, while embedding knowledge transfer into every stage of the project.

Training of the Customer specialists is carried out as a coordinated program both during implementation of the Forbis CBS in the Customer as well as during further stages and may be conducted both in the office of the Forbis, as well as on the territory of the Customer in the form of audit studies and practical work. The key moments of the training process are:

- Development of the training program, agreeing upon the training schedule together with the Customer.
- Conducting training in the form of theoretical studies and practical work.
- Conducting testing with the purpose of controlling the gained knowledge.
- If repeated training or testing is required.
- Submission of the reports containing the results of the test performed to the management.
- Issuing of the certificates of the Forbis to the specialists of the Customer, who have completed the training and passed the testing.

Additional training courses may be conducted both at the initiative of the Customer, as well as in the framework of the planned raising the level of the Customer's specialist qualification. The cost of the additional training depends on the program of the courses and is determined on the basis of the daily rate of the specialists of the Forbis.

3.1 Training Methodology

Forbis will deliver the training phase as a multi-stage process integrated into the overall implementation lifecycle, covering preparation, delivery, evaluation, and post-go-live support.

Forbis will conduct a structured Training Needs Analysis (TNA) to identify user groups (business users, IT administrators, key users); assess current competencies and knowledge gaps and map training requirements to system modules, business processes, and project phases.

This ensures that the training program is tailored to the specific operational context and roles within NBM.

Based on the analysis, Forbis will provide role-based training programs, including:

- Clearly defined learning objectives per audience.
- Modular training structure aligned with CBS functionalities.
- Development of relevant training materials and system-based scenarios consistent with project documentation.

Training materials include both theoretical and practical elements, ensuring a balance between conceptual understanding and hands-on experience.

Forbis will deliver training sessions according to a structured plan integrated with the project timeline, ensuring readiness before Go-Live.

Training will be conducted using a hybrid delivery model, combining:

- Instructor-led classroom sessions (on site/remote/hybrid),
- Interactive workshops dedicated to specific subjects (on site/remote/hybrid).
- Practical system exercises in a controlled training environment (on site).

Remote/virtual training sessions will be applied to where appropriate, in accordance with project delivery.

Important part of successful training is evaluation and continuous improvement. Forbis implements evaluation mechanisms, including participant assessments (tests, practical exercises), feedback collection after each session, continuous refinement of training content and delivery.

Following system deployment, Forbis will provide refresher and advanced training sessions, as well as on-the-job support during early operational phases.

3.2 Training planning

Forbis will develop and submit a detailed training plan, tailored for the project. Our standard training plans include:

- Training objectives and scope
- Definition of target groups and roles
- Detailed training program per module and function
- Training schedule aligned with implementation phases
- Duration of each session (number of hours/days per course)
- Delivery format (on-site, remote, hybrid)
- Required infrastructure and resources
- Trainers' roles and responsibilities

Forbis adopts a role-based and scenario-driven training approach, ensuring that each participant receives training relevant to their responsibilities.

Example of training invitation

3.3 Training delivery

Forbis offers instructor-led training for structured knowledge transfer. As a rule, instructors are experts in their dedicated field and offer hands-on approach using real-life business scenario.

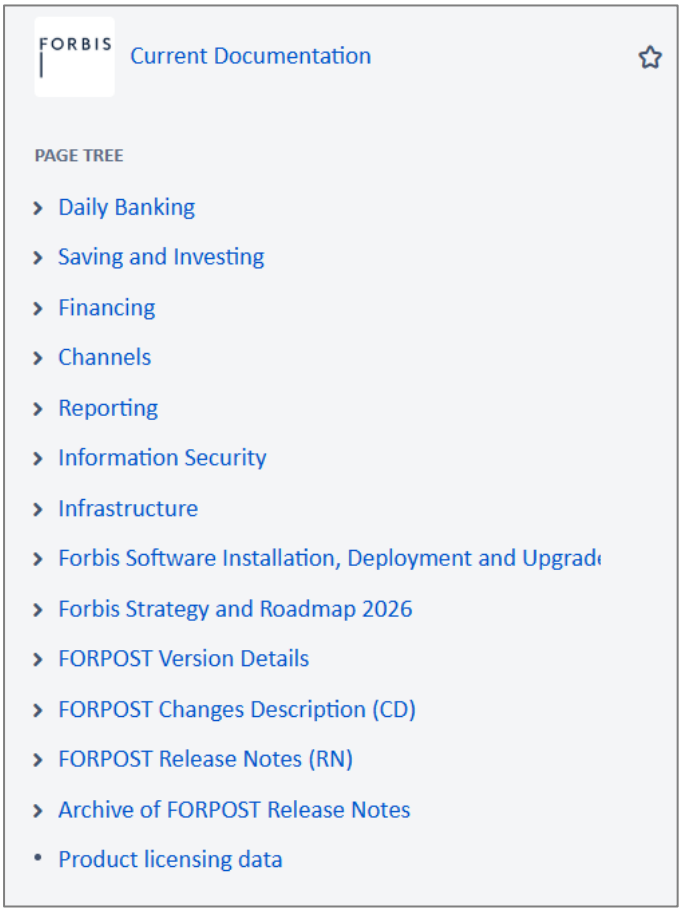
Training is conducted in a dedicated test/training environment. Virtual training sessions are used for flexibility and wider accessibility. Self-learning materials and recorded sessions for continuous learning are available at documentation portal and SharePoint.

Training methods:

- Train-the-Trainer Model
- Structured documentation (user manuals, technical and administration guides, operational procedures, troubleshooting guides etc)
- On-the-Job Training during testing and Go-Live phases:
- Workshops and deep-dive sessions
- Ongoing advisory during warranty and support period

In accordance with the requirements, Forbis will provide a comprehensive set of training deliverables,:

- Master Training Plan
- Detailed training schedules
- Role-based training programs
- Session agendas and timelines
- Training materials
- Participant lists and records, completion status and evaluation results, certification
- Training completion reports, evaluation and feedback summaries



3.4 Documentation

Forbis treats documentation as a critical operational asset, with a centralized knowledge base, i.e. the Forbis wiki.

All system descriptions, configurations, and procedures follow consistent structure, naming, and ownership to ensure clarity and accountability.

Documentation is continuously maintained, to keep content accurate and relevant. Forbis provides 24/7 access to Confluence/Wiki documentation portal with user manuals, administrator manuals, operation documentation, system functionality description, release notes etc. Documentation is provided in English.

4. Post-implementation support and warranty period

Forbis will provide post-implementation maintenance and comprehensive support to NBM in resolving all solution-related incidents throughout the warranty and support period, regardless of the underlying cause.

As mentioned above, Forbis is ISO 20000, ISO 27001, ISO 9001 certified, therefore services will be covered by these standards and ITIL v.4.0 framework.

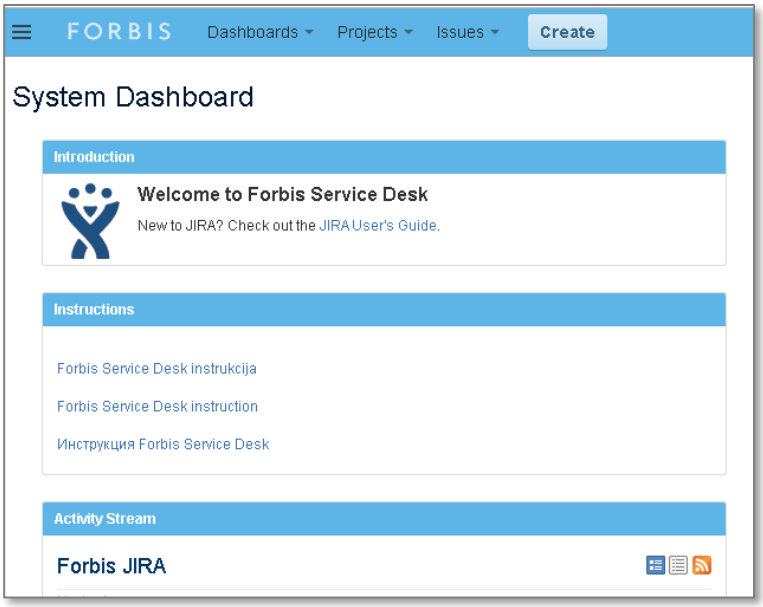
4.1 Requirements for support services CP.14.

In general, support includes the following services:

- Supply with new releases and patches of the system in accordance with the regulations of support and maintenance.
- Upgrade of the testing environment at installing of new releases and patches.
- Consulting of employees regarding the issues related to everyday operations, changes and amendments of CBS.
- Informing employees about new developments in the sphere of financial information technologies.
- Documentation update.
- Access to the Service Desk (Wiki knowledge database and documentation, Jira task system, and document exchange system).

In more detail, the support service will be provided according to ITIL structure. The processes performed within the service are the following:

- Incident Management
- Problem Management
- Configuration Management
- Change request Management



Service Desk system

The Service Desk system based on Atlassian JIRA is the general entry point for operational communication of all the services provided by the Tenderer.

The Service Desk system ensures that the NBM requests are processed in a timely manner by the appropriate people, and according to the agreement with the Customer. The Service Desk system also ensures that the information of the Service Requests is up-to-date and presented in a consistent manner.

The Service Desk system supports three main methods of managing and communicating the requests:

- The Service Desk system is used to manage the Service Requests (input, changes during the process, reporting).
- Phone call processing is used to coordinate urgent matters and High priority Incidents registration.
- E-mail is used for sending general information and notifications – support@forbis.lt.

A Service Request is registered by entering the request into the Service Desk system.

4.2 Incident Management CP.15.

Forbis will act as the primary point of contact for incident management and will coordinate troubleshooting, analysis, and resolution activities with all relevant parties to ensure timely restoration of services and proper functioning of the solution.

Support services shall include incident registration, classification, prioritization, root cause analysis, workaround provision where applicable, resolution implementation, and communication with NBM regarding incident status and resolution progress.

Incident Reaction

The Tenderer will start working on NBM registered incident within the specified timeframe counting from receiving an RFS (Request for Service) with the incident details and context of occurrence.

RFS is registered when:

- Receiving phone calls with CRITICAL or HIGH PRIORITY, or
- RFS is entered in Service Desk system by the NBM

NBM sets the Incident priority (CRITICAL, HIGH, NORMAL, LOW). For more details of classification please refer to CP. 29. “Support service level” chapter.

The Tenderer may change the priority of the Incident if no objection of the NBM in Service Desk system is received in reasonable time and prioritization of the Incident is clearly not correct. In all cases, a change of priority must be motivated and justified.

For CRITICAL or HIGH PRIORITY, phone call based RFS must be registered in Service Desk by the NBM.

All other RFS are registered by the NBM in Service Desk system.

Applicable to the following NBM’s environments:

- Production (PROD) (highest possible priority is CRITICAL or HIGH)
- PRELIVE (highest possible priority is NORMAL)

The Tenderer will provide NBM detailed information regarding the identified cause of the incident, the rationale for the corrective actions undertaken, and the planned preventive measures intended to avoid the recurrence of similar incidents in the future.

Patch Delivery

Patch is delivered to NBM with intent to resolve the root cause of a registered incident. Patch is an expected permanent fix to a problem or incident.

Workaround

Workaround to an incident or problem is delivered to NBM with intent to quickly remedy issues due to a registered Incident (based on RFS) with goal of resuming normal or limited operations with system within the agreed SLA timeframe. The NBM shall ensure remote access to the system live environment to the Tenderer’s specialist in 30 minutes after High Priority Incident is registered. If no workaround could be presented, the Patch is delivered according to the SLA terms.

4.3 Problem Management CP.16.

Root Cause Analysis

RCA delivers reports and solutions to Incident Root Causes in the form of software Patch or other means that avoid similar Incidents in the future. Results of RCA are:

- Permanent fix to the Root Cause (Patch)
- Root Cause Analysis Report
- Other possible means including reasonable instructions

The goal is that all incidents must have root causes determined with patch or other solutions provided.

RCA can include intermediate means to help isolate the root cause during the next incident and/or to alleviate impact of the next incident.

Problem Management

Forbis keeps a list containing:

- all incidents connected with NBM with unresolved root causes and current status;
- incidents connected with NBM that have occurred more than once;
- Relevant Events from Event Management that have or may have direct effect on the NBM's system installation, such as required component update, required version upgrade, required patch of system component, etc. which can rise from system intrinsically (e.g. a resolved root cause and resulting patch from RCA with another customer) or from the underlying technologies that system is built on (e.g. Oracle database mandatory upgrade or software Patch).

The goal of Problem management is to guarantee that system can run on up-to-date system components, has clear upgrade path to newer versions of system and underlying technologies and that different events are cross-correlated and analysed for resulting effect or unexpected potential Incidents.

The Tenderer will receive, collect, analyse, and document all relevant information related to the identified problem in order to ensure effective investigation and resolution. Such information should include, but shall not be limited to, observed symptoms, operational impacts and effects on the solution or business processes, frequency and recurrence patterns, affected components or interfaces, logs and diagnostic data, as well as any specific technical or environmental conditions under which the problem occurs.

The Tenderer will perform detailed analysis and localization of the problem at the solution component level in order to accurately determine the source and scope of the issue. The analysis will include evaluation of affected modules, interfaces, integrations, infrastructure elements, databases, system software, and related services that may contribute to or be impacted by the problem.

Regular status updates or status meetings regarding problems and incidents solving will be established with NBM.

4.4 Configuration Management CP.16e.

The Tenderer, where the identified solution requires configuration-level changes, will provide NBM with detailed guidance for their implementation. This includes step-by-step instructions, validation steps, and any prerequisites necessary to ensure correct and safe application of the changes.

Configuration Approvals:

- The Tenderer will confirm planned configuration changes by NBM.
- The NBM will enter RFS to Service Desk with request to confirm planned configuration change with details of planned change.
- The Tenderer will perform evaluation of planned changes to NBM system and will confirm planned changes or propose amendments within agreed timeframe.
- The goal is to avoid changes that can cause disruptions or degradation of system availability and functional and non-functional quality.

4.5 Configuration Management CP.16f.

Request for Change (RFC)

The NBM can register in Service Desk System RFC regarding major functional or architectural changes development or consultancy requiring extensive analysis, custom design, business process transformation, or project-based activities needs which has been not involved in tender scope.

The Tenderer reviews RFC, evaluates it and does one of the following:

- accepts RFC and initiates Proposal for Change, or;
- sends RFC rejection notes including exhaustive list of issues preventing acceptance.

If the requirements submitted by the NBM are insufficiently detailed, the Tenderer shall have the right not to accept the RFC for evaluation or may propose to charge for the requirement gathering and detailing services.

Request for Proposal (RFP)

The Tenderer has Accepted RFC and initiated building a proposal for a change with the scope of Analysis or Development, depending on the RFC scope.

The RFP includes cost and possible deadline for completion. RFP shall be forwarded to the NBM on RFP form and nominally constitutes a binding proposal.

Once the Tenderer proposal has been accepted by the NBM, a Work Order shall be issued and signed by both Parties, with the changes to be made.

4.6 Service Maintenance CP.18., CP.19.

The Tenderer will provide comprehensive maintenance services to ensure that the solution remains stable, secure, fully supported, and operates at optimal performance levels throughout the entire service lifecycle.

For this purpose, the Tenderer plans to deliver, implement, and support relevant software updates, patches, fixes, modifications, enhancements, and new solution versions necessary to maintain operational continuity,

security compliance, compatibility with supported infrastructure environments, and alignment with evolving business and technical requirements.

Maintenance services will include corrective, adaptive, preventive, and evolutionary maintenance activities, including issue resolution, some optimizations and security improvements, where is possible, of supported software versions within mutually agreed timelines and maintenance procedures.

4.7 Release Management CP.20., CP.21.

New releases will consist of consolidated software packages of the solution provided by the Tenderer to NBM, incorporating all previously implemented updates, modifications, fixes, patches, and enhancements delivered under the maintenance services.

Such releases may additionally include new functionalities, components, technical improvements, architectural enhancements, security updates, performance optimizations, compatibility adjustments, or other changes introduced as part of the ongoing evolution and development of the solution.

The Tenderer will ensure that each new release is fully tested, documented, version-controlled, and delivered in accordance with release management best practices.

As part of the maintenance services, Tenderer will ensure that supported versions and functional updates of the solution continue to align with EU GDPR existing requirements. Further, any substantial customer-specific compliance adaptations, business process redesign activities, or implementation of new regulatory requirements requiring significant custom development may be subject may be subject to separate commercial agreement.

4.8 Distinction between Maintenance and Development Requests CP. 24.

Requests related to the correction of defects, errors, or malfunctions in existing functionality, as defined under maintenance and support services, shall not be considered development or modification requests and shall be handled under the applicable corrective maintenance procedures.

A modification or development request (RFC) in accordance with CP.16 f. "Change request Management" shall be defined as a formal request from NBM to the Tenderer for changes to the solution’s functionality or for the delivery of new functionality according to mutual agreed commercial conditions.

4.9 Support service level CP. 29.

Response Time (RT) – the time within which the Tenderer will respond to a support request, diagnose the issue, and determine the actions necessary to resolve it.

This includes, where applicable, the classification of the incident severity, identification of potential root causes, and definition of the next steps for resolution, such as workaround provision, escalation, or assignment to the appropriate support or development team.

The Response Time is intended to ensure timely engagement by the Tenderer and the prompt initiation of investigative and corrective activities in accordance with the agreed Service Level Agreement (SLA).

Resolution Time (RS) – the objective time within which Tenderer is expected to take all actions within its area of responsibility to fully resolve the NBM's request.

This includes, where applicable, the implementation of corrective measures, application of fixes or workarounds, system adjustments, configuration changes, or other technical activities required to restore normal operation of the solution and eliminate the underlying issue. If there are system changes, they shall be delivered with patches for dedicated environment (TEST or PRELIVE or PROD accordingly in sequence one by one).

The Resolution Time represents the period from the initial acceptance of the request until the complete resolution of the incident, in accordance with the agreed Service Level Agreement (SLA) and severity classification rules.

JIRA classification - NBM's support and maintenance incidents/problems/requests (further – requests) are classified according to their importance for NBM. The importance is assessed based on the impact (actual or potential) of the event that triggered the request on the quality parameters of the solution's operation (see definitions above). Requests will be classified on the following scale:

Classification	Impact on application operational quality parameters
Critical	Availability: the application is unavailable for all or most business users. Important transactions must be processed as soon as possible (within hours). Usability: key business functions are unusable. No alternative procedures or functionalities exist. Performance: response time to user queries renders the application practically unusable. Security: major risks to the confidentiality, integrity, or availability of information.
High	Availability: the application is unavailable to a significant number of users. Important transactions and operations must be processed by the next day. Usability: key business functions are usable only in a limited way. Performance: response time significantly affects key business processes. Security: high risks to confidentiality, integrity, or availability of information.
Medium	Availability: the application is unavailable to a portion of users. Important transactions and operations must be processed within three days. Usability: business functionality is usable but limited. Performance: response time moderately affects business processes. Security: risks to confidentiality, integrity, or availability of information.
Low	Availability: the application is unavailable for a limited number of users. No critical transactions or operations are pending for the next three days. Usability: minor impact on functionality. Alternative procedures or functionalities exist. Performance: response time is slower than usual but does not affect business operations. Security: minor risks to confidentiality, integrity, or availability of information.

When placing a support or maintenance request, NBM will assign a classification and include brief justification in Service desk system JIRA. NBM may reclassify submitted requests depending on changes in the request context. As well The Tenderer may change the priority of the incident/request if no objection of the NBM in Service Desk system is received in reasonable time and prioritisation of the incident/request is clearly not correct. In all cases, a change of priority must be motivated and justified.

4.10 Response Time (RT) and Resolution Time (RS) SLA CP. 32.

The indicative level of support services provided by the Tenderer will meet the following requirements:

Request Classification	Response Time (RT)	Resolution Time (RS)
Critical	60 min	4 hours
High	3 hours	1 day
Medium	24 hours	3 days
Low	3 days	Best effort

4.11 New solution versions upgrade terms CP. 33.

Implementation of new solution versions shall not be mandatory for NBM and shall be performed only upon NBM's acceptance. At the same time, NBM shall ensure that the implementation of new versions is carried out at least once within a maximum period of three (3) years, in order to maintain the solution within a supported and up-to-date product lifecycle.

The Tenderer will provide appropriate support, documentation, and technical assistance required for the planning, testing, and deployment of new versions.

Tenderer will provide NBM with a forward-looking schedule of planned updates and new version releases to ensure adequate planning and preparation.

For software updates, the Tenderer will notify NBM at least one (1) month in advance of the planned release, including relevant information on scope, impact, and required actions.

For new solution versions, the Tenderer shall provide notification at least six (6) months in advance, including preliminary release information, expected changes, and any anticipated impact on the solution, enabling NBM to properly assess, plan, and execute necessary testing and deployment activities in accordance with its internal procedures.

4.12 Support services providing approach CP. 43.

Tenderer specialists provide Support services remotely. In case of Tenderer's specialists shall travel to NBM headquarters, NBM shall cover related travel and accommodation costs. In any travel case, both Parties must agree such travel plans in advance.

All changes to the solution arising from the provision of post-implementation support and maintenance services shall be managed in accordance with a mature change management process according to ISO 20000 and ITIL principles.

4.13 Change management and solution level CP. 50.

Precondition - base information regarding Change Management is provided in "Initial Project Management Plan (CMP.17) document's Chapter 10 Change management plan".

Below is provided more detailed information regarding the proposed Change management and solution level approach.

Main principles

The Tenderer applies established IT Service Management (ITSM) principles and industry best practices aligned with the ITIL framework to ensure the effective delivery of support, maintenance, and development services throughout the solution lifecycle.

The objective of the proposed approach is to ensure service stability, controlled implementation of changes, continuous service improvement, and transparent cooperation with NBM.

Service management.

The Tenderer's service management model is based on the following principles:

- Customer-focused service delivery.
- Defined roles and responsibilities.
- Risk-based decision-making.
- End-to-end service ownership.
- Controlled and traceable change implementation.
- Continuous monitoring and service improvement.
- Transparency and regular reporting.
- Compliance with security and regulatory requirements.

All support, maintenance, and development activities are performed according to documented procedures and governed through agreed service management processes.

Incident and service request management.

The Tenderer operates a centralized Service Desk that serves as the primary point of contact for all incidents, service requests, and change requests.

The process includes:

- Request registration and categorization.
- Priority assignment based on business impact and urgency.
- Initial analysis and diagnosis.
- Escalation to appropriate technical specialists when required.
- Resolution and service restoration.
- User communication and status updates.
- Formal closure and documentation.

Service performance is measured through agreed Service Level Agreements (SLAs), including Response Time and Resolution Time targets.

Change management.

All changes affecting the solution are managed through a formal Change Management process designed to minimize operational risks and ensure service continuity.

The Change Management process includes:

Change identification - changes may originate from:

- Maintenance activities;
- Corrective actions;
- Regulatory requirements;
- Security updates;
- Business-driven enhancement requests;
- New functionality requests.

Change Assessment - Each change request is evaluated considering:

- Business impact;
- Technical impact;
- Dependencies;
- Risks;
- Required effort and resources;
- Expected implementation timeline.

Change Approval - changes are reviewed and approved according to their nature, complexity, and risk level. Where applicable, approval is obtained from NBM before implementation activities commence.

Change Implementation - approved changes are implemented according to agreed development and deployment procedures.

Implementation activities may include:

- Configuration updates;
- Software modifications;
- New functionality development;
- Security enhancements;
- System integrations.

Testing and Validation - before deployment, changes undergo appropriate testing to validate:

- Functional requirements;
- Integration requirements;
- Performance expectations;
- Security requirements;
- Regression impact.

Deployment and Release - changes are deployed in a controlled manner according to agreed deployment procedures and release schedules.

Where required, rollback procedures and contingency plans are prepared to reduce operational risks.

Release and Version Management.

The Tenderer maintains a structured approach to release and version management.

Updates and new versions are planned, documented, tested, and communicated in advance to NBM.

Release management activities include:

- Release planning;
- Release documentation;
- Deployment preparation;
- User communication;
- Post-release verification.

All releases are designed to maintain system stability while introducing improvements, corrections, and new capabilities.

Service Monitoring and Continuous Improvement.

The Tenderer continuously monitors service quality and operational performance.

Key activities include:

- SLA monitoring;
- Incident trend analysis;
- Root cause identification;
- Service quality reviews;
- Preventive and corrective actions;
- Process optimization initiatives.

According mutual agreement, monthly or quarterly service reports are provided to NBM, including service performance metrics, incident statistics, SLA compliance indicators, and continuous improvement activities.

Governance and Communication.

Effective governance and communication are essential components of the service delivery model.

The Tenderer maintains regular communication with NBM through:

- Service Desk operations;
- Status updates;
- Change coordination activities;
- Service review meetings;
- Periodic reporting.

All activities are documented to ensure transparency, traceability, accountability, and alignment between the Parties.

The proposed ITSM and Change Management approach provides a structured framework for delivering support, maintenance, and development services. Through the application of ITIL-aligned practices, the Tenderer ensures service reliability, controlled change implementation, operational efficiency, and continuous improvement while supporting NBM's evolving business and technical requirements.

Detailed description of Change management is presented in the document Forbis_Change_Management.docx

4.14 Approach for the termination of post-implementation support and maintenance services (High-Level Approach) CP. 60.

Precodition – Support and maintenance services agreement is valid, but planned to terminate it (i.e. not prolong). Below provided suggestions regarding high level approach.

Generally, the Tenderer proposes a structured, ITIL-aligned approach to the termination of post-implementation support and maintenance services, ensuring service continuity and a controlled transition in accordance with NBM requirements.

As mentioned earlier, the Tenderer confirms full compliance with the EBA Guidelines on Outsourcing Arrangements (EBA/GL/2019/02), particularly the requirements on exit strategies set out in Sections 99–104, which require institutions to ensure the continuity of critical or important functions in the event of termination. In line with these provisions, Forbis ensures that non-extension of post-implementation support and maintenance services will not adversely impact the NBM’s operations, and that the solution remains fully operational, accessible, and independently maintainable.

In accordance with EBA/GL/2019/02 Section 102 (exit plans and transition), Forbis maintains documented exit and transition procedures, including complete technical documentation, data accessibility, and structured knowledge transfer. These measures ensure that the NBM can seamlessly transfer services to another provider or take over maintenance internally without disruption, fully preserving operational continuity and avoiding vendor lock-in.

The exit approach includes, at a minimum, the following key activities.

Exit planning and coordination

- Initiation of exit process upon contract termination or expiration
- Agreement on exit timeline, scope, and responsibilities with NBM
- Definition of transition governance and communication channels

Service continuity assurance (in terms of valid agreement or if would be concluded separate mutual services prolongation agreement including terms, plans and financial parts)

- Ensuring ongoing support activities remain stable during the transition period
- Controlled handling of open incidents and service requests
- Avoidance of disruption to business-critical operations

Knowledge transfer

- Transfer of relevant technical and operational knowledge
- Walkthrough sessions covering system architecture and configuration
- Sharing of support procedures, troubleshooting guidelines, and best practices

Documentation handover

- Delivery of up-to-date technical and user documentation
- Provision of system design, integration, and configuration details
- Handover of relevant operational and support documentation

Operational transition support

- Assistance to NBM or a designated third party in understanding the solution
- Participation in clarification sessions and knowledge-sharing workshops
- Support in onboarding new support provider where applicable

Data and service closure activities

- Final service reporting and performance summary
- Closure of outstanding tickets or agreed transfer of ownership
- Removal of operational dependencies in a controlled manner

Security and compliance

- Continued compliance with confidentiality and security obligations during exit
- Secure handling of all transferred information and artifacts

This approach ensures a structured, low-risk termination process and supports NBM in maintaining uninterrupted service operations.

Above has been mentioned high level approach, therefore all details shall be agreed separately by both Parties.