

**NON-FUNCTIONAL REQUIREMENTS**

Note: The Tenderer will indicate the extent to which its tender meets the requirements by completing the cells in the "Tenderer's Response" column with one of the following options: <Yes - the solution fully meets the requirement>; <Partially yes - The

Requirement Code	Requirement	The level of obligation	Lot I/II	Tenderer's Response	Tenderer's Comment
<b>1. Non-functional requirements</b>					
CNF.1	Non-functional specifications define requirements that are not directly tied to the core functionalities provided by the requested solution(s). Instead, they focus on aspects crucial for the solution's usability, maintainability, and adaptability to evolving business needs over time. The applicative solution(s) proposed in this acquisition must fully align with the established non-functional requirements outlined below.	Informative	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE and Oracle Banking Product Processor are designed to fully meet non-functional requirements by incorporating a modular, scalable, and secure architecture that supports long-term adaptability and maintainability. The solution emphasizes usability through a standardized user interface built on Oracle's Redwood UX principles, ensuring consistent interactions across modules and user roles. It supports maintainability through parameter-driven configuration, separation of business logic from presentation, and clear layering of components for easier upgrades and extensions. The architecture is also highly adaptable to evolving business needs, with support for integration via open APIs (REST, SOAP), compliance with industry standards (such as ISO 20022, PCI DSS, and Java EE), and deployment flexibility across on-premise, cloud, and hybrid environments. High availability, robust audit trails, granular role-based access control, and support for regulatory reporting further ensure that the platform meets the non-functional expectations critical to running modern banking operations.
<b>1.1. Solution-level architecture</b>					
CNF.2	<p>The proposed solution's architecture must be fully aligned with the NBM's requirements, prioritizing usability, flexibility, interoperability, and maintainability. The NBM mandates the adoption of an open, modular architecture, based on pre-integrated components and compliant with industry-leading standards, facilitating straightforward integration processes.</p> <p>The solution's architecture should embed contemporary industry best practices, incorporating modern concepts such as:</p> <ul style="list-style-type: none"> <li>- <b>Unified Contextual Experience:</b> The architecture must prioritize a unified and intuitive user experience across all system contexts, ensuring operational cohesion.</li> <li>- <b>Real-time Operation:</b> The solution must demonstrate the capability for real-time processing to meet the dynamic needs of the NBM's operations.</li> <li>- <b>Plug-and-Play:</b> The architecture should support seamless integration and interaction with external systems, enabling a "Plug-and-Play" approach for additional components or functionalities.</li> <li>- <b>Cloud-Ready Capabilities:</b> It is imperative that the solution's architecture is designed with cloud-ready features, ensuring scalability, accessibility, and efficiency in a cloud ready environment.</li> <li>- <b>Future-Ready Architectural Design:</b> The proposed architecture must exhibit forward-thinking attributes, anticipating technological advancements and accommodating future developments without substantial reengineering.</li> </ul> <p>These principles are foundational and should be incorporated at all levels of the proposed solution's architecture.</p>	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE and Oracle Banking Product Processor deliver an open, modular architecture built on pre-integrated, standards-based components that align with NBM's priorities of usability, flexibility, interoperability, and maintainability. A unified contextual experience is achieved through the Redwood UX framework and role-based workspaces that present consistent screens and data across retail, corporate, and back-office contexts, eliminating the need to navigate multiple applications. Real-time operation is inherent in the platform's event-driven, in-memory processing and immediate database posting, ensuring balances, limits, and transaction statuses are always current. Plug-and-play integration is enabled by a comprehensive suite of REST and SOAP APIs conforming to ISO 20022 and other industry standards, allowing external systems to be added or replaced without code changes. The solution is cloud-ready, packaged as containerized microservices deployable on Oracle Cloud Infrastructure or any CNCF-compliant Kubernetes environment, providing elastic scaling, automated failover, and DevSecOps pipelines. Its future-ready design leverages domain-driven microservices, parameterized product factories, and extension hooks that let new business capabilities or regulatory changes be introduced through configuration rather than redevelopment. Together, these attributes ensure the proposed solution can evolve with NBM's strategic goals while minimizing total cost of ownership and safeguarding long-term technological relevance.

	<p><i>The Tenderer is expected to provide a comprehensive description and explanation in their bid, detailing the extent to which the proposed solution aligns with these requirements. The Tenderer should specifically address how each mentioned concept is integrated into the architecture, ensuring clarity on the adaptability, responsiveness, and longevity of the proposed solution.</i></p>				
CNF.3	<p>It is strongly recommended that the proposed solution adopts a standardized concept for user interaction to enhance usability, efficiency, and overall user experience. The key guiding principle is to provide a unified interface for each distinct group of users (e.g. users with process management role, external users / customers, report users, users with administrative role etc.), ensuring seamless access to essential business functions.</p> <p>By implementing a standardized interface for each user group, the solution aims to:</p> <ul style="list-style-type: none"> <li>- <b>Enhance Consistency:</b> Provide a consistent look and feel across different functionalities, reducing the learning curve for users and promoting a cohesive user experience.</li> <li>- <b>Improve Efficiency:</b> Streamline user interactions by presenting relevant features in a user-friendly manner, optimizing task execution and minimizing complexity.</li> <li>- <b>Facilitate Training and Onboarding:</b> Simplify training processes and onboarding for new users by offering uniform interfaces tailored to their specific roles.</li> </ul> <p><i>The Tenderer is required to elaborate on how the proposed solution aligns with this user interaction standardization recommendation in their bid. Specifically, please provide insights into the design rationale, user testing methodologies, emphasizing the commitment to delivering a user-centric and operationally efficient system.</i></p>	Recommended	Lot I	Yes - the solution fully meets the requirement	<p>Oracle FLEXCUBE and Oracle Banking Product Processor adopt a standardized and role-based user interaction model that enhances usability, efficiency, and user experience by delivering a consistent and intuitive interface across all functional areas. The interface design is based on Oracle's Redwood UX standards, ensuring a uniform look and feel across screens, workflows, and navigation patterns regardless of the user role or business function. Each user group, whether it be process managers, operations staff, report users, or administrators, is assigned specific menus and task views aligned with their responsibilities, ensuring that only relevant features are visible and accessible. This streamlining reduces complexity and supports faster task execution. The use of standardized screen structures, consistent labeling, and logical field groupings significantly lowers the learning curve, enabling users to move seamlessly across modules without retraining. Furthermore, the platform's modular and parameter-driven configuration allows institutions like NBM to tailor user interfaces to evolving operational needs without changing the underlying application, thus simplifying training and accelerating onboarding for new users.</p>
CNF.4	<p>The application architecture must adhere to open standards or widely adopted standards to guarantee seamless compatibility, interoperability, and scalability. This ensures that the system remains adaptable to evolving technological landscapes and can effectively integrate with other systems and technologies. Furthermore, the application architecture will be designed, integrated, and developed utilizing industry best practices (e.g. TOGAF, BIAN etc.).</p> <p><i>To demonstrate alignment with this requirement, Tenderers are requested to:</i></p> <ul style="list-style-type: none"> <li>- <i>Provide detailed documentation showcasing how the proposed architecture aligns with recognized open or widely used standards. This should include references to specific standards and protocols utilized within the architecture.</i></li> <li>- <i>Describe how the proposed architecture aligns with industry best practices and frameworks. Reference industry-recognized resources such as TOGAF, BIAN etc.</i></li> <li>- <i>Highlight architectural components or design principles that contribute to scalability and adaptability over time.</i></li> </ul>	Mandatory	Lot I	Yes - the solution fully meets the requirement	<p>Oracle FLEXCUBE and Oracle Banking Product Processor are architected using widely adopted open standards and align with globally recognized frameworks such as TOGAF and BIAN to ensure interoperability, scalability, and long-term adaptability. The architecture is based on a service-oriented model that utilizes standard protocols including REST and SOAP for service communication, ISO 20022 and XML for financial messaging, and Java EE for application development, all of which support seamless integration with third-party systems and evolving enterprise landscapes. From a best-practice standpoint, the solution's architectural governance is aligned with TOGAF principles, ensuring that business, data, application, and technology layers are clearly separated and independently scalable. BIAN-aligned service domains ensure functional modularity, enabling NBM to plug in, replace, or extend capabilities without disturbing core processing components. Scalability is further achieved through horizontal scaling of stateless application components, containerization for cloud portability, and Oracle RAC for database clustering. The use of industry-standard integration patterns, parameter-driven configuration, and a decoupled front-end architecture ensures that the system can evolve in response to regulatory, business, and technology shifts without requiring fundamental reengineering, making it a future-proof solution for modern banking needs.</p>
	<p>The application architecture will be designed to be service-oriented, embracing either Service-Oriented Architecture (SOA) or microservices-based deployments.</p> <p><i>To demonstrate alignment with this requirement, Tenderers are requested to:</i></p>				<p>Oracle FLEXCUBE and Oracle Banking Product Processor use a hybrid service-oriented architecture</p>

CNF.5	<p>- Provide a rationale for selecting either SOA or microservices architecture, considering factors such as the system's complexity, scalability requirements, and organizational capabilities. Justify how the chosen approach aligns with the project's objectives and anticipated future needs.</p> <p>- Describe how the architecture facilitates modularity and loose coupling between services or components. Highlight mechanisms for service discovery, communication, and orchestration that promote independence and flexibility.</p> <p>- Explain how the architecture supports scalability and elasticity, allowing the system to handle varying workloads and adapt to changing demands. Describe strategies for horizontal scaling, load balancing, and resource optimization within the chosen architectural paradigm.</p> <p>- Address how the architecture ensures resilience and fault tolerance, minimizing the impact of service failures or disruptions. Describe mechanisms for fault isolation, and automatic recovery to maintain system integrity and availability.</p>	Mandatory	Lot I	Yes - the solution fully meets the requirement	<p>that combines mature SOA principles with containerised microservices for new functional domains, a choice that balances the stability required for complex core banking transactions with the agility needed for rapid digital expansion. This approach matches project objectives by allowing established, high-volume processes to run on proven SOA services while enabling new capabilities—such as real-time APIs or regulatory add-ons—to be delivered as independently deployable microservices, ensuring future scalability and ease of change. Modularity and loose coupling are achieved through well-defined REST and SOAP interfaces, an internal service registry for discovery, and an event bus that orchestrates inter-service communication without hard dependencies. Scalability and elasticity are provided by stateless application tiers that can be horizontally scaled under a Kubernetes or Oracle WebLogic cluster, fronted by load balancers that distribute traffic and optimise resource utilisation; database scalability is delivered through Oracle RAC and partitioning. Resilience is built in through circuit breakers, retry logic, and container health checks that isolate faults, while orchestrated auto-healing restarts failed services and maintains high availability with near-zero disruption to end-users.</p>
CNF.6	<p>The system must seamlessly integrate with external systems and delivery channels by supporting a comprehensive range of industry-standard protocols, such as:</p> <ul style="list-style-type: none"> <li>- ISO 20022</li> <li>- SOAP/REST/gRPC and HTTP/S for web services-based interfaces</li> <li>- XML</li> <li>- Secure FTP</li> <li>- SMTP / SMPP</li> <li>- Others</li> </ul> <p>To demonstrate alignment with this requirement, Tenderers are requested to:</p> <p>- Describe how the system fully implements each specified protocol, ensuring compliance with industry standards and specifications. Provide details on protocol versions supported and any extensions or customizations implemented to enhance functionality.</p> <p>- Explain the security measures implemented to safeguard data exchanged through supported protocols. Address encryption, authentication, and access control mechanisms to ensure the confidentiality, integrity, and availability of exchanged data.</p>	Mandatory	Lot I	Yes - the solution fully meets the requirement	<p>Oracle FLEXCUBE and Oracle Banking Product Processor are designed to seamlessly integrate with a wide variety of external systems and delivery channels using a comprehensive set of industry-standard protocols. ISO 20022 messaging is natively supported across multiple payment and financial transaction flows, with schema-level validation and customizable message enrichment. Web services are exposed using both SOAP and REST over HTTPS, with REST APIs following OpenAPI specifications and supporting JSON payloads, while SOAP interfaces use WSDL and XML standards for system-to-system integrations. The platform also supports gRPC in containerized deployments for low-latency communication in microservices environments. XML is used extensively for data exchange with regulatory bodies and legacy systems, and mappings are fully configurable. Secure file transfers are enabled through SFTP with PGP encryption, ensuring confidentiality and data protection during batch file exchanges. Email notifications are supported via SMTP, and SMS delivery through SMPP or integration with external gateways. All protocols are secured using TLS 1.2 or higher, with mutual certificate authentication where applicable, and access control is enforced through OAuth2, API keys, and IP whitelisting. Message queues, retry frameworks, and audit logs further ensure that all integrations are traceable, resilient, and aligned with global best practices for financial system interoperability.</p>
	<p>The application architecture will adopt a modern client-server paradigm organized into a minimum of three well-defined vertical layers.</p> <p>The architecture must adhere to industry best practices, emphasizing clear and independent delineation between each layer to ensure a robust and scalable system. Specifically:</p> <ul style="list-style-type: none"> <li>- <b>Presentation Layer:</b> This top-level layer will be dedicated to user interface components and user experience management. It should focus on delivering a responsive and intuitive user interface, leveraging contemporary technologies and design patterns to enhance accessibility and engagement.</li> </ul>				<p>Oracle FLEXCUBE and Oracle Banking Product Processor implement a modern three-tier client-server architecture that cleanly separates presentation, application, and data access concerns. The presentation layer is browser-based and built with Oracle Redwood UX components rendered via HTML5, CSS3, and JavaScript, providing a responsive interface that adapts across devices without local installations. The application layer houses all business rules and processing logic in</p>

CNF.7	<p>- <b>Application (or Business Logic) Layer:</b> The middle layer will encapsulate the application's business logic, rules, and processing functionalities. This layer must be designed to be independent of the presentation layer, fostering a modular and maintainable architecture. The use of industry-standard design patterns and frameworks is encouraged to enhance scalability and ease of maintenance.</p> <p>- <b>Data Access Layer:</b> The bottom layer will handle data storage, retrieval, and management. It should be designed to function independently of both the presentation and application layers, ensuring data integrity and facilitating seamless integration with diverse data sources. Utilizing recognized data access patterns and technologies is imperative for optimal performance and reliability.</p>	Mandatory	Lot I	Yes - the solution fully meets the requirement	stateless Java EE services and PL/SQL packages that expose functionality through REST and SOAP APIs; this layer operates independently of the UI, enabling changes to workflows or rules without affecting the client. The data access layer interacts with Oracle Database using optimized PL/SQL, stored procedures, and ORM abstractions that shield upper layers from physical schema details, enforce data integrity, and support performance features such as partitioning and RAC clustering. Each layer communicates through well-defined interfaces, employing standard design patterns like MVC and DAO to ensure maintainability, scalability, and straightforward integration with additional channels or data sources.
CNF.8	All communication between application components must be securely conducted, exclusively utilizing the internal interfaces of the application components. Additionally, the deployment of all internal components must align with the Zero Trust Network Access (ZTNA) paradigm and fully support this deployment configuration.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE and Oracle Banking Product Processor secure all inter-component communication by restricting traffic to authenticated internal interfaces protected with TLS 1.2 or higher and mutual certificate authentication, enforcing message-level integrity and confidentiality at every hop. Internal services register with an API gateway or service mesh that applies Zero Trust principles—each call is verified for identity, authorisation scope, and policy compliance before it is allowed to proceed. Network micro-segmentation is achieved through Kubernetes network policies or WebLogic channel security, while database connections are constrained to encrypted listeners with enforced wallet-based credentials. Service-to-service requests use signed JWT tokens issued by an internal Identity Provider, and granular access control lists limit east-west traffic to the minimum required ports. Continuous monitoring and audit logging detect anomalous behaviour, and automated revocation of certificates or tokens prevents lateral movement, ensuring the entire deployment aligns with ZTNA requirements and maintains rigorous security even inside the data centre boundary.
CNF.9	The application will have capabilities for optimized processing of user queries (e.g. caching).	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE and Oracle Banking Product Processor support optimized processing of user queries through multiple mechanisms including in-memory caching, indexed data retrieval, and query optimization techniques at both the application and database levels. Frequently accessed reference data and configuration parameters are cached in memory at the application layer to reduce database hits and improve response times. The underlying Oracle Database uses cost-based optimization, materialized views, and adaptive execution plans to enhance the performance of dynamic queries. Screen-level searches leverage indexed columns, pagination, and query filters to handle large data sets efficiently. Additionally, application logs and performance monitoring tools are used to identify long-running queries and tune them proactively, ensuring a consistently responsive user experience even during peak usage.
	<p>The production environment must exhibit a resilient architecture that supports active-passive configurations across two distinct geosite locations. This setup is required to ensure high availability and operational stability.</p> <p>To align with the NBM standards and facilitate appropriate sizing of the architecture, the following parameters are to be considered:</p> <p>- <b>High Availability Configuration:</b> The production environment is mandated to operate in an active-passive configuration across two geosite locations. This design ensures redundancy and fault tolerance, minimizing the risk of downtime and providing high availability services to users.</p>				Oracle FLEXCUBE and Oracle Banking Product Processor support deployment in an active-passive high availability configuration across two geographically distinct sites, fully aligning with NBM's

CNF.10	<p>- <b>Service Level Agreement (SLA):</b> The IT solution's SLA is set at 99.7%, measured on a monthly basis during the system's operating hours from 8:00 to 18:00. This commitment underscores the dedication to providing a consistently high level of service availability during crucial operational periods.</p> <p>- <b>Recovery Time Objective (RTO):</b> The stipulated Recovery Time Objective (RTO) is set at 4 hours. In the event of a disruption, the system must be restored to full functionality within this timeframe, minimizing downtime and ensuring a prompt return to normal operations.</p> <p>- <b>Recovery Point Objective (RPO):</b> The system's Recovery Point Objective is established at zero data loss. This means that in the event of a failure, the system must be capable of recovering to a state where no data loss has occurred, ensuring data integrity and consistency.</p> <p>- <b>Switchover Time Between Primary and Backup Sites:</b> Switchover between primary and backup sites is expected to be executed swiftly, with a time constraint of no more than 1 hour. This requirement emphasizes the importance of a rapid transition to the backup environment in case of a geosite failure, further minimizing any potential service interruptions.</p>	Mandatory	Lot I	Yes - the solution fully meets the requirement	<p>requirement for operational resilience and fault tolerance. The solution leverages Oracle Data Guard for real-time database replication with zero data loss, ensuring that the Recovery Point Objective (RPO) is met. In the event of a disruption at the primary site, automated or manual switchover to the secondary site can be completed within the required one-hour window, supported by pre-configured failover scripts and health monitoring services. Application servers deployed in a clustered architecture can be restarted or redirected in the secondary site with minimal manual intervention, supporting a Recovery Time Objective (RTO) of under four hours. Load balancers, DNS redirection, and session replication mechanisms are configured to facilitate a swift transition and continuity of user access. The overall architecture, including middleware and database layers, is designed to meet or exceed the specified SLA of 99.7% availability during business hours by minimizing single points of failure and ensuring redundancy across all tiers.</p>
<b>1.1.2. Requirements for presentation layer</b>					
CNF.11	<p>The presentation layer serves as the user interface through which users interact with the business functions of the application. By effectively managing user interactions and providing a user-friendly interface for accessing business functions, the presentation layer plays a pivotal role in ensuring a positive user experience and maximizing the application's utility for both business and administrative purposes.</p>	Informative	Lot I	Yes - the solution fully meets the requirement	<p>The presentation layer in Oracle FLEXCUBE and Oracle Banking Product Processor is designed as a browser-based user interface that serves as the primary interaction point for all users, including business, operational, and administrative roles. It is built using modern web technologies and follows Oracle's Redwood UX standards to ensure a clean, intuitive, and consistent user experience across modules. The UI is responsive and role-driven, providing contextual access to relevant functions and streamlining navigation through dynamic menus, form validations, and guided flows. By separating the presentation logic from the business logic and data layers, the system maintains a modular architecture that enables easy updates to the interface without disrupting core processing. This design supports high usability and accessibility, allowing users to efficiently execute transactions, monitor operations, and perform administrative tasks with minimal training, thereby enhancing productivity and maximizing the value derived from the application.</p>
	<p>All graphical user interfaces must comply with the following high-level principles:</p> <ul style="list-style-type: none"> <li>i. <b>The structure principle</b> - This principle concerns the general architecture of user interfaces and assumes that they are designed and organized in a structured and intuitive way, being based on clear and consistent models, which are easily recognized by users. These models must follow common approaches to similar components and behaviours;</li> <li>ii. <b>The simplicity principle</b> - interfaces should make the user's tasks as simple and optimized as possible, with minimal effort, displaying and communicating in a user-friendly language the available commands and providing intuitive shortcuts that make it easier to access options related to the execution of longer procedures;</li> <li>iii. <b>The visibility principle</b> - interfaces must make visible all the options and commands necessary for a certain activity / task, without distracting the user with information, or improper or redundant operations.</li> </ul>				<p>Oracle FLEXCUBE and Oracle Banking Product Processor implement a Redwood UX-based GUI that embodies the structure, simplicity, visibility, feedback, tolerance, and reuse principles through a consistent design language and reusable component library. Screens follow a predictable header-content-action layout that groups related fields and commands in logical sections, so users immediately recognize where to enter data, review results, and trigger actions, eliminating guesswork and reinforcing a clear mental model. The interface simplifies tasks with wizard-style</p>

CNF.12	<p>iv. <b>The feedback principle</b> - users must be adequately informed about the actions to be taken, or about changes in status, or conditions, but also about errors, or exceptions relevant and of interest to the user in clear, concise and unambiguous language, familiar to users.</p> <p>v. <b>The tolerance principle</b> - interfaces must be flexible and tolerant of user operating errors, reducing the impact of errors and the possibility of misuse of functions, allowing cancellation and repetition of actions, while preventing errors whenever possible.</p> <p>vi. <b>The reuse principle</b> - interfaces must reuse as much as possible both internal and external components and behaviours, maintaining their consistency and reducing the user's effort to reshape the interaction experience.</p> <p><i>To demonstrate alignment with this requirement, Tenderers are requested to:</i></p> <ul style="list-style-type: none"> <li>- <i>Describe how the GUI architecture is designed and organized in a structured and intuitive manner.</i></li> <li>- <i>Showcase examples of GUI components and interactions that reflect intuitive design principles.</i></li> <li>- <i>Showcase how the GUI simplifies user tasks and optimizes usability. Highlight user-friendly language, intuitive navigation, and shortcuts that streamline user interactions. Provide examples of how complex procedures are simplified and made accessible through clear, concise, and optimized interfaces.</i></li> </ul>	Mandatory	Lot I	Yes - the solution fully meets the requirement	flows for complex operations such as account opening or loan disbursement, auto-complete search boxes that anticipate input, contextual menus that surface the most relevant options, and keyboard shortcuts for frequently performed actions, significantly reducing clicks and data entry effort. Visibility is maintained by displaying only role-appropriate fields and actions while keeping key indicators—such as balances, status badges, or pending approvals—prominently on screen, ensuring users see what they need without clutter. Immediate, plain-language feedback is provided through toast messages, inline validations, and color-coded status alerts that confirm success, warn of exceptions, or guide corrective steps, all localized into the user's preferred language. Error tolerance is built in through data pickers, masked inputs, undo options, and maker-checker workflows that allow reversal or correction before final posting, minimizing risk from accidental mistakes. The underlying component library reuses common widgets—buttons, tables, calendar pickers, and dialog boxes—across every module, reinforcing familiarity and reducing the cognitive load when users move between CASA, payments, or administrative screens, thus fully aligning the GUI with industry-recognized usability principles.
CNF.13	The presentation layer of the system shall be accessible exclusively through modern and largely used web browsers, ensuring compatibility with standard operating environments without the need for additional installations.	Mandatory	Lot I	Yes - the solution fully meets the requirement	The presentation layer of Oracle FLEXCUBE and Oracle Banking Product Processor is fully browser-based and designed to be accessible exclusively through widely used modern web browsers such as Google Chrome, Microsoft Edge, Mozilla Firefox, and Safari. The interface is developed using standard web technologies including HTML5, CSS3, and JavaScript, ensuring compatibility across platforms and eliminating the need for any client-side installations, plugins, or proprietary software. This zero-footprint approach allows users to access the application securely from standard enterprise desktops and laptops, while ensuring consistent performance, usability, and compliance with institutional IT policies.
CNF.14	Presentation layer will not implement business rules, except for validating input data.	Mandatory	Lot I	Yes - the solution fully meets the requirement	In Oracle FLEXCUBE and Oracle Banking Product Processor, the presentation layer is strictly responsible for managing user interaction and input validation, while all business rules are implemented in the application layer or database logic. The UI layer performs only front-end validations such as mandatory field checks, input formats, and range constraints to ensure data integrity before submission. Core business logic—such as eligibility checks, rule-based routing, product conditions, and transaction validations—is encapsulated in service components or stored procedures that are invoked after data is submitted from the presentation layer. This clear separation of concerns ensures modularity, maintainability, and alignment with enterprise architecture principles, while also reducing the risk of inconsistent rule enforcement across channels.
<b>1.1.3. Requirements for Business logic layer</b>					

CNF.15	At this level of architecture the basic functionality of the application is implemented. Business logic layer contains the relevant business logic of the application. The business logic is responsible for accessing, processing and transforming the data in the application, manages the business rules and ensures the consistency and correctness of the data. Business logic layer is accessed by Presentation layer to make the business functions of the application available to the user. It can also provide these functions to external applications, through application interfaces that are also part of Business logic layer.	Informative	Lot I	Yes - the solution fully meets the requirement	In Oracle FLEXCUBE and Oracle Banking Product Processor, the business logic layer serves as the core of the application, where all critical banking functionalities and rules are implemented and managed. This layer is entirely decoupled from the user interface and is responsible for receiving validated input, processing transactions, enforcing business rules, and ensuring data consistency across modules such as accounts, loans, and payments. It interacts with the data layer to retrieve and persist information while maintaining referential and transactional integrity. The business logic is built using a combination of Java EE components and PL/SQL procedures, offering both performance and flexibility. This layer is also exposed to external systems through secure and well-documented APIs, including REST and SOAP web services, allowing third-party applications to invoke core business functions such as customer creation, transaction posting, or limit checks. By centralizing the rule execution and data processing in the business logic layer, the system ensures uniform behavior across internal users and external consumers, supports compliance and auditability, and provides a robust foundation for scalability and modular extension.
CNF.16	<p>The business logic layer must demonstrate a high degree of granularity in its component blocks. Each logic block is required to expose its functionalities through well-defined internal and/or external interfaces, facilitating smooth interaction with other system components.</p> <p><i>Please demonstrate how your proposed architecture achieves granularity in the Business Logic Layer components. Please provide insights into the decomposition of business logic into smaller, specialized components, each serving specific functionalities or business capabilities.</i></p>	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE and Oracle Banking Product Processor achieve granular decomposition in the business logic layer by segmenting functionality into fine-grained service components, each mapped to a discrete banking capability such as customer onboarding, account maintenance, limits management, interest accrual, or payment posting. These components correspond to BIAN service domains and are implemented as stateless Java EE services or PL/SQL packages that encapsulate a single responsibility, publish their contracts through versioned REST or SOAP interfaces, and register with an internal service catalogue for discovery. For example, the payments domain exposes separate services for instruction validation, AML screening, fee calculation, posting, and status inquiry, allowing other modules or external systems to invoke only the needed step without loading the entire payment workflow. Each service can be independently scaled, upgraded, or extended via user exits and event hooks without impacting adjacent logic blocks, while integration is handled through lightweight messaging or direct API calls secured by
CNF.17	The Business Logic Layer must maintain independence from the Presentation Layer and external applications accessing it. Regardless of the architectural paradigm chosen (SOA or microservices), the Business Logic Layer should function autonomously, ensuring modularity and separation of concerns.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE and Oracle Banking Product Processor maintain strict architectural separation between the business logic layer and the presentation layer, ensuring that business rules, transaction workflows, and core processing logic are completely independent from the user interface and any external applications. The business logic is implemented as self-contained services using Java EE and PL/SQL components that operate independently of how data is submitted or consumed. These services are exposed through standardized REST and SOAP APIs, enabling controlled access by both internal UI components and third-party systems without embedding presentation logic or channel-specific behavior. This autonomy ensures that changes to the user interface—such as branding, layout, or channel-specific interactions—do not require any modification to the business logic, preserving modularity and facilitating parallel development. Whether deployed using SOA or containerized microservices, the business logic layer in both FLEXCUBE and OBPP is designed to be stateless, reusable, and interoperable, allowing the same set of services to serve different front ends or integrations while enforcing consistent business rules and data integrity.

CNF.18	Business logic layer must contain and have delimited "business workflow" type components and "business entity" type components.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE and Oracle Banking Product Processor distinctly separate "business workflow" and "business entity" components within the business logic layer to support clear modularization and maintainability. Business workflow components are responsible for orchestrating end-to-end processes such as account opening, loan disbursement, payment initiation, or customer onboarding. These workflows define the sequence of steps, enforce rule execution order, and manage state transitions using configurable process flows and approval rules. On the other hand, business entity components handle the core operations associated with specific domain objects such as customers, accounts, products, or transactions. These components encapsulate the data attributes and business rules specific to the entity, such as validation checks, computations, and life cycle management. For example, the "account entity" component manages account-level rules and behaviors, while the "account opening workflow" governs how the account is initiated, approved, and activated. This separation allows for the reuse of entity logic across multiple workflows and ensures that workflows remain loosely coupled to the data model, facilitating independent changes, easier testing, and better scalability.
CNF.19	Accessing the "business entity" type components will be done through the "business workflow" type components.	Mandatory	Lot I	Yes - the solution fully meets the requirement	In Oracle FLEXCUBE and Oracle Banking Product Processor, access to "business entity" components is systematically routed through "business workflow" components to ensure controlled and context-aware interaction with core business data. Workflow components act as orchestrators, managing the overall sequence of operations, enforcing validations, and applying approval logic while invoking entity components to perform specific actions such as fetching customer data, updating account status, or calculating interest. This layered approach ensures that direct access to business entities is not exposed to external layers or channels, thereby preserving data integrity, enforcing process compliance, and maintaining a consistent business context. By encapsulating entity access within workflow-driven controls, the system achieves better auditability, role-based authorization, and modularity, aligning with best practices in enterprise application design.
CNF.20	Business entities must be clearly identified at the level of business logic and encapsulated in the "business entities" components.	Mandatory	Lot I	Yes - the solution fully meets the requirement	In Oracle FLEXCUBE and Oracle Banking Product Processor, business entities are clearly defined and encapsulated within dedicated components at the business logic layer, ensuring a structured and modular approach to domain modeling. Each business entity—such as Customer, Account, Loan, Product, or Transaction—is represented through a specific logic component that manages its associated attributes, behaviors, and rules. These components handle all entity-specific functions including data validation, life cycle management, and rule enforcement, independent of the workflows that may utilize them. For example, the Customer entity component encapsulates all logic related to customer categorization, risk scoring, and document verification, while the Account entity component manages balance types, limits, and product relationships. By encapsulating business logic around these entities, the system promotes code reuse, simplifies maintenance, and provides a clear separation between entity management and process orchestration. This design ensures consistency across multiple workflows and channels that interact with the same underlying business data.
CNF.21	<p>The "business entity" components must encapsulate all data and business logic relevant to the associated business entity. These components should be designed to:</p> <ul style="list-style-type: none"> <li>- <b>Provide all necessary functionality</b> to perform operations related to the business entity.</li> <li>- <b>Enforce applicable rules and constraints</b> to ensure compliance with business requirements.</li> <li>- <b>Preserve the accuracy, consistency, and correctness of the data contained within the component.</b></li> </ul> <p>This ensures that each business entity component remains self-contained, cohesive, and aligned with the principles of modularity and maintainability.</p>	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE and Oracle Banking Product Processor fully comply with this principle by designing each business entity component to encapsulate all data and logic specific to that entity, ensuring self-contained and cohesive functionality. For example, the Account entity component includes operations for balance updates, product eligibility checks, status transitions, and account closure rules, while also enforcing constraints such as overdraft limits, product-specific conditions, and relationship validations. These components serve as the single source of truth for entity behavior, providing clearly defined APIs that expose all supported actions without exposing internal details to external layers. Built-in validations ensure that only valid operations are allowed, and any data updates go through structured checks that preserve accuracy and business integrity. As a result, each business entity remains modular, easy to test, and adaptable to future changes without affecting unrelated parts of the system, thereby aligning with best practices for enterprise-grade application architecture.

CNF.22	The related Business logic layer components must communicate with each other through dedicated internal interfaces / functions (tight coupling).	Mandatory	Lot I	Yes - the solution fully meets the requirement	In Oracle FLEXCUBE and Oracle Banking Product Processor, business logic components communicate with each other through well-defined internal interfaces and tightly coupled function calls within the same application boundary. These interfaces are implemented as service invocations or stored procedure calls that ensure direct and efficient communication between related business logic blocks while preserving execution control and transactional integrity. For example, the loan disbursement workflow component directly invokes account entity logic to validate settlement accounts and post disbursements, ensuring consistency in business rule enforcement. These internal calls are optimized for performance and reliability within the controlled environment of the application server or database engine, and they allow developers to maintain clarity on component interactions while enabling shared use of core logic. Though this design uses tight coupling at the internal level for efficiency, it remains logically modular, as the communication occurs through documented function signatures and parameter structures, allowing changes to be managed centrally and predictably.
CNF.23	Business logic layer components must be accessible to external applications only through the external applicative interfaces defined for this purpose.	Mandatory	Lot I	Yes - the solution fully meets the requirement	In Oracle FLEXCUBE and Oracle Banking Product Processor, access to business logic layer components by external applications is strictly controlled and facilitated only through officially defined external interfaces such as RESTful APIs, SOAP web services, and ISO-standard message interfaces. These external APIs act as a secure and abstracted layer over the internal business logic, exposing only the necessary operations while encapsulating the internal workflows and data structures. This design ensures that external systems—such as digital channels, payment gateways, or regulatory platforms—can interact with the core system without directly accessing internal components, thereby preserving modularity, enforcing security boundaries, and supporting version control. Access to these interfaces is further governed by authentication, authorization, and rate-limiting mechanisms to ensure safe and compliant integration, in alignment with enterprise architecture and governance standards.
CNF.24	Business logic layer architecture will allow concurrent access to application functions.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE and Oracle Banking Product Processor are architected to support high levels of concurrent access to application functions by leveraging a stateless, multi-threaded business logic layer running on clustered application servers. The underlying architecture uses Java EE concurrency mechanisms and Oracle Database transaction management to allow multiple users and external systems to simultaneously invoke business services without conflict or data inconsistency. Each function within the business logic layer operates independently within its own execution context, ensuring thread safety, isolation, and consistency even under heavy transaction loads. Database-level locking, session management, and optimistic concurrency controls further ensure data integrity while supporting high throughput. This design enables the system to scale horizontally and handle concurrent access by large numbers of users and integration points without degradation in performance or reliability.
<b>1.1.4. Requirements for Data layer</b>					
CNF.25	At this level of architecture, application data is stored and accessed. Application data is accessible through database management system (DBMS). At the DBMS level, data integrity rules are established. Data layer must ensure that the data can only be accessed by authorized entities, and the data will remain intact and correct.	Informative	Lot I	Yes - the solution fully meets the requirement	In Oracle FLEXCUBE and Oracle Banking Product Processor, the data layer is implemented using Oracle Database, which acts as the central repository for all application data and enforces data access, integrity, and security rules. Data is accessed only through controlled interfaces such as stored procedures, views, or APIs, ensuring that business logic and presentation layers interact with data in a consistent and secure manner. The database enforces referential integrity, uniqueness, and validation constraints at the schema level to prevent inconsistent or invalid data entry. Role-based access control, database user privileges, and fine-grained access policies restrict data visibility and operations to authorized users only. Additionally, Oracle Advanced Security features such as Transparent Data Encryption (TDE), auditing, and row-level security can be applied to ensure that data remains confidential, unaltered, and protected from unauthorized access or tampering. This architecture ensures that all application data is managed reliably, securely, and in compliance with regulatory and institutional standards.

CNF.26	The data layer must provide the data necessary for the application for providing the functionalities and activity services requested by the NBM.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE and Oracle Banking Product Processor ensure that the data layer is fully capable of providing all required data to support the functionalities and activity services demanded by NBM. The data model is comprehensive, covering all key banking domains such as customer information, accounts, transactions, limits, products, and regulatory data. Data is structured in normalized relational schemas with optimized indexing and partitioning strategies to ensure high-performance retrieval. The business logic layer accesses this data through well-defined stored procedures and views, ensuring accurate and timely delivery of information for both internal processing and external integrations. The system also supports configurable data extraction tools and standard reporting frameworks to deliver activity-level insights and operational data in real-time or on schedule, based on business needs. This ensures that all application functionalities are backed by a robust, consistent, and secure data layer.
CNF.27	The data model implemented at the Data layer level must be normalized. The data will not be stored redundantly, the integrity relationships between the data will be completely and correctly defined and implemented, starting from the business role of the data.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE and Oracle Banking Product Processor implement a fully normalized data model at the data layer, adhering to relational database design best practices. Data is structured to eliminate redundancy, ensure consistency, and reflect the underlying business semantics accurately. Each business entity—such as customer, account, product, or transaction—is represented in its own dedicated table, with clearly defined primary and foreign key relationships that enforce referential integrity. Normalization ensures that updates or changes to data occur in a single location, reducing duplication and preventing anomalies. These integrity relationships are directly derived from the business rules and domain logic, ensuring that the data model is both logically sound and aligned with functional requirements. This design not only optimizes storage and query efficiency but also guarantees data quality and consistency across all modules and processes.
CNF.28	The application must support an integrated data model for the reference information at the application level (common or synchronized nomenclatures).	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE and Oracle Banking Product Processor support an integrated data model for reference information through centralized master and reference tables that store common nomenclatures used across all modules and business processes. Elements such as country codes, currency codes, branch identifiers, customer types, product classifications, and transaction codes are maintained in unified repositories accessible system-wide. These reference data sets are synchronized across application components to ensure consistency and eliminate duplication. Changes to nomenclature or master data are managed centrally and propagated to all dependent functions in real time or via scheduled synchronization processes, depending on configuration. This integrated approach ensures alignment across modules, reduces maintenance overhead, and supports data accuracy throughout the application lifecycle.
CNF.29	The data model must ensure the possibility of migrating data from existing systems in the requested application, as required by the NBM. Data migration must ensure that data will be migrated completely and correctly. The reference source for the allowable range of values and data format is established as the existing systems. Deviations from this requirement may be accepted by the NBM provided that the quality of the migrated data is not affected.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE and Oracle Banking Product Processor are designed to support comprehensive and controlled data migration from existing systems, fully accommodating the requirements set by NBM. The data model is well-documented and includes detailed entity-relationship mappings that allow for clear alignment with legacy system structures. Oracle provides robust tools and frameworks, such as Oracle Data Integrator (ODI), PL/SQL-based scripts, and migration staging layers, to extract, transform, and load (ETL) data while preserving data integrity, completeness, and accuracy. Mapping rules can be customized to align incoming data formats and permissible values with the target model, and validation routines ensure that migrated data adheres to referential integrity and business rule constraints. Any deviations from legacy formats can be handled through transformation logic, with exception reporting and reconciliation processes in place to track and correct mismatches. This ensures that NBM's historical and operational data is fully and correctly migrated into the new system, maintaining continuity and compliance.

CNF.30	The application data must be accessible only through the components contained in the Business logic layer.	Mandatory	Lot I	Yes - the solution fully meets the requirement	In Oracle FLEXCUBE and Oracle Banking Product Processor, access to application data is strictly governed and only permitted through components in the business logic layer. Direct access to the data layer from the presentation layer or external systems is not allowed, ensuring that all data retrieval, updates, and processing go through controlled business services. These business logic components encapsulate the necessary validations, rules, and access controls, thereby enforcing consistency, data integrity, and security. This architecture ensures a clear separation of concerns, prevents unauthorized data manipulation, and maintains traceability and auditability of all data-related operations.
CNF.31	The data stored in the application must be neutral and independent of the Business logic layer.	Mandatory	Lot I	Yes - the solution fully meets the requirement	In Oracle FLEXCUBE and Oracle Banking Product Processor, the data stored in the application is designed to be neutral and independent of the business logic layer, ensuring that the data model reflects core banking domain concepts rather than being tightly coupled to any specific processing logic. The database schema is structured based on normalized relational models that represent business entities such as customers, accounts, transactions, and products in a way that allows for consistent use across various modules and workflows. This neutrality allows the same data to be used by different business processes without modification and supports extensibility, integration, and reporting without reliance on embedded logic. Such a design enables flexibility in adapting or replacing business rules in the application layer without requiring changes to the underlying data, ensuring long-term maintainability and alignment with enterprise architecture best practices.
CNF.32	The data architecture needs to be optimized both in terms of accessing data for transactions (OLTP) and for analysis and reporting (OLAP).	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE and Oracle Banking Product Processor implement a data architecture that is optimized for both Online Transaction Processing (OLTP) and Online Analytical Processing (OLAP) requirements. For OLTP, the application leverages a normalized relational data model with efficient indexing, partitioning, and transaction management features of Oracle Database to support high-volume, low-latency transactional operations across various banking functions. For OLAP and reporting purposes, the solution supports integration with dedicated data marts and data warehouses through standard ETL tools, materialized views, and reporting schemas that are denormalized and optimized for complex queries and aggregation. Additionally, key operational and historical data is extracted in near real-time or scheduled intervals into reporting layers, enabling performance-intensive analytical queries to run without impacting live transaction processing. This dual optimization ensures that the system can efficiently support both day-to-day operations and strategic data analysis requirements.
CNF.33	The data model implemented at the Data layer level must be properly documented. The documentation must contain both the technical description of the data layer (database structures, database objects, integrity relationships, etc.) and the semantic description (association of data structures to business entities and their properties). The semantic description of the data must be available to users within the application, where useful (e.g. customization of reports).	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE and Oracle Banking Product Processor provide comprehensive documentation of the data model implemented at the data layer, covering both technical and semantic aspects. The technical documentation includes detailed descriptions of database tables, views, primary and foreign key relationships, indexes, and other database objects, ensuring a clear understanding of how the data is structured and interrelated. In parallel, semantic documentation maps each database structure to corresponding business entities such as customer, account, product, and transaction, along with descriptions of their attributes and business purpose. This helps in understanding the role and meaning of each data element within the banking context. Additionally, through configuration tools and built-in reporting frameworks, the semantic metadata is made accessible to business users, enabling them to define or customize reports and extract relevant data with clarity. This level of documentation supports transparency, eases maintenance, and empowers users to work effectively with the application's data in a meaningful and business-aligned manner.

CNF.34	The application architecture must ensure the integrity and correctness of the data when accessing and modifying the data simultaneously by several entities (users, internal processes, external applications), with the notification of the user.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE and Oracle Banking Product Processor are designed to ensure data integrity and correctness during simultaneous access and modification by multiple entities including users, background processes, and external systems. This is achieved through robust concurrency control mechanisms such as transaction isolation levels, row-level locking, and atomic operations managed by Oracle Database. The system employs ACID-compliant transaction processing to maintain consistency and prevent data corruption during concurrent updates. When conflicting updates or access attempts occur, the application notifies the user through system messages or validation alerts, indicating that the data has been modified or is currently being used. In critical scenarios, maker-checker workflows and session-based locks are used to control concurrent data changes, ensuring that business rules are enforced and data remains accurate and synchronized across all interfaces. This architecture guarantees reliable and predictable behavior even under high concurrent usage.
<b>1.1.5. Requirements for Technology layer</b>					
CNF.35	This layer encompasses the necessary software and hardware components to support the application components from the Data layer, Business Logic layer, and Presentation layer.	Informative	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE and Oracle Banking Product Processor are supported by a robust infrastructure layer that includes the necessary software and hardware components to host and execute the Data layer, Business Logic layer, and Presentation layer efficiently. This includes enterprise-grade application servers (such as Oracle WebLogic), database servers (Oracle Database), and load balancers, all of which operate within a scalable and secure environment. The infrastructure supports deployment on-premises, in private or public cloud, or in hybrid configurations, offering flexibility based on organizational preferences. Middleware components handle messaging, session management, and integration services, while underlying hardware or virtualized environments are sized for high availability, fault tolerance, and performance. This comprehensive infrastructure foundation ensures that each application layer functions reliably and in coordination with the others to deliver end-to-end banking services.
CNF.36	The technological architecture must ensure the continuous availability and accessibility of application components.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE and Oracle Banking Product Processor are designed with a technological architecture that ensures continuous availability and accessibility of all application components. The solution supports high availability through active-passive and active-active clustering, load balancing, and failover mechanisms across application, database, and web tiers. The architecture allows for redundancy at each level, ensuring that if a component fails, another instance can immediately take over without interrupting service. The system also supports session persistence, seamless recovery, and real-time monitoring to detect and address failures proactively. These capabilities are further enhanced by support for deployment in cloud or hybrid environments, allowing infrastructure scalability and resilience. Together, these design elements ensure that the application remains accessible to users and integrated systems with minimal disruption, even under adverse conditions or peak usage periods.
CNF.37	The technological architecture of the application must have a high level of resistance to failures, not to contain single points of failure (SPOF) at the component level (e.g. microservices, redundant components, balancing etc.).	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE and Oracle Banking Product Processor are architected to achieve high fault tolerance and eliminate single points of failure (SPOF) at the component level. The solution supports a distributed deployment model with redundancy across all critical layers—including database, application servers, and web components—using clustering, load balancing, and active-passive or active-active configurations. Each service component, can be deployed in multiple instances behind load balancers to ensure continuous availability. Oracle Database supports Real Application Clusters (RAC) for database-level fault tolerance, while application services run on clustered middleware platforms such as Oracle WebLogic with automatic failover and session replication. Network components and integration touchpoints can also be configured with redundancy. This architecture ensures that no single component failure can disrupt end-to-end service delivery, thereby maintaining system stability, resilience, and high availability under all operational scenarios.

CNF.38	The technological architecture must ensure the rational and balanced use of processing resources.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE and Oracle Banking Product Processor are built on a scalable, multi-tiered architecture that ensures rational and balanced use of processing resources across application, database, and web layers. The system uses load balancing mechanisms to distribute user requests and processing workloads evenly across multiple application server instances, preventing bottlenecks and ensuring optimal performance. Background jobs and batch processing are scheduled and managed in a way that minimizes impact on real-time transactions, while the database layer utilizes indexing, partitioning, and query optimization techniques to efficiently handle large volumes of data. Resource usage is continuously monitored, and system components can be scaled vertically or horizontally based on performance metrics and business needs. This balanced resource utilization not only enhances response times and system throughput but also improves cost-efficiency and infrastructure sustainability.
<b>1.2. Technological platform</b>					
CNF.39	Technological platform consists of all soft and hard components needed to ensure the operating environment in which the application will run. Technological platform includes: development platforms and programming languages in which the application code is developed, database management services, operating systems based on which they can run the application components, special system software needed to be installed for the correct running of application, the hardware platform on which the application components can run, etc.	Informative	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE and Oracle Banking Product Processor run on a comprehensive technological platform that includes all necessary software and hardware components to ensure a stable and optimized operating environment. The applications are primarily developed using Java EE and PL/SQL, and run on Oracle WebLogic Server or equivalent Java application servers. The backend relies on Oracle Database, which provides advanced data management, security, and performance features. The solution is compatible with leading operating systems such as Oracle Linux, Red Hat Enterprise Linux, and Windows Server. Any required middleware components, including messaging systems and schedulers, are included as part of the solution stack or supported through integration. The platform is flexible enough to be deployed on physical hardware, virtualized environments, or cloud infrastructure (private, public, or hybrid), ensuring adaptability to different IT strategies. This end-to-end platform coverage ensures that all components—from development to execution—are aligned, tested, and optimized for reliable, secure, and scalable performance.
CNF.40	The application should possess minimal dependence on the underlying technology platform to ensure scalability, flexibility, and ease of maintenance.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE and Oracle Banking Product Processor are designed with minimal dependence on the underlying technology platform, ensuring scalability, flexibility, and ease of maintenance. The applications follow open standards and modular architecture principles, enabling deployment across various operating systems, databases (primarily Oracle), and middleware stacks without requiring significant customization. Business logic is decoupled from infrastructure components, allowing seamless scalability through horizontal and vertical scaling, whether on-premise or in cloud environments. The use of Java EE standards, RESTful APIs, and XML/JSON messaging ensures platform independence and facilitates integration with diverse systems. Additionally, configuration-driven design and parameterization allow changes in behavior without altering the core codebase, simplifying upgrades and maintenance. This abstraction from platform-specific dependencies supports long-term adaptability and aligns with enterprise IT governance practices.
<b>1.2.1. General requirements</b>					
CNF.41	The platform technologies present in the application architecture must be open technologies (without proprietary technologies of the supplier), or widely used technologies.  <i>Please provide complete information on the technological platforms supported by the proposed solution.</i>	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE and Oracle Banking Product Processor are built using open and widely adopted technologies that ensure long-term viability, interoperability, and ease of integration. The core application is developed using standard Java EE technologies, which are open and widely supported across platforms and vendors. The business logic and database interactions leverage PL/SQL and Oracle Database, a globally established and enterprise-proven RDBMS technology. Middleware components such as Oracle WebLogic Server and RESTful/SOAP APIs are based on <del>open industry standards like HTTP/S, XML, JSON, and WSDL, allowing integration with third-party</del>
CNF.42	Application components should be hardware-agnostic, capable of running on x86 processors.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE and Oracle Banking Product Processor are fully hardware-agnostic and are designed to run efficiently on industry-standard x86 processor architectures

CNF.43	<p>The application architecture must be tailored for optimal performance in cloud computing environments (at least PaaS). Key characteristics of a system designed for implementation in private clouds include considerations for latency, resilience to component failures, efficient parallelization, and optimization of resource utilization.</p> <p><i>To demonstrate alignment with this requirement, Tenderers are requested to:</i></p> <ul style="list-style-type: none"> <li>- <i>Showcase how the application architecture is optimized for cloud computing environments, particularly private clouds.</i></li> <li>- <i>Provide evidence of how the architecture addresses the unique challenges and opportunities presented by cloud computing, ensuring the application's readiness for deployment in private cloud environments.</i></li> </ul>	Mandatory	Lot I	Yes - the solution fully meets the requirement	<p>Oracle FLEXCUBE and Oracle Banking Product Processor are architected to operate optimally in cloud computing environments, including private cloud and Platform-as-a-Service (PaaS) models. The applications support containerized deployments using Docker and orchestration through Kubernetes, enabling efficient resource utilization, automated scaling, and resilience. The architecture supports microservices and modular components that can be independently deployed and scaled, allowing for better fault isolation and parallel processing of transactions and services.</p> <p>Built-in support for stateless session handling, load balancing, and clustering ensures high availability and low latency in distributed environments. Moreover, the applications leverage cloud-native features such as dynamic provisioning, monitoring, and centralized logging through tools like Prometheus and ELK stack when deployed in private clouds. Oracle's cloud readiness certification and successful deployments on Oracle Cloud Infrastructure (OCI), as well as private clouds like VMware and OpenStack, demonstrate the system's maturity and adaptability in cloud environments. This ensures that the solution meets the performance, scalability, and reliability</p>
CNF.44	The technologies present at the level of the technology platform must be homogeneous (minimum number of different technologies, e.g. different operating systems for middleware and database).	Mandatory	Lot I	Yes - the solution fully meets the requirement	<p>Oracle FLEXCUBE and Oracle Banking Product Processor support a homogeneous technology stack that minimizes the use of disparate technologies, ensuring operational simplicity, easier maintenance, and streamlined support. The solution is typically deployed on Oracle Linux or Red Hat Enterprise Linux for both the middleware and database layers, promoting uniformity in system administration and patch management. The middleware (such as Oracle WebLogic Server) and the database (Oracle Database) are part of the Oracle ecosystem, designed to work seamlessly together, offering optimized performance, integrated security, and coordinated support. This homogeneous approach reduces integration complexity, enhances system stability, and enables more efficient use of IT resources, aligning well with enterprise architecture policies that favor consistency and standardization across the technology platform.</p>
CNF.45	The application must support the creation, modification, processing, storage and access of textual data in Unicode format.	Mandatory	Lot I	Yes - the solution fully meets the requirement	<p>Oracle FLEXCUBE and Oracle Banking Product Processor fully support the creation, modification, processing, storage, and access of textual data in Unicode format. The underlying Oracle Database is configured with Unicode character sets such as AL32UTF8, ensuring that all application data, including multilingual textual content, is handled accurately and consistently. This allows seamless processing of customer names, addresses, product descriptions, and other textual fields in multiple languages and scripts. The user interface and integration layers also support Unicode, enabling end-to-end data exchange without character corruption or data loss. This capability ensures compliance with internationalization standards and supports global deployments across diverse linguistic environments.</p>
<b>1.2.2. Presentation layer</b>					
CNF.46	The application must be accessible to any authorised user, using the standard computing resources available at workplace (desktop stations, virtual desktop / VDI, laptops, printers).	Mandatory	Lot I	Yes - the solution fully meets the requirement	<p>Oracle FLEXCUBE and Oracle Banking Product Processor are designed to be accessible to any authorized user through standard workplace computing resources such as desktop stations, virtual desktops (VDI), laptops, and connected peripherals like printers. The application is browser-based and does not require any client-side installation, making it compatible with standard operating systems and enterprise IT environments. Authorized users can securely access the system via supported web browsers over intranet or VPN connections, ensuring flexibility and ease of access from various endpoints. Print functionalities for reports, statements, and transaction confirmations are supported through native browser print capabilities and integrated reporting tools, allowing seamless use of locally or network-connected printers. This ensures that users can interact with the application using existing infrastructure without the need for specialized hardware or software.</p>

CNF.47	The application will have capabilities to allow access to certain functions (e.g. authorization actions, or accessing operational dashboards and reports) from mobile devices.	Recommended	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE and Oracle Banking Product Processor provide capabilities to allow access to selected functions such as authorization actions, operational dashboards, and reports from mobile devices. While the core application is primarily accessed via desktop browsers, it includes responsive web design for specific screens and functions, allowing them to adapt to smaller form factors like tablets and smartphones. Role-based access control ensures that only authorized users can perform critical actions such as approvals or view sensitive reports from mobile environments. Additionally, integration with mobile device management (MDM) solutions and support for secure mobile connectivity protocols ensures that mobile access remains compliant with enterprise security policies. This flexibility enhances operational efficiency by enabling key decision-makers to act on essential tasks even when away from their primary workstations. Oracle FLEXCUBE and Oracle Banking Product Processor provide capabilities to allow access to selected functions such as authorization actions, operational dashboards, and reports from mobile devices. While the core application is primarily accessed via desktop browsers, it includes responsive web design for specific screens and functions, allowing them to adapt to smaller form factors like tablets and smartphones.
CNF.48	All views and reports in the application must be able to be printed on the indicated page format. The application must automatically size the output documents to fit the format indicated by the user (e.g. A2/3/4, portrait / landscape, etc.).	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE and Oracle Banking Product Processor support printing of all views and reports in user-specified formats such as A2, A3, A4 in both portrait and landscape orientations. The application auto-adjusts layout and scaling to fit the selected paper size, ensuring proper formatting and readability without manual intervention.
CNF.49	The client application must be able to run in Windows 10/11 operating environments and newer.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE and Oracle Banking Product Processor are web-based applications accessible via modern browsers, and are fully compatible with Windows 10, Windows 11, and newer operating environments without requiring local installation or customization.
<b>1.2.3. Business logic layer</b>					
CNF.50	The components constituting the Business logic layer must be developed using modern, widely used developing frameworks and programming languages at the moment.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE and Oracle Banking Product Processor components in the Business Logic Layer are developed using modern, widely adopted technologies such as Java EE for business services and PL/SQL for database logic. These technologies are industry-standard, platform-independent, and supported by a large developer ecosystem, ensuring long-term maintainability, scalability, and ease of integration with other enterprise systems.
CNF.51	The technologies present at this layer must allow the integration of the components that are or will be developed by the NBM through the interfaces provided.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE and Oracle Banking Product Processor support integration with externally developed components through well-defined, standards-based interfaces at the Business Logic Layer. The technologies used—such as RESTful and SOAP web services, JMS, and message queues—ensure that components developed by NBM can interact with the system securely and efficiently. These interfaces are extensible, documented, and designed to support modular integration without impacting core functionality.
<b>1.2.4. Data layer</b>					
CNF.52	The application must be compatible with the latest Long Releases of the following types of databases: Oracle, or MS SQL.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE and Oracle Banking Product Processor are fully compatible with the latest Long-Term Release versions of Oracle Database, which is the preferred and natively supported database platform for these applications. The solution leverages advanced Oracle Database features for performance, security, and scalability. MS SQL Server is not a supported database for these applications. The use of Oracle Database ensures deep integration, optimal performance, and vendor-aligned support, making it the most suitable and proven choice for deployment.
	However, consideration will be given to other database management systems if the Tenderer can sufficiently demonstrate their suitability, including any relative benefits, such as financial advantages, that justify their utilization.		Lot I		
CNF.53	All functional features of the application (OLTP) will be implemented on a single database management platform.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE and Oracle Banking Product Processor implement all functional features (OLTP) on a single Oracle Database platform. This centralized data architecture ensures data consistency, simplifies management, enhances performance, and supports ACID-compliant transaction processing across all business modules without the need for multiple database platforms.
<b>1.2.5. Technology layer</b>					

CNF.54	All application components, including middleware and databases, must be capable of operating in a fully virtualized environment. Compatibility with the VMware hypervisor and support for the x86 platform with either Linux or Windows Server operating systems are essential. Furthermore, the supported versions of these operating systems must be maintained by their providers as part of the last two major releases.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE and Oracle Banking Product Processor are fully compatible with virtualized environments and operate seamlessly on VMware hypervisors. All application components—including middleware and Oracle Database—can be deployed on x86-based infrastructure running either Linux (e.g., Oracle Linux, RHEL) or Windows Server, provided they are among the last two major supported releases. This ensures compliance with modern IT infrastructure standards, enabling flexibility, scalability, and efficient resource utilization in virtualized data centers.
CNF.55	Only standard equipment will be required to run the application, available to be freely purchased on the market by the NBM.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE and Oracle Banking Product Processor are designed to run on standard, commercially available hardware and software components. The solution does not require any proprietary or specialized hardware, allowing NBM to procure infrastructure—such as x86 servers, storage systems, and networking equipment—from any preferred vendor. This ensures flexibility, vendor independence, and cost-effectiveness in infrastructure procurement.
CNF.56	The Tenderer must include in its proposal comprehensive details about the recommended infrastructure platform, ensuring it is appropriately dimensioned to meet the requirements specified in this Technical Specification and the specific needs of the NBM. If the bid is successful, the proposed infrastructure dimensioning will form the basis for further refinement and deployment during the application's implementation phase.	Mandatory	Lot I	Yes - the solution fully meets the requirement	The sizing reference is provided as part of annexure on hardware and technology software requirement.
CNF.57	The Tenderer will propose the technological platform related to the application based on all available information regarding volume, performance, and other relevant factors (presenting all the available alternatives), and the NBM will review the alternatives and make the final decision on the final configuration.	Mandatory	Lot I	Yes - the solution fully meets the requirement	The sizing reference is provided as part of annexure on hardware and technology software requirement.
<b>1.3. Interoperability requirements</b>					
CNF.58	Interoperability is defined as the application's ability to communicate effectively with other systems.	Informative	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE and Oracle Banking Product Processor are built with high interoperability capabilities, enabling seamless communication with other systems through open standards and well-defined integration interfaces. The solution supports RESTful and SOAP web services, ISO 20022 messaging, XML/JSON data formats, and secure file-based protocols such as SFTP, allowing smooth integration with internal and external applications, third-party services, and national or international payment systems.
CNF.59	In order to support the business processes of the NBM, the requested application must be integrated with other existing applications within the organization, as well as with the IT solutions requested in other lots of this tender procedure.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE and Oracle Banking Product Processor are designed for easy integration with existing applications and third-party IT solutions through a comprehensive set of open APIs and industry-standard protocols. The solution supports integration via REST/SOAP web services, message queues, ISO 20022, and file-based interfaces (e.g., SFTP/XML), enabling interoperability with systems already in use at NBM as well as with other solutions procured through this tender. This ensures that end-to-end business processes can operate seamlessly across heterogeneous environments.
<b>1.3.1. Requirements for Enterprise Service Bus component</b>					
CNF.60	As an integral part of the proposed solution, the Tenderer is required to propose and deliver an Enterprise Service Bus (ESB) middleware component. This ESB will serve as a centralized integration platform for all applications and components required under other lots in this tender procedure. In a further perspective it must be capable of being scaled and spanned across the entire organization, facilitating seamless communication and data exchange among all applications operated within the NBM.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Based on these requirements, Fiorano ESB is well-suited for this solution, offering robust integration capabilities and API management to meet both current and future scalability needs.

CNF.61	<p>This component must be capable to serve as an organization-wide integration platform, facilitating the exchange of data and functionalities among disparate systems. Among key capabilities and features to be delivered as part of this component include:</p>	Mandatory	Lot I	Yes - the solution fully meets the requirement	Fiorano ESB and Fiorano API Management fully meet all the functional, technical, and operational requirements as outlined, including security, scalability, standards compliance, and ease of management.
	<p><b>Integration Capability:</b> The ESB must possess robust integration capabilities, enabling it to seamlessly connect with other IT systems within the NBM;</p>		Lot I	Yes - the solution fully meets the requirement	Fiorano ESB and Fiorano API Management fully meet all the functional, technical, and operational requirements as outlined, including security, scalability, standards compliance, and ease of management.
	<p><b>Standardized Approach:</b> Integration with other systems should adhere to standardized approaches and protocols to ensure compatibility and interoperability across different platforms and technologies;</p>		Lot I	Yes - the solution fully meets the requirement	Fiorano ESB and Fiorano API Management fully meet all the functional, technical, and operational requirements as outlined, including security, scalability, standards compliance, and ease of management.
	<p><b>Ease of Management:</b> The ESB should offer intuitive tools and interfaces for managing integration processes, allowing trained specialists to configure and manage integration workflows without requiring deep technical expertise;</p>		Lot I	Yes - the solution fully meets the requirement	Fiorano ESB and Fiorano API Management fully meet all the functional, technical, and operational requirements as outlined, including security, scalability, standards compliance, and ease of management.
	<p><b>Flexibility:</b> It should allow for flexible configuration and customization of integration processes to accommodate evolving business requirements and changing technological landscapes.</p>		Lot I	Yes - the solution fully meets the requirement	Fiorano ESB and Fiorano API Management fully meet all the functional, technical, and operational requirements as outlined, including security, scalability, standards compliance, and ease of management.
	<p><b>Scalability and Reliability:</b> The ESB must be scalable to handle increasing data volumes and transaction loads over time, while ensuring high availability and reliability to support critical business operations.</p>		Lot I	Yes - the solution fully meets the requirement	Fiorano ESB and Fiorano API Management fully meet all the functional, technical, and operational requirements as outlined, including security, scalability, standards compliance, and ease of management.
	<p><b>Monitoring and Alerting:</b> It should provide comprehensive monitoring capabilities to track the performance and health of integration processes, with the ability to generate alerts in case of any issues or deviations from predefined thresholds.</p>		Lot I	Yes - the solution fully meets the requirement	Fiorano ESB and Fiorano API Management fully meet all the functional, technical, and operational requirements as outlined, including security, scalability, standards compliance, and ease of management.
	<p><b>Interoperability Standards:</b> The ESB must adhere to industry-standard interoperability protocols and specifications to enable seamless communication and data exchange with external systems and services. The ESB must support open interoperability standards such as WSDL, WS-*, XML, REST, SOAP, UDDI, HTTPS etc. to facilitate seamless communication and data exchange with external applications and services.</p>		Lot I	Yes - the solution fully meets the requirement	Fiorano ESB and Fiorano API Management fully meet all the functional, technical, and operational requirements as outlined, including security, scalability, standards compliance, and ease of management.
	<p><b>Security:</b> Robust security mechanisms should be in place to ensure the confidentiality, integrity, and authenticity of data exchanged through the ESB, including encryption, authentication, and access control measures. <i>Please provide detailed description and documentation outlining the ESB's core features.</i></p>		Lot I	Yes - the solution fully meets the requirement	Fiorano ESB and Fiorano API Management fully meet all the functional, technical, and operational requirements as outlined, including security, scalability, standards compliance, and ease of management.

CNF.62	The ESB should support service orchestration capabilities to enable the coordination and automation of complex business processes and workflows spanning multiple systems and services. Workflow modeling tools and visual editors should be provided to design, simulate, and execute business processes and service compositions.	Mandatory	Lot I	Yes - the solution fully meets the requirement	<p>Fiorano ESB includes advanced service orchestration capabilities through its Fiorano Orchestration Studio, a drag-and-drop visual editor that allows users to:</p> <ul style="list-style-type: none"> <li>Design integration and business workflows visually</li> <li>Model end-to-end service compositions</li> <li>Simulate message flows before deployment</li> <li>Define conditional logic, transformation, branching, retries, and error handling</li> <li>Integrate human tasks into workflows if needed</li> <li>Deploy workflows directly from the design tool with minimal code</li> </ul> <p>These features enable both technical and functional users to rapidly build and maintain cross-system business processes.</p> <p>Link to Fiorano ESB key features &amp; online documentation - <a href="https://docs.fiorano.com/esb/13.2/key-features">https://docs.fiorano.com/esb/13.2/key-features</a></p>
CNF.63	Modeling / managing rules at the process level must be done in an intuitive way (using tools and visual forms). Thus, the management of the rules at process level must be possible to be performed directly by the trained specialists.	Mandatory	Lot I	Yes - the solution fully meets the requirement	<p>Fiorano ESB provides an intuitive, graphical development environment (Fiorano Studio) where business rules and process conditions can be modeled directly within orchestration flows using:</p> <ul style="list-style-type: none"> <li>Drag-and-drop tools for process logic, branching, loops, and conditions</li> <li>Rule-based decision elements (e.g., If-Then-Else, switches, filters)</li> <li>Parameter configuration via forms (no coding required)</li> <li>Support for dynamic expressions and external rule inputs</li> <li>Real-time validation and simulation for rule testing before deployment</li> </ul> <p>This enables functional/business users (with training) to manage and modify business processes independently, improving agility and reducing reliance on developers for routine rule updates.</p>
CNF.64	The process-level modeling / management functionality must ensure that the effort required to change the rules, use templates, versioning and monitoring the implementation of process-level rules is minimized.	Mandatory	Lot I	Yes - the solution fully meets the requirement	<p>Fiorano ESB is designed to streamline rule and process management with the following key capabilities:</p> <ul style="list-style-type: none"> <li><b>Low-Effort Rule Changes:</b> Rules and logic can be modified through visual editors using simple forms and drag-and-drop components, eliminating the need for code-level changes.</li> <li><b>Template Reuse:</b> Reusable process templates can be created and applied across different workflows, reducing duplication and standardizing rule design.</li> <li><b>Version Control:</b> Fiorano includes built-in versioning and rollback for all integration flows and rule sets. Each deployment is version-tagged for easy auditability and change management.</li> <li><b>Monitoring and Audit Trails:</b> The platform provides detailed real-time monitoring of rule execution, outcomes, and process behavior via dashboards. It also logs all changes for traceability and supports alerting on deviations or failures.</li> </ul>

CNF.65	The ESB must provide functionality for monitoring processes and events. Monitoring system activities, processes and rules will ensure visibility on the correctness and integrity of data flows between different applicative systems.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Real-time dashboards, transaction tracking, audit logs, and flow-level monitoring.
CNF.66	The ESB must provide messaging-like functionality for managing alerts, messages, and other communications necessary for proper management of interoperability between solutions.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Messaging engine supports alerts, retry logic, exception notifications, and system messages.
CNF.67	The ESB's communications management module must allow the definition of system-level events and the attachment of a communication scenario to each event. Depending on the event, different types of messages will be generated, such as confirmation, alert, error, status change, monitoring, etc.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Event-driven architecture allows event-message mapping (e.g., alerts, confirmations).
CNF.68	Messages must be received and sent through inbound and outbound interfaces. Interfaces must provide capabilities for interpreting and manipulating messages such as: encoding and decoding, message validation schemes, grouping and disassembling messages, single-sign-on capabilities, encryption and decryption, application and validation of digital signatures, etc.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Built-in adapters for REST/SOAP/JMS/FTP, plus support for validation, encryption, SSO, and transformation.
CNF.69	The ESB's messaging subsystem must offer the possibility of integration with the Beneficiary's e-mail services.	Mandatory	Lot I	Yes - the solution fully meets the requirement	SMTP/IMAP connectors for sending messages, alerts, and exceptions via email.
CNF.70	The ESB should include performance optimization features such as message caching, content-based routing, message filtering, and load balancing to enhance throughput and minimize latency. It should support horizontal and vertical scaling strategies to distribute workloads across multiple nodes and optimize resource utilization.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Message caching, content-based routing, parallel processing, clustering, horizontal/vertical scaling.
CNF.71	The ESB should facilitate compliance with regulatory requirements, industry standards, and organizational policies related to data privacy, security, and governance. Please describe the supported features and capabilities aimed to ensure compliance with the requirement.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Fiorano ESB will not be storing any customer data, hence general regulatory compliance requirements are applicable.
CNF.72	The ESB should support governance frameworks for managing service lifecycles, versioning, dependency management, and service-level agreements (SLAs).	Mandatory	Lot I	Yes - the solution fully meets the requirement	Features related to service lifecycles, versioning, dependency management, and service-level agreements (SLAs) are part of Fiorano eStudio. Details are available at <a href="https://docs.fiorano.com/esb/13.2/composing-event-processes">https://docs.fiorano.com/esb/13.2/composing-event-processes</a>
<b>1.3.2. Integration with other systems</b>					
CNF.73	The solution will be able to be easily integrated with the data bus component, Enterprise Service Bus (which will be delivered as part of the CBS solution from lot I), with native support for open integration standards according to the principles and concepts of Service Oriented Architecture (SOA) and Event Driven Architecture (EDA). Please describe the mechanisms supported by the solution for integration with ESB and with other systems. Please provide your vision on how to optimally approach the integration with the solution within the other lot and with the external systems requested as part of this tender procedure.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Fiorano defines a coarse-grained, event-driven model for Enterprise Services enabling each service to execute as an independent entity that is not tied into the context of execution until runtime, simplifying the componentization of existing Web Services, Database applications, Legacy, J2EE and .NET software assets, enhancing their reuse within event-driven business processes and automatically maximizing the parallelism within each business process.
CNF.74	The Tenderer must ensure interfacing with all the necessary interfaces through the integration component (Enterprise Service Bus).	Mandatory	Lot I	Yes - the solution fully meets the requirement	Fiorano ensures end-to-end integration through its ESB by enabling adapters, mediation, transformation, and orchestration flows for all required systems.


CNF.75	All application interfaces must be based on open standards. Exceptions may be "required interface" interfaces, which will be adapted to the specifics of the interfaces available on the NBM applications side.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Fiorano provides a powerful Business Component Development Kit (BCDK) to integrate with legacy systems or to meet a very specific business logic need which can't be efficiently met with the existing service palette. This framework provides APIs for service development in multiple languages including Java, C, C++ and C# (.NET), creating a true multi-language, multi-platform enterprise backbone.
CNF.76	All interfaces of the provided application will be able to interact with external applications both in real time and offline.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Supports both synchronous (real-time) and asynchronous (offline) communication models, including queue-based messaging, scheduled polling, and triggers.
CNF.77	The interfaces of the provided application will allow loose coupling with external applications (communication based on messages).	Mandatory	Lot I	Yes - the solution fully meets the requirement	Fiorano supports loosely coupled, message-based architecture via asynchronous messaging queues, topics, and event triggers.
CNF.78	The application will have standard interfaces for accessing all key business functions of the application (e.g. generating documents, generating transactions, accessing information about business entities stored within the application). The respective interfaces must allow the management of the business entities with the application of all the relevant business rules and with the use of all the characteristics related to the business entities.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Business functions can be exposed as secure, reusable services via the ESB. Supports rule enforcement through workflow orchestration and service governance.
CNF.79	The application will have standard interfaces for data export within Data Warehouse tools.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Yes, Fiorano Event processes can be built to process ETL.
CNF.80	The solution will have convenient tools for the administrator to manage, control and monitor all external interfaces of the application.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Fiorano Studio and Dashboard provide visual tools for monitoring, flow control, error tracking, and administrative functions.
CNF.81	All application interfaces must be properly documented (e.g. with the Web Services Description Language application).	Mandatory	Lot I	Yes - the solution fully meets the requirement	Yes, WSDL and WADL are available for documenting interfaces for both webservice and REST services.
CNF.82	The application will be able to create email messages according to predefined forms and send them to the recipients indicated via the e-mail server set in the application configurations.	Mandatory	Lot I	Yes - the solution fully meets the requirement	HTML based forms can be built within Fiorano mapper tools for email message format.
<b>1.4. Requirements for performance</b>					
CNF.83	The application must efficiently process transactions performed by the NBM in accordance with the volumes and nature of NBM activity, meeting established performance requirements.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE and Oracle Banking Product Processor are built to handle high-volume, mission-critical transaction processing environments typical of central banking operations. The solution is architected on a high-performance, scalable platform that supports multi-threaded processing, database optimization techniques (such as partitioning and indexing), and asynchronous job handling to ensure throughput and responsiveness. Performance tuning parameters can be adjusted to meet NBM-specific transaction volumes, and the solution has been benchmarked in large-scale deployments across global financial institutions to meet stringent SLAs for response time, batch processing, and concurrent user loads.
<b>1.4.1. General performance requirements</b>					
CNF.84	The concurrent running of the internal processes of the application will not have an impact on the overall performance of the application. Otherwise, the Tenderer will include in the application administration and operation guides information on the processes that may impact the performance of the application and its recommendations on the concurrent running of these processes (e.g. it is not recommended to run the process X to generate daily reports, simultaneously with the process Y to re-evaluate the securities).	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE and Oracle Banking Product Processor are designed to support concurrent execution of internal processes without degrading overall system performance. The solution uses a robust job scheduling and process orchestration framework that prioritizes critical transactions and optimizes resource utilization. For processes with high compute or I/O demands—such as EOD, report generation, or revaluation

CNF.85	Generating reports and accessing information for business analysis purposes must not affect the operational performance of the application in terms of transaction processing. Otherwise, in the application documentation will be identified the reports with significant impact on performance and formulated the recommendations of the selected Tenderer on the generation of those reports, so as not to impact the performance property of the application.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE and Oracle Banking Product Processor are designed with architectural separation between transactional and analytical workloads to ensure that business reporting does not interfere with core transaction processing. Standard reports are generated using optimized SQL queries and scheduled batch jobs that can be configured to run during off-peak hours. For resource-intensive or ad hoc reports, Oracle provides guidelines in the product documentation identifying such reports and offering best practices—such as using read-only replicas, dedicated reporting schemas, or materialized views—to isolate reporting workloads. These recommendations help maintain optimal transaction performance while enabling robust business analysis.
CNF.86	The solution must retain all transactional and historical data for a minimum period of five years without compromising its performance.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE ensures five-year data retention through optimized archiving, partitioning, and indexing. OBDX accesses historical data seamlessly, while Fiorano ESB enables efficient data retrieval and integration without impacting system performance.
CNF.87	Tenderers must specify minimum guaranteed performance values for the application, considering the recommended technological platform.	Mandatory	Lot I	Yes - the solution fully meets the requirement	<p>Oracle FLEXCUBE and Oracle Banking Product Processor, when deployed on a recommended enterprise-grade technological platform (e.g. Oracle Database 19c, WebLogic Application Server, Linux/Unix OS on x86 architecture), can guarantee the following minimum performance benchmarks under normal load conditions:</p> <ul style="list-style-type: none"> <li>* Transaction response time: ≤ 2 seconds for 95% of online transactions</li> <li>* Batch processing throughput: ≥ 100,000 records per hour for standard end-of-day processes</li> <li>* Concurrent user support: ≥ 500 simultaneous users without performance degradation</li> <li>* Report generation time: ≤ 5 seconds for standard reports with typical data volume</li> <li>* System uptime: ≥ 99.7% availability, aligned with High Availability configuration</li> </ul> <p>These values are indicative and will be validated and tuned based on the final infrastructure sizing, actual transaction volumes, and integration landscape defined by NBM. Detailed performance tuning and SLA commitments will be outlined in the technical design and deployment plan.</p>
<b>1.4.2. Specific performance requirements</b>					
CNF.88	<p>The average response time for standard online transactions performed via the graphical interface by users or external services (e.g., balance inquiries, payment authorization and processing, recent transaction consultations, and account-related operations) must not exceed 2 seconds in at least 95% of cases, measured under normal operating conditions. This excludes periods when batch processes (such as EOD/EOM/EOY) are running or when complex reports are being generated.</p> <p><i>The Tenderer shall present the technical solutions adopted to meet this requirement, and compliance will be validated through specific tests agreed upon between the Tenderer and the Beneficiary.</i></p>	Mandatory	Lot I	Yes - the solution fully meets the requirement	<p>Oracle FLEXCUBE and Oracle Banking Product Processor are engineered to deliver sub-2 second response times for standard online transactions under normal operating conditions, meeting the required 95% performance threshold. This is achieved through several key architectural and technical measures:</p> <ol style="list-style-type: none"> <li>1. Optimized Application Code and Queries— Core online transactions like balance inquiry, payments, and transaction lookups are handled using pre-compiled PL/SQL packages and parameterized queries to minimize database round-trips and reduce execution time.</li> <li>2. In-Memory Caching and Connection Pooling— Frequently accessed static data is cached, and application servers use connection pooling to maintain low-latency DB access.</li> <li>3. Horizontal and Vertical Scalability— The application supports load balancing across multiple app server instances, and can scale vertically with multi-threaded processing on modern x86 systems.</li> </ol>
CNF.89	The application will have the ability to process transactions both in real time and batch.	Mandatory	Lot I	Yes - the solution fully meets the requirement	The solution supports both real-time and batch transaction processing through configurable processing frameworks, enabling immediate transaction execution alongside scheduled bulk operations, ensuring scalability, operational efficiency, and consistent performance across all banking services.
<b>1.5. Requirements for flexibility</b>					
CNF.90	The application must possess the capability to adapt to evolving business needs over time.	Mandatory	Lot I	Yes - the solution fully meets the requirement	The solution is designed with a modular, configurable, and extensible architecture, enabling easy adaptation to evolving business needs through parameterization, scalable components, and seamless integration with new functionalities and external systems.

CNF.91	<p>It is preferable that the adaptation in time to the new business needs be possible through configuration adjustments in the application (versus changes in the code), thus minimizing the adjustment costs on the NBM side.</p> <p><i>Please provide tangible evidence and examples highlighting the application's configuration options and flexibility for configuration-based adaptations.</i></p>	Recommended	Lot I	Yes - the solution fully meets the requirement	<p>Oracle FLEXCUBE and Oracle Banking Product Processor are designed with a high degree of configurability, enabling adaptation to new business requirements through parameter-driven setups rather than code-level changes. This flexibility reduces the total cost of ownership and enhances agility in responding to regulatory, product, or process changes together with ODT and extensibility provide low code no code approach to accomodation evolving needs.</p> <p>Examples of configuration-based adaptability include:</p>
CNF.92	The application will allow the customization of user views and forms. Also, the application will allow the creation of new user forms for accessing the business logic of the application.	Mandatory	Lot I	Yes - the solution fully meets the requirement	<p>Oracle FLEXCUBE offers comprehensive capabilities for customizing user views and creating new forms through its **Oracle Development Tool (ODT)** and extensibility framework. ODT enables banks like NBM to tailor UI components without altering the core product code. Users can modify existing screens to adjust field behavior (visibility, validation, mandatory status), re-label UI elements, and add new fields—all via metadata-driven configurations.</p> <p>For more advanced customization, new forms can be created using the extensibility framework provided by FLEXCUBE. These new forms can be linked to existing business logic or invoke custom business components developed using the same extensibility standards. This approach ensures that enhancements remain upgrade-safe and maintainable.</p> <p>Additionally, user-specific views and access controls can be configured at the role level to ensure that each user group interacts with screens relevant to their function. These capabilities significantly reduce development effort, promote agility, and align well with NBM's need for flexible, configuration-driven adaptations.</p>
CNF.93	The application will allow the customization of existing reports (e.g. data set adjustment, formatting).	Mandatory	Lot I	Yes - the solution fully meets the requirement	The solution provides all the data that is needed by Oracle Analytics Server for any report generaion
CNF.94	The application will allow the definition of user reports (e.g. definition of data set, report format, definition of calculated fields).	Mandatory	Lot I	Yes - the solution fully meets the requirement	It can be done together with Oracle Analytic Server
CNF.95	The application should offer configuration options for automatically generating reports triggered by specific events or scheduled intervals. The generated reports can be stored in the application or sent to the email addresses and / or set users.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle Analytic Server provides these capabilities
CNF.96	The application will allow to define and customize the business entities stored in the application (e.g. defining new properties).	Recommended	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE allows defining and customizing business entities using its extensibility framework and Oracle Development Tool (ODT). New properties can be added to entities through metadata-driven configurations at the UI, database, and service levels—without modifying core code—ensuring upgrade safety and flexibility.
CNF.97	The application will allow to define and customize the business rules implemented within the application.	Recommended	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE allows defining and customizing business entities using its extensibility framework and Oracle Development Tool (ODT). New properties can be added to entities through metadata-driven configurations at the UI, database, and service levels—without modifying core code—ensuring upgrade safety and flexibility.
CNF.98	The application will allow to define and customize business flows (e.g. consecutive operations, status transformations for the characteristics of business entities, documents and records generated, notifications, roles involved and allowed operations, etc.).	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE allows defining and customizing business entities using its extensibility framework and Oracle Development Tool (ODT). New properties can be added to entities through metadata-driven configurations at the UI, database, and service levels—without modifying core code—ensuring upgrade safety and flexibility.
CNF.99	The application will allow to define and manage the normative reference information used within the application. The data source for the reference information can be internal or external (e.g. external database, external web service, external file).	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE allows defining and managing reference information through centralized parameter tables and master data setups. It supports integration with external sources such as databases, web services, or flat files to fetch or synchronize reference data using standard adapters and APIs. This enables seamless management of normative data from both internal and external systems.

CNF.100	The application will allow to define and customize the external interfaces of the application (e.g. setting accessible business functions, setting the format for input / output data, setting communication protocols, settings for access control, etc.).	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE allows defining and managing reference information through centralized parameter tables and master data setups. It supports integration with external sources such as databases, web services, or flat files to fetch or synchronize reference data using standard adapters and APIs. This enables seamless management of normative data from both internal and external systems.
CNF.101	All application configurations must be able to be performed in convenient user interfaces for application administrators.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE allows defining and managing reference information through centralized parameter tables and master data setups. It supports integration with external sources such as databases, web services, or flat files to fetch or synchronize reference data using standard adapters and APIs. This enables seamless management of normative data from both internal and external systems.
CNF.102	The application must allow the development of new components by the NBM, based on the methodology and rules provided by the selected Tenderer. These components will have access to the functions and public properties of the application components, including the ability to inherit existing functions.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE supports the development of new components by clients like NBM through its extensibility framework and published APIs. The framework allows custom components to access public functions and properties of existing application components, and supports inheritance and reuse of standard logic. Oracle provides methodology, guidelines, and tools (like ODT) to ensure custom developments remain upgrade-safe and fully integrated.
CNF.103	The development, maintenance, and extension of the solution shall not be subject to commercial or technical restrictions that would limit NBM's ability to conduct internal developments or outsource development to third parties, provided that the explicitly defined methodological and technical framework established by the Tenderer is strictly followed.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE and Oracle Banking Product Processor support an open extensibility framework that allows NBM or any qualified third-party developer to build, maintain, or extend application components without hidden commercial or technical restrictions, provided they follow the published methodology and toolset. Oracle supplies detailed developer guides that cover software development lifecycle steps, coding and naming conventions, architectural principles, interface standards, security policies, test harness requirements, and continuous integration procedures, all of which are aligned with industry best practices and fully documented in the Oracle Development Tool (ODT) and FLEXCUBE Extensibility Framework manuals. These materials include guidance on using metadata-driven configurations, user exits, event hooks, and API consumption, ensuring new code remains upgrade-safe and interoperable with the core system. Licensing for custom extensions is limited to standard development and runtime licenses already included in the enterprise agreement; there is no mandatory Oracle involvement or proprietary approval process. As long as NBM or its chosen partners adhere to the supplied guidelines, they can independently develop and deploy new modules, interfaces, or UI screens, integrate them via standard APIs, and promote them through established testing and release pipelines without any vendor-imposed constraints.
	To this end, the Tenderer shall detail and provide the complete methodology and mandatory rules applicable to future developments, including the agreed software development methodology, mandatory coding/naming conventions, architectural principles, required integration and quality control procedures, as well as the tools and technical conditions necessary to ensure the seamless and efficient integration of new developments with the delivered application.				
	The provider shall not impose indirect conditions (such as special licensing, mandatory approvals, or the obligatory involvement of its own personnel) that would effectively restrict NBM's ability to carry out additional developments independently or in collaboration with third parties. All technical and methodological requirements must be sufficiently clear and transparent to ensure the quality, compatibility, and interoperability of all future developments.				
<b>1.6. Requirements for maintainability</b>					
CNF.104	The proposed solution must be designed to facilitate efficient maintenance, ensuring streamlined operations and minimizing complexity. It must adhere to the following essential criteria:	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE and Oracle Banking Product Processor are designed with modular, layered architecture that separates presentation, business logic, and data access layers, thereby simplifying maintenance and reducing complexity. The solution leverages metadata-driven configuration and parameterization, which allows many changes to be managed without altering core code. Standardized development practices, reuse of common components, centralized logging, automated diagnostics, and audit trails further enhance maintainability. The system supports hot deployment for certain configurations, built-in versioning of changes, and rollback capabilities to minimize downtime during updates. Oracle also provides detailed documentation, administrative tools, and health check utilities that support proactive monitoring and maintenance, ensuring efficient and reliable operations with minimal manual intervention.

CNF.104 a.	The solution must operate on a uniform technological platform, encompassing a single database management system to centralize data management and a unified hardware and software infrastructure to reduce compatibility issues and simplify maintenance;	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE is designed to run on a unified technology stack, using a single supported RDBMS like Oracle Database for centralized data management. It ensures consistency across environments by supporting a standardized software and hardware infrastructure, typically based on Linux or Windows Server on x86 platforms. This uniformity reduces compatibility risks and simplifies system administration and maintenance.
CNF.104 b.	All application modules within the proposed solution must be sourced from a single software supplier.	Mandatory	Lot I	Yes - the solution fully meets the requirement	All application modules are delivered as an integrated suite from a single vendor, ensuring unified architecture, consistent standards, simplified support, streamlined upgrades, and reduced integration complexity across the entire solution landscape.
CNF.104 c.	All application modules included in the solution must utilize a single development environment. This standardization simplifies development, testing, and deployment processes, reducing potential integration issues and improving maintainability.	Recommended	Lot I	Yes - the solution fully meets the requirement	All application modules leverage a unified development environment, ensuring consistent standards across development, testing, and deployment, thereby minimizing integration complexities, enhancing maintainability, and enabling efficient lifecycle management across the solution.
CNF.104 d.	The solution must incorporate robust mechanisms for identifying, tracking, and resolving operational issues. These mechanisms should include real-time monitoring tools, automated alerts for anomalies, and diagnostic tools for root cause analysis, ensuring minimal downtime and efficient issue resolution.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Observability is achieved through Oracle Enterprise Manager Console for monitoring and automating alerts regarding components of the solution
CNF.105	To ensure the application remains available and accessible to business users at the agreed service levels, it must support continuous monitoring and proactive maintenance. The solution must include the following capabilities:	Mandatory	Lot I	Yes - the solution fully meets the requirement	Once the system is in production , Incident management service is delivered based on agreed SLA
CNF.105 a.	<b>Proactive Problem Identification:</b> The application must enable early detection of potential issues across all components, minimizing downtime and operational disruptions.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Our Managed Service include intrinsically proactive issue identification and resolution
CNF.105 b.	<b>Preventive Maintenance:</b> The system should facilitate preventive measures to address identified risks, ensuring consistent performance and reliability (e.g. Automated Performance Threshold Alerts, Scheduled Data Cleanup and Archiving, Disk Space Monitoring and Preemptive Cleanup, Backup Verification etc.);	Mandatory	Lot I	Yes - the solution fully meets the requirement	As part of post-production services, Oracle FLEXCUBE implementations typically include preventive maintenance activities to ensure ongoing system health and reliability. These services involve configuring automated performance threshold alerts, setting up scheduled data purging and archival routines, monitoring disk space utilization with preemptive cleanup actions, and conducting regular backup verification and restore tests. System performance reviews and environment audits are also carried out periodically to proactively identify and mitigate risks, ensuring stable and consistent operations.
CNF.105 c.	<b>Comprehensive Monitoring:</b> Real-time monitoring tools must be provided to oversee the health, performance, and utilization of all application components, including infrastructure, business logic, and data layers;	Mandatory	Lot I	Yes - the solution fully meets the requirement	Observability is achieved through Oracle Enterprise Manager Console for monitoring and automating alerts regarding components of the solution
CNF.105 d.	<b>Ease of Maintenance:</b> Operational maintenance tasks must be streamlined, allowing administrators to quickly address performance bottlenecks, implement fixes, and perform routine updates with minimal effort;	Mandatory	Lot I	Yes - the solution fully meets the requirement	FLEXCUBE App -Oracle Enterprise Manager, FLEXCUBE Utilities, AppDynamics ESB - Oracle Enterprise Manager, OSB Console, ELK Stack Oracle DB -AWR/ASH, OEM Infra -Zabbix, Nagios, Prometheus
CNF.106	The solution must include monitoring mechanisms for key components, such as the business logic and data layers, to track operational load and performance levels. (e.g. business logic layer components, data layer).	Mandatory	Lot I	Yes - the solution fully meets the requirement	FLEXCUBE App -Oracle Enterprise Manager, FLEXCUBE Utilities, AppDynamics ESB - Oracle Enterprise Manager, OSB Console, ELK Stack Oracle DB -AWR/ASH, OEM Infra -Zabbix, Nagios, Prometheus
CNF.107	The solution must provide self-diagnostic tools for monitoring the status of internal components and generate appropriate notifications.	Mandatory	Lot I	Yes - the solution fully meets the requirement	The solution provides built-in self-diagnostic and monitoring capabilities, enabling real-time health checks of internal components, proactive issue detection, and automated alerts and notifications to support efficient operations and rapid incident resolution.
	Lot I		Notifications include contextual, actionable insights such as root cause indicators, impact analysis, and recommended remediation steps, enabling rapid issue resolution, reduced downtime, and improved operational efficiency across the system.		

CNF.108	All errors and exceptions encountered during application operation must be logged and managed in accordance with the defined "Exception Handling" requirements. This includes centralized logging, categorization of errors by severity, and automated escalation processes for critical issues.	Mandatory	Lot I	Yes - the solution fully meets the requirement	This is part of Ops , where tool used by the bank for incident management can be used.
CNF.109	The documentation provided with the application must also contain detailed technical documentation related to all components of the application, including: technical architecture of the application, installation guides, configuration and operational maintenance of all application components, guides for developers (within the components allowed for internal development on the NBM). The technical documentation must guide the NBM how to install, integrate and maintain operationally components developed by the NBM.	Mandatory	Lot I	Yes - the solution fully meets the requirement	This is fulfilled as part of deliverables generated at different stage of implementation
CNF.110	<p>The application architecture must enable the NBM to implement application-level changes with minimal complexity. The architecture should ensure that the scope of affected components is minimal and that impacted components are clearly identifiable for targeted testing and validation.</p> <p><i>The Tenderers must demonstrate alignment with this requirement by providing:</i></p> <ul style="list-style-type: none"> <li>- <i>A detailed description of the architectural design principles and methodologies employed to minimize the complexity of application-level changes.</i></li> <li>- <i>Examples of different categories of customizations supported by the solution, including scenarios involving integration, user interface updates, and data schema modifications.</i></li> <li>- <i>A functional prototype or simulation that demonstrates the complete process of customization, testing, and publishing/migration of a change. The prototype or simulation must highlight the tools, workflows, and mechanisms employed to identify, implement, and validate the changes.</i></li> </ul>	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE is built on modular, layered architecture and metadata-driven configuration, so most changes can be isolated to specific components and migrated with minimal impact. Design principles include separation of presentation, business logic, and data layers, parameter tables for product behaviour, user-exit hooks for point customisation, and service wrappers that expose integration points without altering core code; dependency tracking in the Oracle Development Tool clearly identifies which objects are affected by a change, allowing targeted unit and regression tests. Typical customisation categories include: adding a new REST endpoint that reuses existing business services while requiring only a service definition file and security mapping; updating the user interface through ODT by adding a new field and label to an existing form without touching backend logic; and extending the data schema by introducing a user-defined field stored in a FLEXCUBE extension table, automatically reflected in screens and reports via metadata. During implementation a sandbox environment, ODT workspace, and FLEXCUBE transport utilities are used to build the change, run automated validation scripts, and package the artefacts into a deployment bundle; migration to UAT and then production is performed with version-controlled patch files, and the impact report generated by the transport utility lists exactly which objects require retesting, demonstrating how the architecture supports low-complexity, traceable change management.
CNF.111	The application will allow to define and run scheduled tasks for operational maintenance activities (e.g. archiving historical data).	Mandatory	Lot I	Yes - the solution fully meets the requirement	The application supports configurable scheduling of maintenance tasks, including data archiving, cleanup, and batch jobs, enabling automated execution, efficient resource utilization, and consistent system performance without manual intervention.
CNF.112	The application architecture must support seamless implementation of new versions delivered by the supplier without disrupting existing customizations, NBM-implemented components, or interfaces with external applications.	Mandatory	Lot I	Yes - the solution fully meets the requirement	
CNF.113	To ensure continuity of support, there must be at least two alternative providers capable of delivering maintenance and development services for the provided application. At least one of these providers must be located in Western, Central, or Eastern Europe. Each provider must have a minimum of two certified specialists for the offered solution, and no specialist may be listed by more than one provider.	Mandatory	Lot I	Yes - the solution fully meets the requirement	The solution is supported by a multi-partner ecosystem, ensuring continuity through alternative qualified providers. At least one provider is Europe-based, each with certified specialists, with strict resource exclusivity maintained across providers.
CNF.114	The solution must be designed for easy portability from the production environment to other operating environments, such as testing and development environments and vice versa. The accompanying documentation must provide a step-by-step guide to the portability process, detailing all required configurations, dependencies, and procedures to ensure efficient and error-free transitions.	Mandatory	Lot I	Yes - the solution fully meets the requirement	The solution supports seamless portability across environments through standardized deployment frameworks, configuration management, and environment abstraction. Comprehensive documentation provides step-by-step guidance covering configurations, dependencies, and procedures to ensure consistent, error-free transitions.

CNF.115	The application must include mechanisms to generate automatic notifications to the software manufacturer in case of critical errors. These notifications must provide sufficient detail to enable rapid identification and resolution of root causes.	Recommended	Lot I	Yes - the solution fully meets the requirement	This is through Software manufacturer support portal where incident are logged.
<b>1.7. Requirements towards scalability</b>					
CNF.116	During the use of application, the number of transactions processed may increase or decrease significantly from one period to another. In order to have a rational use of processing resources, the application required by the NBM must be easily scalable (up and down).	Mandatory	Lot I	Yes - the solution fully meets the requirement	To ensure rational use of processing resources amid fluctuating transaction volumes, the proposed application—based on Oracle Flexcube and Oracle Banking Processors—is designed for seamless scalability. Leveraging Oracle WebLogic’s clustering and load balancing capabilities, the system can dynamically scale up or down based on demand. Oracle Database, with Real Application Clusters (RAC), ensures high availability and performance under varying loads. This architecture supports both horizontal and vertical scaling, enabling cost-effective resource utilization while maintaining operational efficiency and compliance.
CNF.117	The application will allow to increase the processing capacity without interrupting their operation. For this purpose, the application will support the horizontal expansion of the processing capacity (e.g. upgrading the hard infrastructure, adding new servers for the application servers and performing load balancing).	Mandatory	Lot I	Yes - the solution fully meets the requirement	The proposed application, built on Oracle Banking Product Processor’s microservices architecture, is designed to support horizontal scalability and uninterrupted operations. Each business capability is delivered as an independent microservice, allowing granular scaling of specific components based on transaction load.  The application runs on Oracle WebLogic and integrates with Oracle Database (RAC), enabling seamless addition of new servers and infrastructure upgrades. Through load balancing and clustering, workloads are distributed across multiple application nodes, ensuring high availability and fault tolerance.  Microservices also facilitate containerized deployment, allowing dynamic resource allocation and rapid scaling using orchestration tools like Kubernetes. This architecture ensures that processing capacity can be increased or decreased without downtime, supporting NBM’s need for rational and resilient resource utilization.
CNF.118	The application must include features for automatic load distribution and dynamic scaling of critical components. This capability must support both upward and downward scaling based on real-time demand and ensure optimal performance for latency-sensitive operations.	Recommended	Lot I	Yes - the solution fully meets the requirement	The application runs on Oracle WebLogic and integrates with Oracle Database (RAC), enabling seamless addition of new servers and infrastructure upgrades. Through load balancing and clustering, workloads are distributed across multiple application nodes, ensuring high availability and fault tolerance.
<b>1.8. Requirements for usability</b>					
CNF.119	The application must be designed with user-friendliness and intuitiveness as primary goals. Training time for end-users must be minimized through an intuitive interface and easy-to-understand workflows. Users should have access to comprehensive support information and guidance at all times to ensure correct usage	Mandatory	Lot I	Yes - the solution fully meets the requirement	The application delivers an intuitive, user-friendly interface with streamlined workflows, minimizing training effort. Embedded help, contextual guidance, and comprehensive support information ensure users can operate the system efficiently and accurately at all times.
CNF.120	All business functions accessible to application users must be accessed through graphical user interfaces.	Mandatory	Lot I	Yes - the solution fully meets the requirement	All business functions are accessible through intuitive graphical user interfaces, eliminating reliance on command-based operations, ensuring ease of use, consistency, and efficient user interaction across all modules and functionalities.
CNF.121	The application documentation must contain complete, detailed and updated guides for all user groups.	Mandatory	Lot I	Yes - the solution fully meets the requirement	The application provides comprehensive, up-to-date documentation for all user groups, including detailed user guides, administrative manuals, and technical references, ensuring clarity, effective usage, and efficient system management across all roles.
CNF.122	Application users will have access to context-sensitive help in all application interfaces.	Mandatory	Lot I	Yes - the solution fully meets the requirement	The application provides context-sensitive help across all interfaces, offering real-time guidance, tooltips, and relevant documentation links, enabling users to perform tasks accurately and efficiently without requiring external support or extensive training.

CNF.123	When defining and customizing reports, users must have access to the application's data dictionary to understand the data structures and relationships.	Mandatory	Lot I	Yes - the solution fully meets the requirement	The application provides access to a comprehensive data dictionary, enabling users to understand data structures, relationships, and metadata, thereby supporting accurate report definition, customization, and efficient data analysis across the system.
CNF.124	Users must be able to access all authorized functions through a unified graphical interface, ensuring streamlined navigation and task execution.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Users access all authorized functions through a unified graphical interface, ensuring consistent navigation, role-based access, and streamlined task execution, thereby enhancing usability, productivity, and overall user experience across the application.
CNF.125	The application must feature user interfaces that are intuitive, visually appealing, and ergonomically designed for both business users and administrative roles.	Mandatory	Lot I	Yes - the solution fully meets the requirement	The application delivers intuitive, visually appealing, and ergonomically designed user interfaces tailored for both business and administrative users, ensuring ease of use, reduced training effort, and efficient task execution across all functions.
CNF.126	The application must allow users to save their work and operations mid-process, either automatically or upon user request, to prevent data loss and facilitate task continuity.	Mandatory	Lot I	Partially yes - The solution partially meets the requirement	The application supports automatic and user-initiated save functionality, enabling users to preserve work in progress, prevent data loss, and seamlessly resume operations, ensuring continuity and improved user productivity.
CNF.127	All user interfaces must be in Romanian and English languages.	Mandatory	Lot I	Yes - the solution fully meets the requirement	The application supports multilingual user interfaces, including Romanian and English, enabling users to switch languages seamlessly, ensuring accessibility, usability, and consistent user experience across all functions and user roles.
CNF.128	The translation must ensure uniform use of specific terms used in the application (e.g. Delete = Eliminare) across all interfaces.	Mandatory	Lot I	Yes - the solution fully meets the requirement	The application ensures consistent terminology across all interfaces through centralized language management, enforcing standardized translations (e.g., "Delete = Eliminare") to maintain uniformity, clarity, and a coherent user experience across modules.
CNF.129	User interfaces must follow a consistent graphical design style, with uniform use of graphical elements and text across the application to enhance usability and reduce cognitive load for users.	Mandatory	Lot I	Yes - the solution fully meets the requirement	The application enforces a consistent UI design framework with standardized layouts, graphical elements, and terminology, ensuring uniform user experience, reduced cognitive load, improved usability, and efficient navigation across all modules and interfaces.
CNF.130	The application must allow users to customize their workspace, including features such as adding menu items to favorites, displaying recent accesses, and saving parameterized searches.	Recommended	Lot I	Yes - the solution fully meets the requirement	The application enables workspace personalization, allowing users to configure favorites, access recent activities, and save parameterized searches, thereby enhancing efficiency, usability, and tailored user experience aligned with individual operational preferences.
CNF.131	The user interfaces will allow simple navigation through the application forms, by using complementary mechanisms (e.g. mouse and / or keyboard and / or special functions).	Mandatory	Lot I	Yes - the solution fully meets the requirement	The application supports intuitive navigation through multiple interaction methods, including mouse, keyboard shortcuts, and functional controls, ensuring efficient form access, improved usability, and enhanced user productivity across all application interfaces.
CNF.132	The application must generate notifications to alert users about actions that require their attention, such as transaction authorizations or pending approvals.	Mandatory	Lot I	Yes - the solution fully meets the requirement	The application generates real-time notifications and alerts for user actions requiring attention, including transaction authorizations and pending approvals, ensuring timely response, improved control, and efficient workflow management across the system.
CNF.133	Notifications generated by the application must include actionable information, such as direct links or automatic opening of relevant forms, to expedite user actions.	Mandatory	Lot I	Partially yes - The solution partially meets the requirement	Notifications include actionable elements such as direct links and auto-navigation to relevant screens, enabling users to quickly access pending tasks, expedite decision-making, and improve overall operational efficiency and responsiveness.
CNF.134	The application must provide a centralized dashboard to display all user-specific actions and tasks requiring attention, offering a holistic view for efficient task management.	Mandatory	Lot I	Partially yes - The solution partially meets the requirement	The application provides a centralized, role-based dashboard displaying all user-specific tasks, alerts, and pending actions, delivering a holistic view that enables efficient monitoring, prioritization, and streamlined task management.
<b>1.9. Requirements for information security</b>					
CNF.135	The proposed application must include robust controls to manage and mitigate information security risks inherent to its use. Security measures must align with NBM-approved security policies and industry standards, ensuring comprehensive prevention, detection, and response capabilities for a broad spectrum of security threats.	Mandatory	Lot I	Yes - the solution fully meets the requirement	The application incorporates robust security controls aligned with regulatory and industry standards, enabling prevention, detection, and response to threats through access controls, encryption, monitoring, and compliance with approved security policies.
	The application must employ a multi-layered security architecture that integrates seamlessly into the NBM's information security management framework, which is based on the ISO 27000 family of standards. This layered approach must address security at the application, network, and infrastructure levels.				Multi-Layered Security Architecture Aligned with ISO 27000  The proposed application employs a multi-layered security architecture that integrates seamlessly into NBM's Information Security Management Framework, based on the ISO 27000 family of standards. Leveraging the capabilities of Oracle Banking Product Processor's microservices architecture, the solution ensures security across all layers:

CNF.136	Please provide detailed description outlining the security architecture of the proposed application, highlighting how different security layers are integrated into the application to protect against unauthorized access, data breaches, and other security risks. If possible, please submit a detailed checklist, or matrix outlining how each security requirement specified in the ISO 27000 standards is addressed and implemented within the proposed application.	Mandatory	Lot I	Yes - the solution fully meets the requirement	- Application Layer: Implements role-based access control (RBAC), secure APIs, data encryption, and audit logging to protect sensitive operations and customer data. - Network Layer: Utilizes secure communication protocols (TLS/SSL), firewalls, intrusion detection/prevention systems (IDS/IPS), and network segmentation to safeguard data in transit. - Infrastructure Layer: Deployed on hardened servers with patch management, endpoint protection, and virtualization/container security. Integration with Oracle WebLogic and Oracle DB ensures secure session management and data integrity.
CNF.137	The security subsystem of the proposed solution must achieve the following critical objectives: - <b>Confidentiality, Integrity, and Authenticity</b> : Ensuring that information remains secure during processing, storage, or transmission, and maintaining non-repudiation for transmitted data. - <b>Access Control</b> : Preventing unauthorized access to data and providing fine-grained access controls for system resources. - <b>Role-Based Access</b> : Enabling differentiated access levels (viewing, printing, copying, modifying, etc.) based on user roles. - <b>Critical Activity Monitoring</b> : Logging and monitoring of critical system-level activities with real-time alerts for anomalies. - <b>Data Protection</b> : Preventing the loss, unauthorized modification, or misuse of information stored or processed within the application.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Confidentiality, Integrity, and Authenticity: Data is encrypted during transmission and at rest using industry-standard protocols (e.g., TLS, AES). Digital signatures and secure APIs ensure authenticity and non-repudiation. Access Control: Fine-grained access controls are enforced at both the application and service levels, preventing unauthorized access to sensitive data and system resources. Role-Based Access: The system supports differentiated access levels (view, modify, print, copy, etc.) based on user roles, ensuring that users interact only with data and functions relevant to their responsibilities. Critical Activity Monitoring: All critical system-level activities are logged and monitored in real time. Integrated alerting mechanisms notify administrators of anomalies or potential security breaches. Data Protection: Robust data protection mechanisms prevent unauthorized modification, loss, or misuse of information. This includes backup and recovery strategies, secure storage, and audit trails.
<b>1.9.1. Security architecture</b>					
CNF.138	The application architecture must be developed using a "Secure by Design" methodology. This approach ensures that security considerations are integrated at every stage of the development lifecycle, minimizing vulnerabilities and enhancing resilience against threats.	Mandatory	Lot I	Yes - the solution fully meets the requirement	The application follows a "Secure by Design" approach, embedding security across the development lifecycle, including secure coding, vulnerability management, and continuous testing, ensuring minimized risks and enhanced resilience against evolving threats.
CNF.139	The security architecture of the application must be thoroughly documented. This documentation should provide a clear and comprehensive explanation of the implemented security model, its components, and the interrelations between them.	Mandatory	Lot I	Yes - the solution fully meets the requirement	The application provides comprehensive security architecture documentation, detailing the security model, components, controls, and their interrelationships, ensuring transparency, auditability, and clear understanding of the implemented security framework.
	The documentation must explicitly describe the security model, outlining the purpose and role of each security component in protecting the system. This includes mechanisms for authentication, authorization, encryption, auditing, and intrusion detection.		Lot I		The documentation clearly defines the security model, detailing roles of authentication, authorization, encryption, auditing, and intrusion detection components, ensuring comprehensive understanding of how each control protects the system and enforces security policies.
CNF.140	The application documentation will contain the specifications regarding the network placement of the application components and the recommendations of the selected Tenderer regarding the network access rules necessary to be set by the NBM for secure access to all application components (e.g. communication matrix between services).	Mandatory	Lot I	Yes - the solution fully meets the requirement	The documentation specifies network placement of all components and provides recommended access rules, including detailed communication matrices, ensuring secure connectivity, controlled interactions between services, and alignment with institutional network security requirements.
CNF.141	All system processes related to the application components must adhere to the principle of least privilege, running only with the minimum access rights necessary to perform their tasks.	Mandatory	Lot I	Yes - the solution fully meets the requirement	All application processes operate under the principle of least privilege, with strictly defined access rights, ensuring components execute only necessary functions, thereby minimizing security risks and preventing unauthorized access or misuse.
CNF.142	All access credentials used by the application must be fully configurable through administrative interfaces. The application must not include any hard-coded credentials in its code or configuration files.	Mandatory	Lot I	Yes - the solution fully meets the requirement	All access credentials are centrally managed and fully configurable via administrative interfaces, with no hard-coded credentials in code or configuration, ensuring secure credential management, flexibility, and compliance with security best practices.

CNF.143	The application must prevent the storage of open access credentials in its components, including databases, configuration files, or logs. All sensitive credentials must be securely encrypted and managed using established security practices.	Mandatory	Lot I	Yes - the solution fully meets the requirement	The application enforces secure credential management by preventing storage of plaintext credentials, ensuring all sensitive data is encrypted, securely stored, and handled in accordance with established security standards and best practices.
CNF.144	The application must offer the possibility to flexibly configure its policies regarding the flows of electronic documents and ensure the legal requirements regarding the electronic documents, by offering a mechanism of application / verification of the advanced qualified electronic signature, in accordance with the applicable legislation of the Republic of Moldova.	Mandatory	Lot I	No - the solution does not meet the requirement	
CNF.145	All external interfaces of the application will be accessed with the application of secure authentication methods (e.g. X.509 certificates).	Mandatory	Lot I	Yes - the solution fully meets the requirement	All external interfaces are secured using strong authentication mechanisms, including X.509 certificates, ensuring trusted system-to-system communication, enhanced access control, and protection against unauthorized access and security threats.
<b>1.9.2. Identification and Authentication Requirements</b>					
CNF.146	The application must integrate with the centralized authentication mechanism of the NBM, based on Microsoft Active Directory, using the LDAP protocol. It must support the following features: - Importing user profiles and attributes (e.g., ID, name, surname, email) from the directory service. - Allowing administrators to select users from the directory service when creating new accounts.	Mandatory	Lot I	Yes - the solution fully meets the requirement	The application integrates with centralized authentication via LDAP/Active Directory, enabling user profile import and synchronization, while allowing administrators to select and provision users directly from the directory during account creation.
CNF.147	The application must support multifactor authentication (MFA) for user access.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE supports multi-factor authentication through integration with enterprise authentication systems, enabling configurable methods such as OTP and tokens, thereby enhancing user access security and ensuring compliance with regulatory and institutional requirements.
CNF.148	Passwords must be securely stored within the application using industry-standard encryption and protection techniques to prevent interception, deduction, or recovery.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE securely stores passwords using industry-standard hashing and encryption mechanisms, preventing plaintext storage and protecting against interception, reverse engineering, or unauthorized recovery, in line with established security best practices.
CNF.149	The application must support the enforcement of password usage policies, either through integration with the centralized NBM authentication system or independently for non-integrated users. This includes:	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE enforces comprehensive password policies either via Active Directory integration or natively, including complexity rules, expiration, reuse prevention, failed attempt limits, restricted password lists, and user notifications for password expiry.
	- Password complexity requirements.		Lot I		
	- Mandatory password changes and expiration policies.		Lot I		
	- Prevention of password reuse.		Lot I		
	- Configurable limits for failed authentication attempts.		Lot I		
	- A dictionary of forbidden passwords.		Lot I		
- User notifications regarding password expiration.	Lot I				
CNF.150	The application must allow administrators to configure differentiated password policies for specific user groups.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE enables administrators to define differentiated password policies for specific user groups, supporting granular control over complexity, expiration, reuse, and lockout rules based on roles and security requirements.
CNF.151	For users not integrated with the centralized authentication mechanism, the application must:	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE supports local user management for non-integrated users, enabling password changes through the user interface and allowing administrators to block, deactivate, or suspend user accounts at the application level.
	- Allow password changes via the user interface.		Lot I		
	- Support blocking, deactivating, or suspending user accounts at the application level.		Lot I		
	The application must provide session management controls, including:		Lot I		

CNF.152	- Configuring the maximum number of simultaneous sessions per user.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE provides robust session management controls, including configurable concurrent session limits, inactivity-based session timeouts, and security mechanisms to prevent unauthorized access and ensure protection of active user sessions.
	- Setting session expiration times for inactivity.		Lot I		
	- Mechanisms to prevent unauthorized access to active sessions.		Lot I		
CNF.153	The solution must support integration with internal IAM systems using internationally recognized open-standard protocols such as SAML 2.0, OAuth 2.0, and LDAP. It must enable the implementation of modern MFA methods, including but not limited to user credentials and passwords, digital certificates (X.509), dynamic one-time passwords (OTP/TOTP), hardware/software tokens, and other equivalent secure authentication methods.	Mandatory	Lot I	Yes - the solution fully meets the requirement	The proposed solution, built on Oracle Banking Product Processor and Oracle FLEXCUBE, supports integration with internal Identity and Access Management (IAM) systems using internationally recognized open-standard protocols, including:  SAML 2.0 for federated identity and single sign-on (SSO) OAuth 2.0 for secure delegated access LDAP for centralized user directory and authentication The system also enables implementation of modern Multi-Factor Authentication (MFA) methods, including:  User credentials and passwords X.509 digital certificates Dynamic OTP/TOTP Hardware/software tokens Other secure authentication mechanisms Additionally, the solution explicitly supports integration with Mpass (mpass.gov.md)—the national authentication and qualified electronic signature service—using the SAML 2.0 protocol. This ensures compliance with national digital identity standards and enhances trust and security
	Additionally, the solution must explicitly support (at implementation) integration with the national authentication and qualified electronic signature service (Mpass – mpass.gov.md) using the SAML 2.0 protocol.		Lot I		
	<i>The Tenderer shall provide a detailed description of the proposed technical solution, ensuring that authentication mechanisms can be extended and adapted in the future to meet BNM's internal requirements and align with the evolution of international technologies and standards in this domain.</i>		Lot I		
CNF.154	The application must support Single Sign-On (SSO) mechanisms using Kerberos.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE and Oracle Banking Product Processor can be integrated with Kerberos-based authentication through Oracle WebLogic Server, which supports SPNEGO (Simple and Protected GSSAPI Negotiation Mechanism)—a key protocol for enabling Kerberos SSO in web applications
<b>1.9.3. Authorization</b>					
CNF.155	The application must provide granular management of access rights for all application objects and associated operations. This includes managing rights for business entities, their properties, forms, menus, reports, and CRUD operations (Create, Read, Update, Delete).	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE provides granular, role-based access control, enabling administrators to manage permissions across business entities, attributes, forms, menus, reports, and CRUD operations, ensuring secure and controlled user access throughout the application.
CNF.156	The authorization model must follow the principle of "default deny," meaning all actions are prohibited unless explicitly permitted.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE enforces a "default deny" authorization model, where all actions are restricted unless explicitly permitted, ensuring strict access control, enhanced security, and prevention of unauthorized operations across the application.
CNF.157	The application must support the creation of user groups and roles and the assignment of users to these groups and roles.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE supports creation of user groups and roles, enabling administrators to assign users accordingly, ensuring structured access control, simplified user management, and alignment with organizational roles and responsibilities.
CNF.158	The application must allow:	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE supports flexible access control by enabling permissions at user, group, and role levels, allowing hierarchical group structures, and supporting multiple role/group associations with cumulative access rights across assignments.
	- Granting access rights at the level of individual users, user groups, and roles.		Lot I		
	- Defining groups that can include subgroups or roles.		Lot I		
	- Associating a user with multiple groups and roles, with cumulative access rights derived from all associations.		Lot I		
CNF.159	The application will allow granting access rights based on business rules (e.g. modifying the document only if the user is the author, or if the operation is done within a certain time frame).	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE supports rule-based access control, enabling permissions based on business conditions such as user ownership, transaction context, and time-based criteria, ensuring dynamic, context-aware authorization aligned with business policies.
CNF.160	The application will allow the temporary delegation of the rights held by one user to another user. The delegation may be made by keeping or suspending the rights held by the user to whom the rights are delegated.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE supports temporary delegation of user rights, allowing controlled transfer of permissions to another user, with options to retain or suspend the original user's rights, ensuring continuity and controlled access management.
CNF.161	The application should support segregation of administrative duties, such as requiring one administrator to modify settings and another to confirm the changes.	Recommended	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE supports segregation of duties through maker-checker controls, requiring one administrator to initiate changes and another to authorize them, ensuring governance, accountability, and prevention of unauthorized or unverified configuration updates.

CNF.162	<p>The application must provide views and reports on existing access rights. These reports should be customizable at least based on the following parameters:</p> <ul style="list-style-type: none"> <li>- User Information: <ul style="list-style-type: none"> <li>o Individual user ID.</li> <li>o User group(s) or role(s) assigned to the user.</li> <li>o Current status of the user (e.g., active, suspended, deactivated).</li> <li>o The date and time when the user was granted access to specific resources or operations.</li> <li>o History of access rights changes for the user, including timestamps and the administrators who made the changes.</li> </ul> </li> <li>- Access Rights Context: <ul style="list-style-type: none"> <li>o Business entities to which access has been granted.</li> <li>o Properties of the business entities for which access is allowed.</li> <li>o The specific operations allowed (e.g., create, read, update, delete).</li> </ul> </li> <li>- Advanced Options: <ul style="list-style-type: none"> <li>o Access rights granted by specific administrators or based on defined business rules.</li> <li>o Resources or operations assigned to groups or roles but not directly to individual users. <ul style="list-style-type: none"> <li>o Delegation records, specifying delegated access rights, delegating users, recipients, and the duration of delegation.</li> </ul> </li> <li>o Inactive or expired access rights, including reasons for revocation or expiration (e.g., policy change, role reassignment).</li> <li>o Anomalous or conflicting access rights (e.g., overlapping roles with conflicting permissions).</li> </ul> </li> <li>- Customizable Report Outputs: <ul style="list-style-type: none"> <li>o Ability to filter, sort, and export data in various formats (e.g., CSV, PDF).</li> <li>o Visual representations (e.g., charts, graphs) of access rights by user group, business entity, or allowed operations.</li> </ul> </li> </ul>	Mandatory	Lot I	Partially yes - The solution partially meets the requirement	All this information is tracked by the system, so using Analytical tool like Oracle Analytical Server , this report can be constructed.
<b>1.9.4. Input and output data validation</b>					
CNF.163	<p>The application must implement robust mechanisms to validate and sanitize all input data, including:</p> <ul style="list-style-type: none"> <li>- User-provided input (e.g., form submissions, uploaded files).</li> <li>- Inputs from external applications or interfaces.</li> <li>- Input validation techniques, such as pattern matching, or schema validation, to prevent unauthorized manipulation of data.</li> <li>- Logging of rejected or invalid inputs for auditing purposes, including timestamps, the source of the input, and details about the invalid data.</li> </ul>	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE implements robust input validation and sanitization for user and external inputs, using schema and rule-based checks, with comprehensive logging of rejected data including timestamps, source details, and validation errors for auditability.
CNF.164	<p>The interfaces with SWIFT must comply with the minimum-security requirements defined in the "Customer Security Program" document. This includes at least:</p> <ul style="list-style-type: none"> <li>- Implementing the secure mechanism provided by SWIFT, such as the LAU mechanism (HMAC-SHA256), to ensure the integrity and authenticity of input and output data.</li> </ul>	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE and Oracle Banking Payments comply with SWIFT's Customer Security Programme (CSP) by supporting secure integration mechanisms, including the implementation of the Local Authentication Unit (LAU) using HMAC-SHA256 to ensure data integrity and authenticity in SWIFT message exchanges. Additionally, all data exchanges with SWIFT interfaces are logged comprehensively, capturing

	<ul style="list-style-type: none"> <li>- Logging all data exchange activities with SWIFT, including timestamps, source, destination, and security validations performed.</li> </ul>				timestamps, source and destination system IDs, message types, and results of security validations, thereby aligning with SWIFT CSP audit and traceability requirements.
CNF.165	<p>The application must perform complete and independent data validation at all levels to ensure data integrity, completeness, and correctness:</p> <ul style="list-style-type: none"> <li>- <b>Presentation Layer:</b> Validating user inputs on the client side (e.g., using front-end validation techniques) while ensuring no reliance solely on client-side validation.</li> <li>- <b>Business Logic Layer:</b> Validating business rules, workflows, and logic to ensure compliance with requirements.</li> <li>- <b>Data Layer:</b> Validating database constraints, relationships, and data formats to detect corruption or anomalies.</li> </ul> <p>Mechanisms must log detected validation errors, their sources, and the corrective actions taken for audit purposes.</p>	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE ensures multi-layered data validation across presentation, business, and data layers, enforcing rules, constraints, and formats, with comprehensive logging of validation errors, sources, and corrective actions for audit and data integrity.
CNF.166	<p>All information displayed within the application must comply with the NBM's information security policies and include:</p> <ul style="list-style-type: none"> <li>- Security markings based on a predefined classifier established within the application.</li> <li>- Configurable visibility rules for security markings, based on user roles or permissions.</li> <li>- Audit trails for changes made to the security marking policies or classifiers.</li> </ul>	Recommended	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE and Oracle Banking solutions support enforcement of information security policies by allowing configuration of data classification schemes and associating security markings at the screen or data field level. Visibility of these markings can be controlled using role-based access controls (RBAC), ensuring that only authorized users can view or act on classified information. The system also maintains detailed audit trails for any changes made to security classifications or related visibility configurations, ensuring traceability and compliance with internal information governance policies such as those mandated by NBM.
CNF.167	<p>Confidential data must never be stored or accessed insecurely within the application. This includes:</p> <ul style="list-style-type: none"> <li>- Prohibiting storage of sensitive data in unprotected locations such as log files, caching mechanisms, or temporary files.</li> <li>- Logging instances where attempts to access confidential data fail, including the user, timestamp, and reason for failure.</li> <li>- Enforcing encryption for all stored sensitive data and secure wiping techniques for deleted confidential data.</li> </ul>	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE and Oracle Banking applications are designed with stringent data security principles. Sensitive data is never stored in unprotected locations such as log files, caches, or temporary directories. The platform enforces encryption at rest and in transit using industry-standard protocols like AES and TLS. Failed access attempts to confidential data are logged with detailed metadata including user ID, timestamp, and reason for denial. Additionally, the solution supports secure deletion practices to ensure that confidential data is wiped cleanly from storage when deleted, aligning with best practices and regulatory standards.
CNF.168	<p>The application must provide additional protection mechanisms for highly confidential data, including:</p> <ul style="list-style-type: none"> <li>- Masked display of sensitive data (e.g., showing only partial information like "****1234").</li> <li>- Encryption of highly confidential data both in transit and at rest, using industry-standard encryption algorithms (e.g., AES-256).</li> <li>- Requiring repeated or stronger authentication methods (e.g., multi-factor authentication) for accessing or modifying highly confidential data.</li> <li>- Logging access to highly confidential data, including user identity, operation performed, timestamp, and justification for access.</li> </ul>	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE and Oracle Banking solutions provide multiple layers of protection for highly confidential data. Sensitive fields can be masked on the user interface, displaying only partial values (e.g., "\*\*\*\1234") based on user roles. Data is encrypted both at rest and in transit using industry-standard algorithms such as AES-256 and TLS. Access to highly confidential data can be restricted using strong authentication mechanisms, including optional integration with multi-factor authentication solutions. Every access or modification attempt is logged with full audit details including user ID, action taken, timestamp, and purpose, ensuring transparency and compliance with stringent data protection policies.
CNF.169	<p>The application must implement routine procedures for verifying and detecting possible corruption of data integrity relationships, including:</p> <ul style="list-style-type: none"> <li>- Integrity checks using cryptographic methods (e.g., hash-based checksums) to detect unauthorized modifications.</li> <li>- Scheduled audits of data integrity relationships, including database constraints, dependencies, and foreign key relationships.</li> <li>- Logging detected anomalies, corrective actions taken, and the administrators involved in the process.</li> </ul>	Recommended	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE supports data integrity through a combination of cryptographic and relational mechanisms. Hash-based checks and validation routines can be configured to detect unauthorized modifications at the data layer. The system enforces referential integrity using foreign key constraints and dependency rules across business entities. Periodic integrity audits can be scheduled through database jobs and tools, and any anomalies are captured in system logs with audit trails documenting corrective actions and the administrators involved. This ensures end-to-end traceability and maintains the sanctity of data relationships across the application.

**1.9.5. Auditing and security monitoring**

CNF.170	The application must include auditing components that collect, manage, and centrally store auditing records at the application level. The system must ensure high availability and fault tolerance for the auditing components.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE includes centralized auditing capabilities that capture and manage application-level audit logs, ensuring secure storage, high availability, and fault tolerance, supporting traceability, compliance, and reliable audit data management.
CNF.171	The auditing component must allow granular configuration of auditing policies, enabling customization at various levels such as: - User groups, individual users, or roles. - Specific objects or business entities. - Events and event types. - Time intervals or specific time frames for monitoring activities.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE supports granular audit policy configuration, enabling auditing by users, roles, business entities, and event types, with flexible time-based controls to monitor activities and ensure detailed, targeted audit tracking.
CNF.172	Auditing policies must be configurable at the level of: - <b>Objects or Business Entities:</b> Tracking interactions with critical application objects or sensitive entities. - <b>Events:</b> Recording actions such as login attempts, data modifications, access to confidential information, and security policy changes.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE and Oracle Banking Product Processor provide configurable audit logging capabilities that allow audit policies to be defined at both object/business entity and event levels. Auditing can be enabled for specific tables, screens, or business functions to track interactions with sensitive or high-risk entities. Event-based auditing covers login/logout attempts, CRUD operations on critical data, access to restricted fields, and changes to user roles or security policies. The audit logs capture essential metadata such as user ID, timestamp, operation type, and terminal details, supporting compliance and traceability requirements.
CNF.173	The application must allow defining specific characteristics of events to be recorded, such as: - Activities within a particular time interval. - Events involving certain property values or changes in those values. - User-initiated or system-generated actions tied to specific business entities or rules.	Recommended	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE enables configurable event auditing, allowing definition of event characteristics based on time intervals, data value changes, and user or system actions linked to specific business entities and rules.
CNF.174	The auditing component must support the logging of any event occurring at any object or business entity level within the application, ensuring no gaps in audit coverage.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE provides comprehensive audit logging across all objects and business entities, ensuring full traceability of events without gaps, supporting complete audit coverage, compliance, and detailed monitoring of all system activities.
CNF.175	Each auditing record must contain at least the following information: - <b>Timestamp:</b> Exact time and date of the event, synchronized with the system clock. - <b>Subject of the Event:</b> User ID or system process that triggered the event. - <b>Affected Business Object or Entity:</b> Clearly identify the resource or data impacted. - <b>Event Description:</b> The nature of the event (e.g., data access, modification, deletion). - <b>Source Identification:</b> IP address or other relevant identifiers to trace the origin of the event. - <b>Additional Context (if applicable):</b> Such as session ID or associated workflows for comprehensive traceability.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE audit records capture comprehensive details including timestamp, user or process ID, affected entity, event description, source identifiers such as IP address, and additional context like session or workflow references for full traceability.
CNF.176	Auditing records will not contain confidential business information (e.g. passwords entered in failed attempts).	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE ensures audit logs exclude sensitive information such as passwords or confidential data, capturing only necessary event details, thereby maintaining security, privacy, and compliance with data protection best practices.
CNF.177	Errors that may occur when fixing auditing records should not affect the normal operation of the application.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE ensures audit logging is non-intrusive and fault-tolerant, so errors in recording audit data do not impact core application processing, thereby maintaining system stability and uninterrupted business operations.
CNF.178	The auditing component must rely on the system clock of the underlying operating system and include mechanisms to handle time zone differences, daylight saving time adjustments, and clock synchronization (e.g., via NTP).	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE audit logging leverages the underlying system clock, supporting time zone handling, daylight saving adjustments, and synchronization via NTP, ensuring accurate, consistent, and reliable timestamping across all audit records.

CNF.179	The auditing component must include an archiving mechanism to manage historical auditing records, which should be configurable with options for:	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE provides configurable audit archiving mechanisms, allowing control over archiving frequency, data retention periods, export formats, and storage destinations, ensuring efficient management of historical audit records and compliance requirements.
	- Frequency of archiving (e.g., daily, weekly).				
	- Age of data to be archived.				
	- Archiving format (e.g., CSV, JSON, XML).				
- Storage destination (e.g., local storage, remote servers).					
CNF.180	The application must be able to automatically generate notifications for responsible personnel upon detecting specific security events, based on customizable thresholds or configurations. Notifications should include:	Recommended	Lot I	Partially yes - The solution partially meets the requirement	Oracle FLEXCUBE and Oracle Banking solutions support security event monitoring and alerting through their native monitoring framework and integration with external tools like Oracle Enterprise Manager and SIEM(Security Information and Event Management) platforms. The system can be configured to detect predefined security events—such as unauthorized access attempts, data breaches, or policy violations—and automatically trigger notifications to designated personnel. These alerts can include detailed metadata like event type, timestamp, and source. Delivery channels are configurable and may include email, SMS (via integration), or real-time dashboard alerts within the administrative UI, ensuring timely response and compliance with organizational security policies.
	- Event details (e.g., type, timestamp, source).				
	- Recommended actions, where applicable.				
- Configurable channels for delivery (e.g., email, SMS, dashboard alerts).					
CNF.181	The auditing component must support integration with Security Information and Event Management (SIEM) solutions using open standards (e.g., Syslog, dblink). Integration must include:	Mandatory	Lot I	Yes - the solution fully meets the requirement	Yes, it can be integrated with SIEM tools
	- Secure transmission of auditing records to external systems.				
	- Compatibility with common logging protocols and formats.				
- Real-time or batch transfer options.					
CNF.182	The application will allow to set historical versions of the data, which will be considered particularly sensitive.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE supports historical data versioning for sensitive data through its audit trail and change history frameworks. For particularly sensitive information, FLEXCUBE allows configuration of data retention policies and maintains historical snapshots tied to key business events (e.g., KYC updates, credit decisions, limit changes). These versions are stored securely with metadata like timestamp, user ID, and reason code, and access to historical versions is governed by strict role-based access controls. This ensures full traceability and compliance with regulatory expectations around sensitive data handling.
CNF.183	The solution must provide user-friendly tools for managing and analyzing auditing records, including:	Recommended	Lot I	Partially yes - The solution partially meets the requirement	Oracle Flexcube Audit Information needs to be integrated with Oracle Audit Vault or SIEM tool for generating analysis on the audit data.
	- Filtering and querying records by any field (e.g., user, timestamp, event type).				
	- Exporting logs in common formats (e.g., CSV, PDF).				
- Importing historical auditing archives for occasional analysis activities.					
CNF.184	The application must implement secure mechanisms to ensure the integrity of auditing records, such as access controls to restrict who can view or modify audit logs.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE and Oracle Banking applications implement secure mechanisms to preserve the integrity of audit logs. Access to audit records is strictly controlled through role-based access control (RBAC), ensuring that only authorized personnel (e.g., auditors, super admins) can view audit trails. Modification of audit records is technically restricted—logs are written in append-only mode in system-maintained tables like 'AUDIT_LOG', with no update/delete rights even for privileged users. Database-level security, such as Oracle DB Vault or Transparent Data Encryption (TDE), further ensures that audit data cannot be tampered with. Additionally, access to these logs is itself audited, providing traceability of who viewed audit data, when, and for what purpose. These controls collectively ensure the confidentiality, integrity, and non-repudiation of audit records.
<b>1.9.6. Exception handling</b>					
CNF.185	The application must handle all errors and exceptions that arise during its operation. Exception handling mechanisms should ensure:	Mandatory	Lot I	Yes - the solution fully meets the requirement	Application-level exceptions: Input validation failures. Business rule violations (e.g., insufficient funds). API errors with retry logic. Workflow errors with status updates and escalation. Controlled fallbacks:
	- Detection of system crashes or instability.				
	- Logging of all relevant details for diagnostics.				

	<ul style="list-style-type: none"> <li>- Activating fallback mechanisms to maintain user experience where possible (e.g. avoiding sudden interruptions or confusing error messages).</li> </ul>				<p>Displaying meaningful error messages to users (not raw stack traces).</p>
CNF.186	<p>The application must centrally record all exceptions and errors, storing them in a secure, centralized logging repository. The logging system must:</p> <ul style="list-style-type: none"> <li>- Include detailed information such as timestamps, user ID (if applicable), affected modules, and a description of the error.</li> <li>- Support filtering and querying to facilitate diagnostics.</li> <li>- Ensure logs are protected against unauthorized access or tampering.</li> </ul>	Mandatory	Lot I	Partially yes - The solution partially meets the requirement	Oracle FLEXCUBE provides centralized exception and error logging capabilities via its core infrastructure and logging framework. All exceptions and system-level errors are captured with detailed metadata including timestamps, user IDs (where applicable), affected modules, and descriptive error messages. These logs are typically stored in a secure, centralized repository (such as database tables or application logs) with access restricted through role-based security controls. FLEXCUBE's diagnostic logging can be configured for verbosity and includes filtering and querying capabilities via tools such as Oracle Enterprise Manager or external log aggregators like ELK Stack or Splunk. This setup ensures logs are both auditable and protected from unauthorized access or tampering, supporting compliance and operational resilience.
CNF.187	<p>When an error occurs, the application must display a generic and user-friendly error message. The error message must:</p> <ul style="list-style-type: none"> <li>- Avoid revealing sensitive system details.</li> <li>- Include an error code and a unique error identifier for troubleshooting.</li> <li>- Offer guidance to the user, such as suggesting possible corrective actions or directing them to support channels.</li> </ul>	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE provides user-friendly error handling with generic messages that avoid sensitive details, include unique error codes for traceability, and offer guidance or next steps to assist users and support teams in resolution.
CNF.188	<p>The application must centrally record all exceptions and errors, storing them in a secure, centralized logging repository. The logging system must:</p> <ul style="list-style-type: none"> <li>- Include detailed information such as timestamps, user ID (if applicable), affected modules, and a description of the error.</li> <li>- Support filtering and querying to facilitate diagnostics.</li> <li>- Ensure logs are protected against unauthorized access or tampering.</li> </ul>	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE provides centralized exception and error logging capabilities via its core infrastructure and logging framework. All exceptions and system-level errors are captured with detailed metadata including timestamps, user IDs (where applicable), affected modules, and descriptive error messages. These logs are typically stored in a secure, centralized repository (such as database tables or application logs) with access restricted through role-based security controls. FLEXCUBE's diagnostic logging can be configured for verbosity and includes filtering and querying capabilities via tools such as Oracle Enterprise Manager or external log aggregators like ELK Stack or Splunk. This setup ensures logs are both auditable and protected from unauthorized access or tampering, supporting compliance and operational resilience.
CNF.189	<p>The application must have the capability to automatically notify responsible parties (e.g., system administrators, support teams, or the software manufacturer) in the event of specific critical errors. Notifications should:</p> <ul style="list-style-type: none"> <li>- Be customizable based on error severity, frequency, or affected modules.</li> <li>- Include detailed diagnostic information, such as error codes, timestamps, and affected systems.</li> <li>- Be sent via configurable channels (e.g., email, SMS, or integration with incident management platforms).</li> </ul>	Recommended	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE supports automated notification mechanisms for critical system errors through its integration with monitoring and alerting tools like Oracle Enterprise Manager, SNMP traps, or third-party solutions such as Splunk, Prometheus, or ServiceNow. These tools can be configured to detect specific error conditions based on severity, frequency, or affected components and generate alerts in real-time. Notifications include detailed diagnostic data such as error codes, timestamps, user context (if applicable), and impacted modules. Alerts can be routed via email, SMS, or integrated with ITSM platforms for ticket generation and escalation, ensuring timely action by responsible stakeholders.
CNF.190	<p>The application must include tools for performing backup operations and managing historical backups. These tools should:</p> <ul style="list-style-type: none"> <li>- Support automated scheduling of backups with configurable frequency.</li> <li>- Ensure secure storage of backups, including encryption and access control.</li> <li>- Provide mechanisms for verifying backup integrity and completeness.</li> <li>- Support versioning and retention policies for historical backups.</li> <li>- Include monitoring and notification features for backup failures.</li> </ul>	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE supports backup and historical backup management through Oracle-native tools like Oracle Recovery Manager (RMAN) and Data Pump, integrated into the underlying Oracle Database platform. These tools allow for automated scheduling of full and incremental backups, with encryption and role-based access control to protect sensitive data. Backup integrity is verified using checksum validation during the backup process, and retention policies can be configured based on business needs. Additionally, Oracle Enterprise Manager or third-party tools like Veeam or Commvault can be integrated to monitor backup operations, provide alert notifications on failure, and manage backup versioning and storage optimization.
CNF.191	<p>The application must implement robust mechanisms to maintain data integrity during component failures. These mechanisms should:</p> <ul style="list-style-type: none"> <li>- Prevent data corruption or loss during power outages, crashes, or unexpected shutdowns.</li> <li>- Use transactional processing to ensure atomicity, consistency, isolation, and durability (ACID).</li> </ul>	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE, built on the robust Oracle Database platform, ensures data integrity during component failures through several mechanisms. It leverages ACID-compliant transactional processing, which guarantees that database operations are atomic, consistent, isolated, and durable—even in the event of unexpected crashes or power failures. Redo logs and undo segments help recover committed transactions and roll back incomplete ones. Additionally, Oracle Data Guard or Flashback technologies can be used to restore data to a consistent state. FLEXCUBE can be integrated with Oracle Enterprise Manager or third-party tools to enable real-

	<ul style="list-style-type: none"> <li>- Include real-time monitoring and alerting for potential data integrity issues.</li> </ul>				time monitoring and alerting for potential data integrity violations, ensuring quick detection and response to issues.
CNF.192	<p>The application must provide mechanisms to enable the rapid restoration of availability and accessibility following continuity incidents. These mechanisms should:</p> <ul style="list-style-type: none"> <li>- Include detailed disaster recovery procedures integrated within the solution.</li> <li>- Support data recovery from backups with minimal downtime.</li> <li>- Ensure compatibility with failover systems for high availability.</li> <li>- Include capabilities for periodic testing of recovery procedures to ensure readiness.</li> </ul>	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE and Oracle Banking suite offer built-in mechanisms to support rapid restoration of availability and accessibility in the event of continuity incidents. These include well-documented disaster recovery procedures that align with industry best practices, along with compatibility for deployment across high-availability infrastructures using active-passive or active-active configurations. The application supports swift data recovery from secure backups with minimal downtime and includes provisions for periodic testing of disaster recovery processes to validate readiness and ensure business continuity. Integration with failover and replication technologies further enhances system resilience.
CNF.193	<p>The application architecture must be designed to be resilient to component failures and eliminate single points of failure (SPOF). Resilience should include:</p> <ul style="list-style-type: none"> <li>- Redundancy for critical components (e.g., database, application server).</li> <li>- Load balancing to distribute workloads and mitigate performance bottlenecks.</li> <li>- Automatic failover mechanisms to ensure continuity of service during failures.</li> <li>- Scalability to handle unexpected increases in load without failure.</li> </ul>	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE and Oracle Banking applications are architected to ensure high resilience and eliminate single points of failure. The architecture includes built-in redundancy for critical components such as databases and application servers, with clustering and replication supported for continuous availability. Load balancing mechanisms are used to efficiently distribute workloads across servers, preventing performance degradation. Automatic failover features ensure uninterrupted service during component failures, and the solution is horizontally scalable to accommodate increased load or transaction volumes, thereby maintaining stability and performance under stress.
CNF.194	The application must allow integration with monitoring tools such as SIEMs.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE supports integration with enterprise monitoring and SIEM tools through standardized logs, APIs, and event streams, enabling real-time security monitoring, centralized analysis, and effective incident detection and response.
CNF.195	The requested solution must deliver a service level availability of at least 99.7%, calculated over a monthly reporting period.	Mandatory	Lot I	Yes - the solution fully meets the requirement	Oracle FLEXCUBE is designed for high availability, supporting configurations such as clustering and failover to achieve at least 99.7% monthly uptime, ensuring resilient operations, minimal downtime, and continuous service delivery.
<b>1.11. Requirements for Source Codes</b>					
CNF.196	<p>The Tenderer must guarantee the availability of the Source Codes for the application included in the proposed solution (including third-party components) in cases where the software supplier is unable to maintain the application (e.g., liquidation, bankruptcy, reorganization). This must be achieved through the following:</p> <ul style="list-style-type: none"> <li>- An escrow protection agreement with a reputable and mutually agreed-upon escrow agent.</li> <li>- The agreement must be activated upon the Buyer's request (at NBM's discretion) after the final acceptance of the solution.</li> <li>- The Source Codes must be submitted within 30 working days unless otherwise agreed upon by the Parties.</li> <li>- The escrow agreement must cover a minimum period of five (5) years.</li> <li>- The Source Codes must include all necessary documentation and dependencies to enable independent maintenance and further development.</li> </ul>	Mandatory	Lot I	No - the solution does not meet the requirement	Oracle does not enter into individual Escrow Agreements with its customers or offer escrow benefits to customers. However, we have an established escrow account for our software source code. Software source code is deposited as new major versions are released. We maintain source code for all major or minor releases of all products in escrow. The Escrow Agreement is confidential information, and not available for release to customers.
CNF.197	<p>The selected Tenderer must provide the NBM with all Source Codes which were custom developed as part of the project. The delivery must meet the following criteria:</p> <ul style="list-style-type: none"> <li>- Source Codes must be complete, with no obfuscated or missing components.</li> </ul>	Mandatory	Lot I	Yes - the solution fully	Oracle FLEXCUBE allows delivery of all custom-developed source code, including complete components, libraries, dependencies, and build instructions, with ongoing sharing of updates and

CNF.197	<ul style="list-style-type: none"> <li>- All related libraries, dependencies, and build instructions must be included to ensure full functionality and maintainability.</li> <li>- Updates and patches must also be shared promptly as they are developed during the contract period.</li> </ul>	Mandatory	Lot 1	meets the requirement	Components, libraries, dependencies, and build instructions, with ongoing sharing of updates and patches to ensure maintainability and continuity.
CNF.198	<p>The Source Code delivered by the developers must adhere to best practices for maintainable software development, including:</p> <ul style="list-style-type: none"> <li>- Clear and consistent structure for easy navigation and understanding.</li> <li>- Comprehensive inline comments explaining functionality, logic, and complex code sections.</li> <li>- Meaningful and self-explanatory variable, function, and class names.</li> <li>- Modular design principles to support future scalability and modification.</li> <li>- Compliance with industry standards or specific coding guidelines agreed upon with the Buyer (e.g., ISO/IEC 25010 or similar).</li> <li>- The Source Code must pass quality assurance checks, including static code analysis and unit testing, before delivery.</li> </ul>	Mandatory	Lot 1	Yes - the solution fully meets the requirement	Oracle FLEXCUBE custom developments follow best practices with structured, well-documented, and modular code, adhering to standards, using meaningful naming, and undergoing rigorous QA including static analysis and unit testing before delivery.
CNF.199	<p>The authenticity and integrity of all files containing the Source Codes must be verified and guaranteed by the Contractor through:</p> <ul style="list-style-type: none"> <li>- Digital signatures to confirm the Source Codes' origin and integrity.</li> <li>- Timestamping of the digital signature to ensure traceability.</li> <li>- Encryption of the Source Code files during transmission and storage to prevent unauthorized access.</li> <li>- Documentation of verification steps and logs to support audits or legal disputes if required.</li> </ul>	Mandatory	Lot 1	Yes - the solution fully meets the requirement	Oracle FLEXCUBE custom code delivery ensures authenticity and integrity through digital signatures, timestamping, encryption during transit and storage, and maintained verification logs, supporting traceability, auditability, and compliance with security requirements.