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 solution partially meets

Requirement Code	Requirement	The level of obligation	Lot II	Tenderer's Response	Tenderer's Comment
1. Non-functional requirements					
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		Yes - the solution fully meets the requirement	Oracle EBS is architected with a strong focus on usability, maintainability, and adaptability. Its modular, open architecture supports evolving business needs over time, fully aligning with NBM's non-functional expectations.
1.1. Solution-level architecture					
CNF.2	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. The solution's architecture should embed contemporary industry best practices, incorporating modern concepts such as: - **Unified Contextual Experience:** The architecture must prioritize a unified and intuitive user experience across all system contexts, ensuring operational cohesion. - **Real-time Operation:** The solution must demonstrate the capability for real-time processing to meet the dynamic needs of the NBM's operations. - **Plug-and-Play:** The architecture should support seamless integration and interaction with external systems, enabling a "Plug-and-Play" approach for additional components or functionalities. - **Cloud-Ready Capabilities:** It is imperative that the solution's architecture is designed with cloud-ready features, ensuring scalability, accessibility, and efficiency in a cloud ready environment. - **Future-Ready Architectural Design:** The proposed architecture must exhibit forward-thinking attributes, anticipating technological advancements and accommodating future developments without substantial reengineering. These principles are foundational and should be incorporated at all levels of the proposed solution's architecture. *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.*	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS features an open, modular, pre-integrated architecture based on industry standards (SOA, web services). It delivers unified contextual experience, real-time processing, plug-and-play integration via SOA Suite, cloud-ready capabilities (PaaS, private cloud), and future-ready design through continuous Oracle enhancements.
CNF.3	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. By implementing a standardized interface for each user group, the solution aims to: - **Enhance Consistency:** Provide a consistent look and feel across different functionalities, reducing the learning curve for users and promoting a cohesive user experience. - **Improve Efficiency:** Streamline user interactions by presenting relevant features in a user-friendly manner, optimizing task execution and minimizing complexity. - **Facilitate Training and Onboarding:** Simplify training processes and onboarding for new users by offering uniform interfaces tailored to their specific roles.	Recommended	+	Yes - the solution fully meets the requirement	Oracle EBS provides role-based dashboards and responsibility-level access, giving each user group (process managers, external users, report consumers, administrators) a unified, intuitive interface. This reduces training time and improves efficiency.

	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.				
CNF.4	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.). *To demonstrate alignment with this requirement, Tenderers are requested to:* - *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.* - *Describe how the proposed architecture aligns with industry best practices and frameworks. Reference industry-recognized resources such as TOGAF, BIAN etc.* - *Highlight architectural components or design principles that contribute to scalability and adaptability over time.*	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS adheres to open standards (SOAP, REST, XML, SQL, LDAP, SAML) and widely adopted frameworks. The architecture follows TOGAF principles, and Oracle's reference architectures align with BIAN for banking.
CNF.5	The application architecture will be designed to be service-oriented, embracing either Service-Oriented Architecture (SOA) or microservices-based deployments. *To demonstrate alignment with this requirement, Tenderers are requested to:* - *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.* - *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.* - *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.* - *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.*	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS is built on a service-oriented architecture with modular components exposed as web services. The included SOA Suite enables loose coupling, orchestration, horizontal scaling, load balancing, and fault tolerance (clustering, RAC).
CNF.6	The system must seamlessly integrate with external systems and delivery channels by supporting a comprehensive range of industry-standard protocols, such as: - ISO 20022 - SOAP/REST/gRPC and HTTP/S for web services-based interfaces - XML - Secure FTP - SMTP / SMPP - Others *To demonstrate alignment with this requirement, Tenderers are requested to:* - *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.* - *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.*	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS supports ISO 20022, SOAP/REST/HTTP/S, XML, SFTP, SMTP, and other protocols natively. The SOA Suite and integration repositories ensure secure, encrypted data exchange with full audit trails.

CNF.7	The application architecture will adopt a modern client-server paradigm organized into a minimum of three well-defined vertical layers. The architecture must adhere to industry best practices, emphasizing clear and independent delineation between each layer to ensure a robust and scalable system. Specifically: - ***Presentation Layer:*** 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. - ***Application (or Business Logic) Layer:*** 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. - ***Data Access Layer:*** 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.	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS follows a strict three-tier model: (1) Presentation layer (web browser, Forms applet), (2) Application/Business Logic layer (WebLogic, Concurrent Managers), (3) Data layer (Oracle Database). Each layer is independent, enhancing scalability and maintainability.
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	+	Yes - the solution fully meets the requirement	All component communication uses encrypted internal interfaces. Oracle EBS supports deployment behind Zero Trust networks, with TLS, mutual authentication, and integration with NBM's existing security infrastructure.
CNF.9	The application will have capabilities for optimized processing of user queries (e.g. caching).	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS uses database caching, result set caching, and Oracle WebLogic's in-memory data grid features to optimize user query performance.
CNF.10	The production environment must exhibit a resilient architecture that supports active-pasive configurations across two distinct geosite locations. This setup is required to ensure high availability and operational stability. To align with the NBM standards and facilitate appropriate sizing of the architecture, the following parameters are to be considered: - ***High Availability Configuration:*** The production environment is mandated to operate in an active-pasive configuration across two geosite locations. This design ensures redundancy and fault tolerance, minimizing the risk of downtime and providing high availability services to users. - ***Service Level Agreement (SLA):*** 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. - ***Recovery Time Objective (RTO):*** 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. - ***Recovery Point Objective (RPO):*** 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. - ***Switchover Time Between Primary and Backup Sites:*** 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.	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS supports active-passive configurations across two geosites using Oracle Data Guard and application clustering. SLA: 99.7% uptime (08:00-18:00), RTO ≤4h, RPO = zero data loss, switchover ≤1h.
1.1.2. Requirements for presentation layer					

CNF.11	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.	Informative		Yes - the solution fully meets the requirement	Oracle EBS presentation layer (OA Framework, Forms) provides a user-friendly, role-based interface that maximizes utility for both business and administrative users.
CNF.12	All graphical user interfaces must comply with the following high-level principles: i. **The structure principle -** 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; ii. **The simplicity principle -** 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; iii. **The visibility principle -** 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. iv. **The feedback principle -** 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. v. **The tolerance principle -** 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. vi. **The reuse principle -** 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. *To demonstrate alignment with this requirement, Tenderers are requested to:* - *Describe how the GUI architecture is designed and organized in a structured and intuitive manner.* - *Showcase examples of GUI components and interactions that reflect intuitive design principles.* - *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.*	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS interfaces follow structure, simplicity, visibility, feedback, tolerance, and reuse principles. Example: consistent menu layouts, inline validation, undo/redo, and shortcut keys
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	+	Yes - the solution fully meets the requirement	Oracle EBS is fully accessible via modern browsers (Chrome, Edge, Firefox) without additional client installations. Java plug-in for Forms is automatically downloaded if needed.
CNF.14	Presentation layer will not implement business rules, except for validating input data.	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS implements only input validation in the presentation layer; all business rules are enforced in the business logic layer (PL/SQL, Java, Workflow).
1.1.3. Requirements for Business logic layer					

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		Yes - the solution fully meets the requirement	Oracle EBS business logic resides in the application tier, managing data access, transformation, and rules. It ensures consistency and correctness of financial and operational data
CNF.16	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. *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.*	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS decomposes business logic into fine-grained components (e.g., subprograms, concurrent programs, web services) with well-defined interfaces. This supports modularity and reuse.
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	+	Yes - the solution fully meets the requirement	The business logic layer is completely independent of the presentation layer. Changes to UI do not affect business rules, and external applications access logic only via published APIs.
CNF.18	Business logic layer must contain and have delimited “business workflow” type components and “business entity” type components.	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS clearly separates workflow components (Oracle Workflow, AME) from entity components (PL/SQL packages, ADF Business Components). This aligns with NBM’s requirement.
CNF.19	Accessing the "business entity" type components will be done through the "business workflow" type components.	Mandatory	+	Yes - the solution fully meets the requirement	In Oracle EBS, business entities are manipulated through workflow components that enforce process rules, ensuring data integrity and segregation of concerns.
CNF.20	Business entities must be clearly identified at the level of business logic and encapsulated in the “business entities” components.	Mandatory	+	Yes - the solution fully meets the requirement	Business entities (e.g., Invoice, GL Journal, Asset) are encapsulated in dedicated PL/SQL APIs or Java objects, hiding internal data structures and exposing only necessary operations.
CNF.21	The "business entity" components must encapsulate all data and business logic relevant to the associated business entity. These components should be designed to: - **Provide all necessary functionality** to perform operations related to the business entity. - **Enforce applicable rules and constraints** to ensure compliance with business requirements. - **Preserve the accuracy, consistency, and correctness of the data** contained within the component. This ensures that each business entity component remains self-contained, cohesive, and aligned with the principles of modularity and maintainability.	Mandatory	+	Yes - the solution fully meets the requirement	Each entity component provides full CRUD operations, enforces business rules, and maintains data consistency through transactional boundaries and validation logic.
CNF.22	The related Business logic layer components must communicate with each other through dedicated internal interfaces / functions (tight coupling).	Mandatory	+	Yes - the solution fully meets the requirement	Related business logic components communicate via internal PL/SQL calls or Java methods (tight coupling) for performance, while external access is loosely coupled.
CNF.23	Business logic layer components must be accessible to external applications only through the external applicative interfaces defined for this purpose.	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS exposes external interfaces via SOAP/REST web services, APIs, or XML gateways. Direct access to internal components is prohibited.
CNF.24	Business logic layer architecture will allow concurrent access to application functions.	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS supports high concurrency through WebLogic connection pools, database row-level locking, and concurrent managers. ACID transactions ensure data integrity.
1.1.4. Requirements for Data layer					
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		Yes - the solution fully meets the requirement	Oracle Database serves as the data layer, enforcing integrity rules via constraints, triggers, and RLS. Data is accessible only via the business logic layer.
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	+	Yes - the solution fully meets the requirement	The data layer contains all necessary schemas for GL, AP, AR, FA, PO, INV, HR, Payroll, etc., fully supporting NBM’s requested services.

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	+	Yes - the solution fully meets the requirement	The application supports a normalized data model at the data layer, ensuring minimal redundancy and optimal data organization. All data entities and their relationships are accurately defined and implemented in alignment with business requirements, maintaining strong referential integrity. The design enforces consistency and eliminates data duplication, ensuring that data remains reliable, structured, and logically aligned with its business purpose.
CNF.28	The application must support an integrated data model for the reference information at the application level (common or synchronized nomenclatures).	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS provides a common, synchronized reference data model (e.g., chart of accounts, supplier, customer, item master) across all modules.
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	+	Yes - the solution fully meets the requirement	Oracle EBS includes robust data migration tools (FBDI, ADFdi, Web ADI, Open Interfaces, APIs) that ensure complete, correct migration from legacy systems, with deviation only upon NBM approval.
CNF.30	The application data must be accessible only through the components contained in the Business logic layer.	Mandatory	+	Yes - the solution fully meets the requirement	The application supports controlled data access by ensuring that all application data is accessed exclusively through components within the business logic layer. This enforces strict separation of concerns, prevents direct database access, and ensures that all data operations are governed by defined business rules, validations, and security controls, thereby maintaining data integrity, consistency, and compliance.
CNF.31	The data stored in the application must be neutral and independent of the Business logic layer.	Mandatory	+	Yes - the solution fully meets the requirement	The application supports a data architecture where stored data remains neutral and independent of the business logic layer, ensuring clear separation of concerns. The data model is designed to be generic, reusable, and not tightly coupled to specific application logic, enabling flexibility, scalability, and easier integration with other systems while maintaining consistency and integrity across different business processes.
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	+	Yes - the solution fully meets the requirement	The application supports an optimized data architecture designed to efficiently handle both transactional (OLTP) and analytical (OLAP) workloads. It ensures high-performance data access for real-time transaction processing while also enabling efficient data aggregation, querying, and reporting for analytics. This is achieved through appropriate data modeling, indexing, and workload separation strategies, ensuring optimal performance, scalability, and responsiveness across operational and reporting use cases.
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	+	Yes - the solution fully meets the requirement	Oracle provides complete data dictionary documentation (EBS Tables and Views) with semantic descriptions. Users can access this via Oracle Business Intelligence Discoverer or data dictionary views.
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	+	Yes - the solution fully meets the requirement	The application supports robust data integrity and consistency by managing concurrent access and modifications from multiple entities, including users, internal processes, and external applications. It leverages transaction management, locking mechanisms, and concurrency control techniques to ensure data correctness during simultaneous operations. Additionally, the system provides appropriate user notifications and feedback in case of conflicts or transaction issues, ensuring transparency and reliability in data handling.
1.1.5. Requirements for Technology layer					
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		Yes - the solution fully meets the requirement	The technology layer includes Oracle Database, WebLogic Server, Oracle HTTP Server, Concurrent Managers, and SOA Suite, all supporting the upper layers.
CNF.36	The technological architecture must ensure the continuous availability and accessibility of application components.	Mandatory	+	Yes - the solution fully meets the requirement	With Oracle RAC, Data Guard, and WebLogic clustering, the technology architecture ensures high availability and accessibility of all components.
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	+	Yes - the solution fully meets the requirement	Oracle EBS design eliminates SPOFs: redundant application servers, load balancers, RAC database nodes, and shared storage. All components can be clustered.
CNF.38	The technological architecture must ensure the rational and balanced use of processing resources.	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS includes resource managers (database, concurrent managers) that prioritize workloads, balance CPU/IO, and prevent resource contention.
1.2. Technological platform					

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	+	Yes - the solution fully meets the requirement	The proposed platform includes Oracle Database EE, WebLogic Suite, SOA Suite, and Analytics Server, running on Linux/Windows x86 VMware virtualized environment.
CNF.40	The application should possess minimal dependence on the underlying technology platform to ensure scalability, flexibility, and ease of maintenance.	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS is hardware-agnostic and supports multiple OS and hypervisors (VMware, OVM). Applications are portable across cloud and on-premise.
1.2.1. General requirements					
CNF.41	The platform technologies present in the application architecture must be open technologies (without proprietary technologies of the supplier), or widely used technologies. *Please provide complete information on the technological platforms supported by the proposed solution.*	Mandatory	+	Yes - the solution fully meets the requirement	All components use open or widely adopted technologies (Java, PL/SQL, SQL, XML, SOAP, REST). No proprietary-only stacks are used.
CNF.42	Application components should be hardware-agnostic, capable of running on x86 processors.	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS runs on x86 processors (Intel/AMD) and supports standard server hardware available on the market.
CNF.43	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. *To demonstrate alignment with this requirement, Tenderers are requested to:* - *Showcase how the application architecture is optimized for cloud computing environments, particularly private clouds.* - *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.*	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS architecture supports private cloud deployments with features like elastic scaling, resource pooling, and automated provisioning. It is certified on Oracle Cloud and VMware.
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	+	Yes - the solution fully meets the requirement	The proposed platform uses a single OS (Linux or Windows), single database (Oracle), and consistent middleware (WebLogic), minimizing technology diversity.
CNF.45	The application must support the creation, modification, processing, storage and access of textual data in Unicode format.	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS fully supports Unicode (AL32UTF8) for creation, modification, storage, and retrieval of textual data in any language, including Romanian.
1.2.2. Presentation layer					
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	+	Yes - the solution fully meets the requirement	End-users access Oracle EBS via standard desktop/laptop browsers and VDI. Printing is supported via native OS drivers.
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	+	Yes - the solution fully meets the requirement	Oracle EBS provides mobile-optimized interfaces for approvals, expense reporting, and dashboards via Oracle Mobile Approvals and responsive OA Framework.
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	+	Yes - the solution fully meets the requirement	Oracle EBS reports (XML Publisher) and forms support automatic scaling to paper sizes (A2, A3, A4, portrait/landscape) with print preview.
CNF.49	The client application must be able to run in Windows 10/11 operating environments and newer.	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS client components (Forms applet, BI Publisher) are compatible with Windows 10, 11, and newer versions using standard Java runtime.
1.2.3. Business logic layer					
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	+	Yes - the solution fully meets the requirement	Oracle EBS business logic uses Java (OAF, SOA), PL/SQL, and modern frameworks. Development tools are up-to-date and widely used.
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	+	Yes - the solution fully meets the requirement	Oracle EBS exposes standard APIs and web services, allowing NBM to develop custom components that seamlessly integrate with the application.
1.2.4. Data layer					
	The application must be compatible with the latest Long Releases of the following types of databases: Oracle, or MS SQL.				

CNF.52	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.	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS runs natively on Oracle Database (certified). MS SQL is not supported; however, Oracle Database Enterprise Edition is included in the BOM and meets all requirements.
CNF.53	All functional features of the application (OLTP) will be implemented on a single database management platform.	Mandatory	+	Yes - the solution fully meets the requirement	All Oracle EBS functional modules use the same Oracle Database instance (single platform), ensuring transactional consistency and simplified management.
1.2.5. Technology layer					
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	+	Yes - the solution fully meets the requirement	Oracle EBS is certified on VMware vSphere and runs on x86 with Linux/Windows Server. Supported OS versions are within last two major releases.
CNF.55	Only standard equipment will be required to run the application, available to be freely purchased on the market by the NBM.	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS runs on standard, commercially available servers, storage, and networking equipment. No proprietary hardware is required.
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	+	Yes - the solution fully meets the requirement	JMR will provide detailed infrastructure sizing (CPU, RAM, storage, network) based on NBM's volume and performance needs, as part of the implementation phase.
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	+	Yes - the solution fully meets the requirement	JMR will present technology alternatives (e.g., RAC vs. standalone, storage options) for NBM to review and select the final configuration.
1.3. Interoperability requirements					
CNF.58	Interoperability is defined as the application's ability to communicate effectively with other systems.	Informative	+	Yes - the solution fully meets the requirement	Oracle EBS is designed for high interoperability using standards-based interfaces, enabling communication with internal and external 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	+	Yes - the solution fully meets the requirement	Oracle EBS will be integrated with NBM's existing applications (ADPS, SWIFT, etc.) via SOA Suite and the CBS-delivered ESB (Lot 1).
1.3.1. Requirements for Enterprise Service Bus component					
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	+	Yes - the solution fully meets the requirement	According to the NBM specification, the ESB is part of Lot 1 (CBS). Oracle EBS will seamlessly connect to that ESB using standard SOA/EDA principles.
	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:			Yes - the solution fully meets the requirement	Oracle EBS supports all listed ESB features: robust integration, standardized protocols, intuitive management, flexibility, scalability, monitoring, security, and open standards.
	Integration Capability: The ESB must possess robust integration capabilities, enabling it to seamlessly connect with other IT systems within the NBM;			Yes - the solution fully meets the requirement	Oracle EBS supports all listed ESB features: robust integration, standardized protocols, intuitive management, flexibility, scalability, monitoring, security, and open standards.
	Standardized Approach: Integration with other systems should adhere to standardized approaches and protocols to ensure compatibility and interoperability across different platforms and technologies;			Yes - the solution fully meets the requirement	Oracle EBS supports all listed ESB features: robust integration, standardized protocols, intuitive management, flexibility, scalability, monitoring, security, and open standards.
	Ease of Management: 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;			Yes - the solution fully meets the requirement	Oracle EBS supports all listed ESB features: robust integration, standardized protocols, intuitive management, flexibility, scalability, monitoring, security, and open standards.
	Flexibility: It should allow for flexible configuration and customization of integration processes to accommodate evolving business requirements and changing technological landscapes.			Yes - the solution fully meets the requirement	Oracle EBS supports all listed ESB features: robust integration, standardized protocols, intuitive management, flexibility, scalability, monitoring, security, and open standards.

CNF.61	***Scalability and Reliability:*** 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.	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS supports all listed ESB features: robust integration, standardized protocols, intuitive management, flexibility, scalability, monitoring, security, and open standards.
	Monitoring and Alerting: 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.			Yes - the solution fully meets the requirement	Oracle EBS supports all listed ESB features: robust integration, standardized protocols, intuitive management, flexibility, scalability, monitoring, security, and open standards.
	Interoperability Standards: 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.			Yes - the solution fully meets the requirement	Oracle EBS supports all listed ESB features: robust integration, standardized protocols, intuitive management, flexibility, scalability, monitoring, security, and open standards.
	Security: 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. *Please provide detailed description and documentation outlining the ESB's core features.*			Yes - the solution fully meets the requirement	Oracle EBS supports all listed ESB features: robust integration, standardized protocols, intuitive management, flexibility, scalability, monitoring, security, and open standards.
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	+	Yes - the solution fully meets the requirement	Oracle SOA Suite (included) provides BPEL, BPMN, and visual editors for orchestrating complex business processes across multiple systems.
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	+	Yes - the solution fully meets the requirement	Oracle Business Rules and Oracle Workflow provide visual, form-based tools for process-level rule management, accessible to trained specialists.
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	+	Yes - the solution fully meets the requirement	Rule changes are made through configuration, not coding. Versioning, template reuse, and monitoring are built into Oracle Workflow and SOA Composer.
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	+	Yes - the solution fully meets the requirement	Oracle Enterprise Manager and SOA Suite dashboards provide real-time monitoring of processes, events, and data flows between systems.
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	+	Yes - the solution fully meets the requirement	Oracle EBS includes a comprehensive alert and messaging system (Oracle Alert, Workflow Mailer) to manage interoperability communications.
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	+	Yes - the solution fully meets the requirement	Oracle EBS allows definition of system events (e.g., PO approval) and attachment of communication scenarios (email, alert, log) using Workflow.
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	+	Yes - the solution fully meets the requirement	Oracle SOA Suite interfaces support encoding/decoding, validation, grouping, SSO, encryption, and digital signatures for messages.
CNF.69	The ESB's messaging subsystem must offer the possibility of integration with the Beneficiary's e-mail services.	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS integrates with NBM's email server via SMTP and Workflow Mailer for automated notifications and document delivery.
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	+	Yes - the solution fully meets the requirement	Oracle SOA Suite includes message caching, content-based routing, filtering, and load balancing. Horizontal/vertical scaling is fully supported.
CNF.71	The ESB should facilitate compliance with regulatory requirements, industry standards, and organizational policies related to data privacy, security, and governance.	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS helps meet data privacy and governance requirements through audit trails, encryption, role-based access, and compliance reporting.

CNF.72	The ESB should support governance frameworks for managing service lifecycles, versioning, dependency management, and service-level agreements (SLAs).	Mandatory	+	Yes - the solution fully meets the requirement	Oracle Enterprise Manager and SOA Suite provide service lifecycle management, versioning, dependency tracking, and SLA monitoring.
1.3.2. Integration with other systems					
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	+	Yes - the solution fully meets the requirement	Oracle EBS will be integrated with the Lot-1 ESB using native support for SOAP/REST, XML, and event-driven architecture. Detailed integration approach will be defined during design phase.
CNF.74	The Tenderer must ensure interfacing with all the necessary interfaces through the integration component (Enterprise Service Bus).	Mandatory	+	Yes - the solution fully meets the requirement	All necessary interfaces between Oracle EBS and external systems will be implemented through the enterprise ESB, as required.
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	+	Yes - the solution fully meets the requirement	Oracle EBS interfaces use open standards (SOAP, REST, XML, WSDL). Any required adapters for NBM-specific systems will be built on these standards.
CNF.76	All interfaces of the provided application will be able to interact with external applications both in real time and offline.	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS supports both synchronous (real-time) and asynchronous (batch, file-based) interactions with external applications.
CNF.77	The interfaces of the provided application will allow loose coupling with external applications (communication based on messages).	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS interfaces are message-based (JMS, SOAP over HTTP), enabling loose coupling with external systems.
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	+	Yes - the solution fully meets the requirement	Oracle EBS provides standard APIs and web services for all key business functions (document generation, transaction creation, entity queries).
CNF.79	The application will have standard interfaces for data export within Data Warehouse tools.	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS includes standard interfaces (ODI, GoldenGate, SQL export) to extract data to Data Warehouse tools like Oracle Analytics or third-party BI platforms.
CNF.80	The solution will have convenient tools for the administrator to manage, control and monitor all external interfaces of the application.	Mandatory	+	Yes - the solution fully meets the requirement	Oracle Enterprise Manager and SOA Composer provide centralized management, control, and monitoring of all external interfaces.
CNF.81	All application interfaces must be properly documented (e.g. with the Web Services Description Language application).	Mandatory	+	Yes - the solution fully meets the requirement	All Oracle EBS interfaces are documented via WSDL (for web services) and API reference guides (for PL/SQL and Java).
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	+	Yes - the solution fully meets the requirement	Oracle Workflow and XML Publisher can generate email messages from predefined templates and send them via configured email servers.
1.4. Requirements for performance					
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	+	Yes - the solution fully meets the requirement	Oracle EBS is benchmarked to handle high transaction volumes typical of central banks. Performance meets NBM's volumetry (Annex 8).
1.4.1. General performance requirements					
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	+	Yes - the solution fully meets the requirement	Oracle EBS concurrent managers allow prioritization and separation of batch processes. Guidelines will be provided to avoid performance conflicts (e.g., not running heavy reports during end-of-day).
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	+	Yes - the solution fully meets the requirement	Oracle EBS separates reporting workload via read-only replicas or BI Server. Reports can be scheduled during low-activity periods to protect transaction processing.
CNF.86	The solution must retain all transactional and historical data for a minimum period of five years without compromising its performance.	Mandatory	+	Yes - the solution fully meets the requirement	Oracle Database supports partitioning, compression, and archiving to retain 5+ years of data without performance degradation.

CNF.87	Tenderers must specify minimum guaranteed performance values for the application, considering the recommended technological platform.	Mandatory	+	Yes - the solution fully meets the requirement	JMR will provide specific performance metrics (e.g., concurrent users, transaction throughput) based on NBM's recommended hardware during the design phase.
1.4.2. Specific performance requirements					
CNF.88	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. *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.*	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS, when properly sized, achieves sub-second response for online transactions. Compliance will be validated through performance tests agreed with NBM.
CNF.89	The application will have the ability to process transactions both in real time and batch.	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS supports real-time transactions via forms/web services and batch processing via concurrent managers and scheduled jobs.
1.5. Requirements for flexibility					
CNF.90	The application must possess the capability to adapt to evolving business needs over time.	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS is highly adaptable through configuration, extensions, and customizations without re-architecting the core system.
CNF.91	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. *Please provide tangible evidence and examples highlighting the application's configuration options and flexibility for configuration-based adaptations.*	Recommended	+	Yes - the solution fully meets the requirement	Many business changes (e.g., approval workflows, chart of accounts, reports) can be made via configuration. Examples: Workflow Builder, Flexfield configurations, BI Publisher templates.
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	+	Yes - the solution fully meets the requirement	Oracle EBS allows personalization of forms and creation of new user forms using OA Framework and Application Personalization.
CNF.93	The application will allow the customization of existing reports (e.g. data set adjustment, formatting).	Mandatory	+	Yes - the solution fully meets the requirement	Oracle BI Publisher and Oracle Reports allow full customization of existing reports (data set, formatting, layout).
CNF.94	The application will allow the definition of user reports (e.g. definition of data set, report format, definition of calculated fields).	Mandatory	+	Yes - the solution fully meets the requirement	Oracle BI Publisher and Discoverer allow end-users to define new reports by selecting data sets, formats, and calculated fields.
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	+	Yes - the solution fully meets the requirement	Oracle EBS can schedule reports to run on events or time intervals, store them, and email results to specified users.
CNF.96	The application will allow to define and customize the business entities stored in the application (e.g. defining new properties).	Recommended	+	Yes - the solution fully meets the requirement	Oracle EBS allows adding descriptive flexfields (user-defined attributes) to business entities without code changes.
CNF.97	The application will allow to define and customize the business rules implemented within the application.	Recommended	+	Yes - the solution fully meets the requirement	Business rules can be modified using Oracle Workflow, AME (Approval Management Engine), and configurable validation rules.
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	+	Yes - the solution fully meets the requirement	Oracle Workflow and BPM allow definition and customization of business flows, including status transitions, notifications, and roles.
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	+	Yes - the solution fully meets the requirement	Oracle EBS provides "Lookups" and "Reference Data" management with sources internal or external (via API or file import).
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	+	Yes - the solution fully meets the requirement	Oracle SOA Suite and API Gateway allow configuration of accessible functions, data formats, protocols, and access controls for external interfaces.
CNF.101	All application configurations must be able to be performed in convenient user interfaces for application administrators.	Mandatory	+	Yes - the solution fully meets the requirement	All configurations are performed through web-based administrator forms (e.g., System Administrator, Application Developer) with intuitive UI.
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	+	Yes - the solution fully meets the requirement	Oracle EBS allows NBM to develop custom components using Oracle's published frameworks (OAF, ADF, APIs) following provided methodology. Inheritance is supported.

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. 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.	Mandatory	+	Yes - the solution fully meets the requirement	
1.6. Requirements for maintainability					
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	+	Yes - the solution fully meets the requirement	Oracle EBS meets all sub-criteria: uniform platform (Oracle DB), single supplier, recommended single development environment (JDeveloper), robust monitoring (OEM).
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	+	Yes - the solution fully meets the requirement	The solution uses Oracle Database as single DBMS and a unified hardware/software stack, simplifying maintenance.
CNF.104 b.	All application modules within the proposed solution must be sourced from a single software supplier.	Mandatory	+	Yes - the solution fully meets the requirement	All application modules are sourced from Oracle via JMR, ensuring consistent support and updates.
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	+	Yes - the solution fully meets the requirement	Oracle recommends JDeveloper and SQL Developer for all EBS customizations, enabling standardized development and testing.
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	+	Yes - the solution fully meets the requirement	Oracle Enterprise Manager provides real-time monitoring, alerts, and diagnostic tools for root cause analysis.
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	+	Yes - the solution fully meets the requirement	Oracle EBS supports proactive problem detection (OEM metrics), preventive maintenance (scheduled jobs, alerts), comprehensive monitoring, and streamlined maintenance tasks.
CNF.105 a.	**Proactive Problem Identification**: The application must enable early detection of potential issues across all components, minimizing downtime and operational disruptions.	Mandatory		Yes - the solution fully meets the requirement	Oracle Enterprise Manager (OEM) provides proactive problem identification across all Oracle EBS components — database, application server, concurrent managers, and integrations. OEM metric thresholds trigger automated alerts before issues impact users, enabling early detection of CPU spikes, memory exhaustion, slow SQL, and disk space warnings.
CNF.105 b.	**Preventive Maintenance**: 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		Yes - the solution fully meets the requirement	Oracle EBS supports preventive maintenance through OEM-scheduled jobs including automated performance threshold alerts, scheduled data cleanup and archiving (ADADMIN), disk space monitoring, and automated backup verification via RMAN. Health checks and advisory reports (e.g., AWR, ADDM) proactively identify risks before they become incidents.
CNF.105 c.	**Comprehensive Monitoring**: 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		Yes - the solution fully meets the requirement	Oracle Enterprise Manager provides comprehensive real-time monitoring dashboards covering database performance, application server health, concurrent manager queues, memory/CPU utilization, and integration middleware. Custom metric extensions allow monitoring of business-critical processes specific to NBM's operations.
CNF.105 d.	**Ease of Maintenance**: Operational maintenance tasks must be streamlined, allowing administrators to quickly address performance bottlenecks, implement fixes, and perform routine updates with minimal effort;	Mandatory		Yes - the solution fully meets the requirement	Oracle EBS streamlines maintenance through OEM's one-click patching, automated job scheduling, and online patching (adop) that minimizes downtime. Administrators can resolve performance bottlenecks via OEM's guided workflow, apply patches using the dual file system, and execute routine maintenance tasks through a central web-based console.
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	+	Yes - the solution fully meets the requirement	Oracle Enterprise Manager provides granular monitoring of business logic layer components (WebLogic server pools, Concurrent Managers, SOA composites) and the data layer (Oracle Database, tablespace usage, wait events, query performance). Dashboards display real-time operational load and performance KPIs with drill-down to root cause.

CNF.107	The solution must provide self-diagnostic tools for monitoring the status of internal components and generate appropriate notifications.	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS includes built-in self-diagnostic capabilities through Oracle Diagnostics Framework, Health Monitor, and the Automated Diagnostic Repository (ADR). The system automatically detects and logs component health issues, generates incident reports, and notifies administrators via OEM alerts and email notifications. Diagnostic advisors (ADDM, SQL Advisor) provide actionable recommendations.
	These notifications must include actionable insights to address the issue promptly.				
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	+	Yes - the solution fully meets the requirement	Oracle EBS implements centralized exception management through Oracle Diagnostics Framework and the Concurrent Manager error logging system. All errors are categorized by severity (informational, warning, error, critical), stored in the ADR repository, and linked to automated escalation rules. Critical errors trigger immediate OEM alerts to designated administrators via configurable notification channels (email, SMS, pager).
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	+	Yes - the solution fully meets the requirement	JMR will deliver comprehensive technical documentation as part of project deliverables including: Technical Architecture Document, Installation Guide, Configuration and Operations Manual, DBA Administration Guide, System Administrator Guide, Developer's Handbook (covering OAF, APIs, customization framework), Integration Specifications, and a step-by-step guide for deploying NBM-developed components. All documentation will be maintained and updated with each patch cycle.
CNF.110	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.	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS's modular architecture ensures application-level changes have minimal blast radius. Customizations via OAF personalizations, Flexfields, or Workflow configurations are isolated from core code. Oracle's dual file system (adop) ensures that changes can be developed, tested in a patched environment, and promoted without disrupting production. The impact scope of any change is clearly identifiable through Oracle's dependency tracking and regression test frameworks.
	The Tenderers must demonstrate alignment with this requirement by providing:				
	- *A detailed description of the architectural design principles and methodologies employed to minimize the complexity of application-level changes.*				
	- *Examples of different categories of customizations supported by the solution, including scenarios involving integration, user interface updates, and data schema modifications.*				
	- *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.*				
CNF.111	The application will allow to define and run scheduled tasks for operational maintenance activities (e.g. archiving historical data).	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS Concurrent Manager provides a comprehensive scheduled task management framework. Administrators can define, schedule, and monitor concurrent programs for operational maintenance activities such as historical data archiving, purging of obsolete records, index rebuilds, statistics gathering, and log cleanup. All tasks have configurable schedules, priority levels, and notification rules.
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	+	Yes - the solution fully meets the requirement	Oracle EBS R12.2 uses the Online Patching (adop) framework with a dual file system, allowing Oracle-delivered patches and new versions to be applied without disrupting production.
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	+	Partially yes - The solution partially meets the requirement	JMR confirms that NBM will have access to at least two Oracle-certified implementation and support partners capable of providing independent maintenance services for Oracle EBS.
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	+	Yes - the solution fully meets the requirement	Oracle EBS supports standardized environment cloning through Oracle's RMAN-based refresh procedures and adcfgclone scripts. The solution can be ported from production to test, development, or training environments with documented, repeatable procedures. JMR will provide a step-by-step Environment Management Guide covering all required configurations, dependency management, connection string updates, and post-clone validation steps to ensure error-free transitions between environments.

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	+		
1.7. Requirements towards scalability					
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	+	Yes - the solution fully meets the requirement	Oracle EBS is designed for elastic scalability, supporting both scale-up (additional CPU/RAM) and scale-down without application changes. Application server tiers can be added or removed without downtime. Database partitioning and compression ensure performance is maintained as transaction volumes fluctuate over time.
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	+	Yes - the solution fully meets the requirement	Oracle EBS supports horizontal expansion through addition of application server nodes behind an Oracle HTTP Server or third-party load balancer, without any application downtime using the rolling restart capability.
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	+	Yes - the solution fully meets the requirement	Oracle WebLogic Server supports dynamic clustering with automatic workload distribution. Oracle RAC provides automatic load rebalancing across database nodes. Oracle EBS Concurrent Manager supports priority-based workload distribution. While full auto-scaling at the application tier requires integration with cloud orchestration tools (e.g., Oracle Cloud, VMware), JMR will implement automated scaling scripts and thresholds appropriate to NBM's infrastructure environment.
1.8. Requirements for usability					
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	+	Yes - the solution fully meets the requirement	Oracle EBS is designed with user-friendliness as a core principle. Online help is available in every form. JMR's training programme ensures end-users are productive quickly, supplemented by quick reference guides and e-learning materials tailored to each role.
CNF.120	All business functions accessible to application users must be accessed through graphical user interfaces.	Mandatory	+	Yes - the solution fully meets the requirement	All Oracle EBS business functions are accessible exclusively through graphical user interfaces — either through the browser-based Oracle Applications Framework (OAF) forms or the Oracle Forms client. There are no command-line-only business functions exposed to end users. All transactions, approvals, reports, and administrative tasks are performed through the GUI.
CNF.121	The application documentation must contain complete, detailed and updated guides for all user groups.	Mandatory	+	Yes - the solution fully meets the requirement	JMR will deliver complete user documentation for all user groups as part of the project: End-User Guides per module (GL, AP, AR, FA, PO, INV, HR, Payroll), Manager/Approver Guides, System Administrator Guide, Report User Guide, and Super User Reference Manuals. All guides will be in Romanian and English, kept up to date with each system change, and accessible from within the application.
CNF.122	Application users will have access to context-sensitive help in all application interfaces.	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS provides context-sensitive online help accessible from every form and page via the 'Help' menu or F1 key. Help content covers field-level descriptions, procedure guides, and error message explanations. JMR will customize the online help content to reflect NBM-specific configurations and business processes, ensuring users always have access to relevant, accurate guidance.
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	+	Yes - the solution fully meets the requirement	
CNF.124	Users must be able to access all authorized functions through a unified graphical interface, ensuring streamlined navigation and task execution.	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS provides a unified Navigator interface through which all authorized functions are accessed from a single entry point. Role-based menus and responsibilities ensure each user sees only the functions they are authorized to use. The Home Page dashboard aggregates tasks, notifications, and shortcuts. Users navigate seamlessly between modules without re-authentication (SSO).
CNF.125	The application must feature user interfaces that are intuitive, visually appealing, and ergonomically designed for both business users and administrative roles.	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS's OAF-based interfaces follow Oracle's Human Interface Guidelines, delivering visually consistent, ergonomically designed forms for both business and administrative users. Consistent layout, colour coding, icon usage, and navigation patterns reduce cognitive load. JMR will apply Oracle's standard branding/theming to align with NBM's corporate style guide where applicable.
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	+	Yes - the solution fully meets the requirement	Oracle EBS implements auto-save and draft-save mechanisms across key transaction forms. Long-running transactions (e.g., Purchase Orders, GL Journals) can be saved as incomplete and resumed later. Oracle Workflow-based processes maintain state throughout multi-step approval flows. Users are prompted to save before navigating away from unsaved changes, preventing data loss.
CNF.127	All user interfaces must be in Romanian and English languages.	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS supports Romanian and English languages natively through Oracle National Language Support (NLS). The NLS framework supports switching between languages at the user profile level without system restart. All menus, labels, messages, and help text can be translated. JMR will configure and validate Romanian language packs as part of the implementation, ensuring NBM's regulatory and operational terminology is correctly translated throughout.

CNF.128	The translation must ensure uniform use of specific terms used in the application (e.g. Delete = Eliminare) across all interfaces.	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS NLS translation ensures uniform use of application-specific terminology across all interfaces. During implementation, JMR will conduct a terminology review with NBM to standardize all translated terms (e.g., Delete = Ștergere, Approve = Aprobare) and apply them consistently across all menus, labels, error messages, and reports using Oracle's translation management tools.
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	+	Yes - the solution fully meets the requirement	Oracle EBS employs a consistent graphical design language across all modules — uniform navigation bars, consistent form layouts, standardized button placement, and coherent iconography.
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	+	Yes - the solution fully meets the requirement	Oracle EBS allows users to personalize their workspace through: adding functions to Navigator Favorites, configuring the Home Page with preferred dashboards and recently accessed items, saving parameterized searches as 'Saved Searches,' and customizing report parameters. The Oracle Personalization framework stores individual user preferences persistently across sessions.
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	+	Yes - the solution fully meets the requirement	Oracle EBS interfaces support comprehensive keyboard and mouse navigation. All forms are fully navigable via keyboard (Tab, arrow keys, function keys), with configurable shortcuts for frequently used actions. The Oracle Forms support screen reader compatibility for accessibility. Customizable toolbars and function-key bindings allow users to optimize navigation for their specific workflows.
CNF.132	The application must generate notifications to alert users about actions that require their attention, such as transaction authorizations or pending approvals.	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS generates workflow notifications for all actions requiring user attention — transaction approvals, pending authorizations, error alerts, and status changes. Notifications appear in the Worklist (accessible from the Home Page Navigator), in-application notification banners, and via email through Oracle Workflow Mailer. Real-time notification counts are displayed on the user's home page.
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	+	Yes - the solution fully meets the requirement	Oracle EBS notification messages contain actionable links that open the relevant transaction or approval form directly, eliminating the need to navigate manually. Workflow notifications include the full transaction context (amount, requester, description) and action buttons (Approve/Reject) embedded directly in the email or worklist item, enabling one-click responses without navigating to the application.
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	+	Yes - the solution fully meets the requirement	Oracle EBS provides a centralized Home Page dashboard configured per role that displays: pending approvals (Worklist), notifications, recently accessed items, favorite functions, and KPI metrics. The Home Page aggregates all user-specific tasks from across modules into a single view, ensuring nothing is missed. JMR will configure role-specific dashboards for NBM's key user groups during implementation.
1.9. Requirements for information security					
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	+	Yes - the solution fully meets the requirement	Oracle EBS provides a comprehensive security framework aligned with industry best practices and NBM's security policies. Security controls span all layers, application, data, and infrastructure
CNF.136	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.	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS implements a multi-layered security architecture: (1) Application Layer — RBAC, function/data security, AME approval controls; (2) Network Layer. JMR will provide a detailed ISO 27001 security checklist mapping Oracle EBS controls to each relevant standard control as part of the Security Architecture Document delivered during the design phase.
	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.				
CNF.137	The security subsystem of the proposed solution must achieve the following critical objectives:	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS's security subsystem addresses all critical objectives: (1) Confidentiality, Integrity, Authenticity, TDE encryption at rest, SSL/TLS in transit, non-repudiation through audit trails; (2) Access Control, fine-grained function and data security, Oracle Database Vault; (3) Role-Based Access, granular responsibility-level and menu-level permissions; (4) Critical Activity Monitoring (5) Data Protection, Oracle Label Security, data masking/redaction, and RMAN-backed integrity controls.
	- ***Confidentiality, Integrity, and Authenticity*** : Ensuring that information remains secure during processing, storage, or transmission, and maintaining non-repudiation for transmitted data.				
	- ***Access Control*** : Preventing unauthorized access to data and providing fine-grained access controls for system resources.				
	- ***Role-Based Access*** : Enabling differentiated access levels (viewing, printing, copying, modifying, etc.) based on user roles.				

	- ***Critical Activity Monitoring*** : Logging and monitoring of critical system-level activities with real-time alerts for anomalies.				
	- ***Data Protection*** : Preventing the loss, unauthorized modification, or misuse of information stored or processed within the application.				
1.9.1. Security architecture					
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	+	Yes - the solution fully meets the requirement	Oracle EBS is developed following Oracle's Secure Development Lifecycle (SDL), which integrates security at every stage of development. The framework includes threat modelling, secure coding standards (OWASP-aligned), mandatory security code reviews, penetration testing, and automated vulnerability scanning. Oracle's quarterly Critical Patch Updates (CPU) address newly discovered vulnerabilities systematically. JMR's implementation follows Oracle's security hardening guides for all deployed components.
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	+	Yes - the solution fully meets the requirement	JMR will deliver a comprehensive Security Architecture Document as part of the project deliverables. This document will cover: the complete security model and its components, authentication mechanisms, authorization model, encryption implementation, audit trail architecture, intrusion detection integration points, and a security component relationship diagram. The document will be maintained and updated throughout the contract period.
	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.				
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	+	Yes - the solution fully meets the requirement	JMR will deliver a Network Placement and Communication Matrix document as part of the technical documentation. This document will specify the network zones for each Oracle EBS component (web tier, application tier, database tier, SOA tier) and NBM's recommended network access control rules for secure deployment. The document will be aligned with NBM's network security policies and reviewed with NBM's security team during the design phase.
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	+	Yes - the solution fully meets the requirement	Oracle EBS follows the principle of least privilege across all system processes. Database schemas use minimum required privileges (no DBA grants to application schemas). OS processes run under dedicated service accounts with restricted permissions. Application server processes have only the rights required to serve their function. Oracle Database Vault enforces command rules to prevent even privileged users from accessing application data outside defined paths.
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	+	Yes - the solution fully meets the requirement	Oracle EBS has no hard-coded credentials in application code or configuration files. All access credentials (database passwords, service account passwords, API keys) are stored in encrypted Oracle Wallet or configured and managed exclusively through Oracle EBS System Administrator interfaces.
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	+	Yes - the solution fully meets the requirement	Oracle EBS prohibits storage of plaintext credentials at any application layer. Database passwords are managed through Oracle Wallet with auto-login capability, preventing plaintext storage. Application connection pools use encrypted credential stores. Access to credential management is restricted to authorized DBAs and System Administrators through Oracle Enterprise Manager.
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	+	Yes - the solution fully meets the requirement	Oracle EBS supports integration with advanced electronic signature mechanisms through Oracle XML Gateway and third-party e-signature providers. JMR will integrate Oracle EBS with the qualified electronic signature infrastructure applicable in the Republic of Moldova, ensuring compliance with applicable legislation. Document approval workflows in Oracle EBS can be configured to require qualified electronic signature at defined workflow steps, with cryptographic verification of signature authenticity.
CNF.145	All external interfaces of the application will be accessed with the application of secure authentification methods (e.g. X.509 certificates).	Mandatory	+	Yes - the solution fully meets the requirement	All external Oracle EBS interfaces use secure authentication methods and Web service interfaces require mutual SSL/TLS authentication using X.509 certificates.
1.9.2. Identification and Authentification Requirements					
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:	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS integrates natively with Microsoft Active Directory via Oracle Internet Directory (OID) synchronization using LDAP protocol. User profiles and attributes (ID, name, surname, email, department) are imported from AD and kept synchronized. Administrators can browse and select users from AD when creating Oracle EBS accounts. Single Sign-On is achieved through Oracle Access Manager's AD integration, eliminating the need for separate Oracle EBS passwords for AD-authenticated users.
	- 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.				

CNF.147	The application must support multifactor authentication (MFA) for user access.	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS supports multi-factor authentication (MFA) through Oracle Access Manager (OAM) integration. OAM supports TOTP (Time-based One-Time Passwords), hardware tokens (RSA SecurID), software tokens, SMS OTP, and push notifications as second factors. MFA policies can be applied selectively by user group, role, IP range, or risk score — for example, requiring MFA for privileged users, remote access, or access to sensitive financial data.
CNF.148	Passwords must be securely stored within the application using industry-standard encryption and protection techniques to prevent interception, deduction, or recovery.	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS stores all passwords using industry-standard one-way cryptographic hashing (SHA-256 or higher) with salting, ensuring passwords cannot be recovered in plaintext. Passwords are never transmitted in cleartext — all authentication exchanges occur over encrypted channels (SSL/TLS). Oracle Access Manager enforces additional credential protection through secure token management and encrypted session cookies.
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	+	Yes - the solution fully meets the requirement	Oracle EBS provides comprehensive password policy enforcement through Oracle User Management (UMX) and Oracle Access Manager, including: configurable complexity requirements (length, character sets), mandatory periodic password changes, configurable expiration intervals, prevention of password reuse (configurable history depth), lockout after configurable number of failed attempts, a configurable dictionary of forbidden passwords, and proactive email/notification alerts to users regarding upcoming password expiration.
	- Password complexity requirements.				
	- Mandatory password changes and expiration policies.				
	- Prevention of password reuse.				
	- Configurable limits for failed authentication attempts.				
	- A dictionary of forbidden passwords.				
	- User notifications regarding password expiration.				
CNF.150	The application must allow administrators to configure differentiated password policies for specific user groups.	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS allows differentiated password policies to be defined for specific user groups or responsibilities. Through Oracle User Management and Oracle Access Manager, administrators can define separate policy profiles for standard users, privileged users, external users, and service accounts — applying different complexity, expiry, and lockout rules as appropriate for each group's risk profile.
CNF.151	For users not integrated with the centralized authentication mechanism, the application must:	Mandatory	+	Yes - the solution fully meets the requirement	For users not integrated with AD/LDAP, Oracle EBS provides: (1) self-service password change via the Oracle EBS login page and Self-Service HR; (2) administrator-initiated account blocking, deactivation, or suspension through the System Administrator responsibility; (3) automated account suspension after configurable inactivity periods; and (4) audit trail recording of all account status changes with timestamps and responsible administrator identity.
	- Allow password changes via the user interface.				
	- Support blocking, deactivating, or suspending user accounts at the application level.				
CNF.152	The application must provide session management controls, including:	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS provides session management controls through Oracle Access Manager and Oracle EBS System Administrator: (1) configurable maximum concurrent sessions per user; (2) configurable session timeout for inactivity (ICX: Session Timeout profile option); (3) prevention of session hijacking through encrypted session tokens and IP-binding options; (4) forced session termination by administrators in real time; and (5) audit logging of all session events.
	- Configuring the maximum number of simultaneous sessions per user.				
	- Setting session expiration times for inactivity.				
	- Mechanisms to prevent unauthorized access to active sessions.				
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	+	Yes - the solution fully meets the requirement	Oracle EBS supports integration with NBM's IAM systems using SAML 2.0, OAuth 2.0, and LDAP. MFA methods supported include user credentials, X.509 digital certificates, TOTP/OTP, RSA tokens, and hardware/software tokens. JMR will implement integration with the relevant authentication service using the SAML 2.0 protocol as explicitly required. The authentication framework is extensible to accommodate future standards and methods through OAM's pluggable authentication provider architecture.
	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.				
	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.				

CNF.154	The application must support Single Sign-On (SSO) mechanisms using Kerberos.	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS supports Single Sign-On using Kerberos through Oracle Access Manager's built-in Kerberos authentication provider. When configured, users authenticated to the NBM Windows/AD domain are automatically authenticated to Oracle EBS without re-entering credentials (transparent SSO).
1.9.3. Authorization					
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	+	Yes - the solution fully meets the requirement	Oracle EBS provides granular access right management for all application objects through Oracle Function Security (menu and function-level access) and Oracle Data Security (data-level row and column access). Administrators can configure access rights for business entities, their properties, forms, menus, reports, and CRUD operations at the responsibility, role, user group, or individual user level. Oracle User Management (UMX) provides a centralized interface for all access right administration.
CNF.156	The authorization model must follow the principle of "default deny," meaning all actions are prohibited unless explicitly permitted.	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS's security model defaults to deny-all — users have no access to any function or data unless explicitly granted through an assigned responsibility or role. This is enforced at the menu level (Function Security), data level (Data Security), and Oracle Database level (Row-Level Security / Oracle Label Security). No implicit or inherited access is granted without explicit administrator action.
CNF.157	The application must support the creation of user groups and roles and the assignment of users to these groups and roles.	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS supports the creation of user groups and roles through Oracle User Management (UMX). Users are assigned to responsibilities (roles) which encapsulate sets of functions and data access rights. Multiple responsibilities can be assigned to a single user. User groups can be defined for bulk responsibility assignment, simplifying administration for large user populations with similar access profiles.
CNF.158	The application must allow:	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS supports: (1) granting access rights at individual user, group, and role level; (2) role hierarchies with sub-roles and inherited permissions; (3) assignment of multiple responsibilities/roles to a single user, with access being the union of all assigned permissions; (4) configurable conflict detection to identify SoD violations when users accumulate incompatible access rights across multiple roles.
	- Granting access rights at the level of individual users, user groups, and roles.				
	- Defining groups that can include subgroups or roles.				
	- Associating a user with multiple groups and roles, with cumulative access rights derived from all associations.				
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	+	Yes - the solution fully meets the requirement	Oracle EBS supports business rule-based access through Oracle Approvals Management Engine (AME) and Oracle Data Security. Examples: a GL journal can only be modified by its creator before posting; a purchase order can only be approved within the approver's authority limit; document access can be restricted to a defined business unit or cost centre. These context-sensitive rules are configured through AME and Oracle Data Security without custom code.
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	+	Yes - the solution fully meets the requirement	Oracle EBS supports temporary delegation of user responsibilities. A user can delegate their approval authority (with or without retaining their own rights) for a defined period (e.g., during leave). Delegation rules specify the delegating user, the delegate, the scope of delegated functions, and the validity period. All delegated actions are recorded in the audit trail with the original authority clearly identified.
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	+	Yes - the solution fully meets the requirement	Oracle EBS supports segregation of administrative duties through Oracle Database Vault's multi-person authorization (MPA) feature, which requires approval from a second administrator before sensitive configuration changes take effect. Oracle's Separation of Duty controls also prevent the same user from both creating and approving transactions. JMR will configure appropriate administrative SoD controls as part of the security design phase.
CNF.162	The application must provide views and reports on existing access rights. These reports should be customizable at least based on the following parameters:	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS provides comprehensive access rights reporting. Reports are fully customizable and filterable by: user ID, assigned groups/roles, account status, access grant date and history, business entities with access, permitted operations (CRUD), delegation records, inactive/expired rights, and SoD conflicts. Reports can be exported in CSV, PDF, and Excel formats. AACG provides visual dashboards of access rights by user group and business entity.
	- User Information:				
	o Individual user ID.				
	o User group(s) or role(s) assigned to the user.				
	o Current status of the user (e.g., active, suspended, deactivated).				
	o The date and time when the user was granted access to specific resources or operations.				
	o History of access rights changes for the user, including timestamps and the administrators who made the changes.				
	- Access Rights Context:				
	o Business entities to which access has been granted.				
	o Properties of the business entities for which access is allowed.				
	o The specific operations allowed (e.g., create, read, update, delete).				

	- Advanced Options:				
	o Access rights granted by specific administrators or based on defined business rules.				
	o Resources or operations assigned to groups or roles but not directly to individual users.				
	o Delegation records, specifying delegated access rights, delegating users, recipients, and the duration of delegation.				
	o Inactive or expired access rights, including reasons for revocation or expiration (e.g., policy change, role reassignment).				
	o Anomalous or conflicting access rights (e.g., overlapping roles with conflicting permissions).				
	- Customizable Report Outputs:				
	o Ability to filter, sort, and export data in various formats (e.g., CSV, PDF).				
	o Visual representations (e.g., charts, graphs) of access rights by user group, business entity, or allowed operations.				
1.9.4. Input and output data validation					
CNF.163	The application must implement robust mechanisms to validate and sanitize all input data, including:	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS implements multi-layer input validation and sanitization: (1) OAF/Forms presentation layer validates format, type, and range before submission; (2) PL/SQL business logic layer validates against business rules and database constraints; (3) all API inputs are validated against schema definitions. Inputs from external interfaces are validated through Oracle SOA Suite's input validation policies. All rejected or invalid inputs are logged in the Oracle EBS exception tables with timestamp, source, user, and rejection reason for audit purposes.
	- User-provided input (e.g., form submissions, uploaded files).				
	- Inputs from external applications or interfaces.				
	- Input validation techniques, such as pattern matching, or schema validation, to prevent unauthorized manipulation of data.				
	- Logging of rejected or invalid inputs for auditing purposes, including timestamps, the source of the input, and details about the invalid data.				
CNF.164	The interfaces with SWIFT must comply with the minimum-security requirements defined in the "Customer Security Program" document. This includes at least:	Mandatory	+	Yes - the solution fully meets the requirement	JMR will implement Oracle EBS's SWIFT interface in full compliance with SWIFT's Customer Security Programme (CSP). The integration will implement the LAU (Local Authentication) mechanism using HMAC-SHA256 for message integrity and authenticity verification on all inbound and outbound SWIFT messages. All SWIFT data exchange activities are logged with full details (timestamp, message reference, source, destination, LAU validation result) in Oracle EBS audit tables and SWIFT's own Alliance Access logs.
	- 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.				
	- Logging all data exchange activities with SWIFT, including timestamps, source, destination, and security validations performed.				
CNF.165	The application must perform complete and independent data validation at all levels to ensure data integrity, completeness, and correctness:	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS implements independent, complete data validation at all three layers: (1) Presentation Layer — client-side validation (OAF validators, Forms triggers) for format, range, and mandatory field checks, with no sole reliance on client-side validation; (2) Business Logic Layer — PL/SQL and Java validation of business rules, workflow state, and cross-field consistency; (3) Data Layer — Oracle database constraints (NOT NULL, CHECK, FOREIGN KEY, UNIQUE) enforce data integrity at the lowest level. All detected validation errors are logged with source, type, timestamp, and corrective action for audit purposes.
	- ***Presentation Layer:*** Validating user inputs on the client side (e.g., using front-end validation techniques) while ensuring no reliance solely on client-side validation.				
	- ***Business Logic Layer:*** Validating business rules, workflows, and logic to ensure compliance with requirements.				
	- ***Data Layer:*** Validating database constraints, relationships, and data formats to detect corruption or anomalies.				
	Mechanisms must log detected validation errors, their sources, and the corrective actions taken for audit purposes.				
	All information displayed within the application must comply with the NBM's information security policies and include:			Yes - the solution fully meets the requirement	Oracle EBS supports information security classification markings through Oracle Label Security (OLS), which allows data to be tagged with security labels based on a configurable classification scheme. Visibility rules for security markings are configurable based on user roles, clearance levels, and data sensitivity. Changes to classification policies and labels are tracked in the Oracle Audit Vault audit trail.

CNF.166	- Security markings based on a predefined classifier established within the application.	Recommended	+		
	- Configurable visibility rules for security markings, based on user roles or permissions.				
	- Audit trails for changes made to the security marking policies or classifiers.				
CNF.167	Confidential data must never be stored or accessed insecurely within the application. This includes:	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS enforces strict controls on confidential data storage: sensitive data is never written to log files or temporary tables in plaintext. Oracle Transparent Data Encryption (TDE) encrypts all data at rest including backups and archived logs. Oracle Data Masking and Redaction masks sensitive data in non-production environments. Access failures to confidential data (e.g., unauthorized query attempts) are logged by Oracle Audit Vault with user identity, timestamp, and reason. Oracle Database Vault prevents even privileged DBAs from viewing application data outside sanctioned paths.
	- Prohibiting storage of sensitive data in unprotected locations such as log files, caching mechanisms, or temporary files.				
	- Logging instances where attempts to access confidential data fail, including the user, timestamp, and reason for failure.				
	- Enforcing encryption for all stored sensitive data and secure wiping techniques for deleted confidential data.				
CNF.168	The application must provide additional protection mechanisms for highly confidential data, including:	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS provides multiple layers of protection for highly confidential data: (1) masked display of sensitive fields (e.g., bank account numbers shown as ****1234) using Oracle Data Redaction; (2) AES-256 encryption at rest (TDE) and TLS 1.2/1.3 in transit; (3) step-up authentication (MFA re-prompt) for access to highly sensitive functions configured via Oracle Access Manager; (4) comprehensive access logging through Oracle Audit Vault capturing user identity, operation, timestamp, and business justification for every access to classified data.
	- Masked display of sensitive data (e.g., showing only partial information like "****1234").				
	- Encryption of highly confidential data both in transit and at rest, using industry-standard encryption algorithms (e.g., AES-256).				
	- Requiring repeated or stronger authentication methods (e.g., multi-factor authentication) for accessing or modifying highly confidential data.				
	- Logging access to highly confidential data, including user identity, operation performed, timestamp, and justification for access.				
CNF.169	The application must implement routine procedures for verifying and detecting possible corruption of data integrity relationships, including:	Recommended	+	Yes - the solution fully meets the requirement	Oracle EBS includes database integrity verification through Oracle's built-in constraint validation, Oracle Health Monitor, and RMAN's block media recovery. Scheduled Oracle DBMS_REPAIR jobs identify and correct data block corruptions. Oracle Audit Vault logs all detected integrity anomalies, corrective actions taken, and the administrators involved, providing a complete integrity audit history.
	- Integrity checks using cryptographic methods (e.g., hash-based checksums) to detect unauthorized modifications.				
	- Scheduled audits of data integrity relationships, including database constraints, dependencies, and foreign key relationships.				
	- Logging detected anomalies, corrective actions taken, and the administrators involved in the process.				
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	+	Yes - the solution fully meets the requirement	Oracle EBS includes Oracle Audit Vault and Database Firewall (AVDF) as the enterprise auditing component, providing centralized collection, storage, and management of all application-level audit records. Audit Vault is architected for high availability with clustered audit servers and redundant storage. All audit data is stored in a tamper-evident, encrypted audit repository independent of the application database, ensuring availability even during application incidents.
CNF.171	The auditing component must allow granular configuration of auditing policies, enabling customization at various levels such as:	Mandatory	+	Yes - the solution fully meets the requirement	Oracle Audit Vault provides granular auditing policy configuration by: user groups and individual users, specific database objects and business entities, event types (login, data access, modification, deletion, privilege use), and defined time intervals. Policies can be applied selectively to critical users (privileged accounts, external users) or sensitive entities (financial tables, HR data) without generating excessive audit volume for low-risk activities.
	- User groups, individual users, or roles.				
	- Specific objects or business entities.				
	- Events and event types.				
	- Time intervals or specific time frames for monitoring activities.				

CNF.172	Auditing policies must be configurable at the level of:	Mandatory	+	Yes - the solution fully meets the requirement	Oracle Audit Vault auditing policies cover: (1) Object/Entity level — DDL/DML on critical tables (GL_JE_LINES, AP_INVOICES, PO_HEADERS, HR_EMPLOYEES), privilege grants, schema changes; (2) Event level — login attempts (successful and failed), data modifications, access to confidential information (salary, payment details), security policy changes, user account modifications, and SoD violations flagged by AACG.
	- ***Objects or Business Entities:*** Tracking interactions with critical application objects or sensitive entities.				
	- ***Events:*** Recording actions such as login attempts, data modifications, access to confidential information, and security policy changes.				
CNF.173	The application must allow defining specific characteristics of events to be recorded, such as:	Recommended	+	Yes - the solution fully meets the requirement	Oracle Audit Vault supports condition-based audit policy definitions including: activity within specific time intervals (e.g., after-hours access), events involving specific property values (e.g., transactions above threshold amounts), changes to sensitive fields (e.g., bank account number modifications), and user-initiated vs. system-generated actions. These fine-grained conditions are configured through Oracle Audit Vault's policy management interface.
	- 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.				
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	+	Yes - the solution fully meets the requirement	Oracle Audit Vault provides comprehensive event coverage across all Oracle EBS application layers and the underlying Oracle Database. All CRUD operations, authentication events, privilege exercises, configuration changes, and security policy modifications are capturable. Audit policies can be extended to cover custom-developed NBM components through Oracle's Unified Auditing framework, ensuring no gaps in audit coverage for any application object or business entity.
CNF.175	Each auditing record must contain at least the following information:	Mandatory	+	Yes - the solution fully meets the requirement	Each Oracle Audit Vault audit record contains: (1) Timestamp — microsecond-precision event time synchronized with NTP; (2) Subject — authenticated user ID or system process name; (3) Affected object — table, view, or business entity name and record identifier; (4) Event description — action performed (SELECT/INSERT/UPDATE/DELETE/LOGIN/LOGOFF/DDL); (5) Source identification — client IP address, OS username, client program name; (6) Additional context — session ID, SQL statement text, module name, and associated workflow instance where applicable.
	- ***Timestamp:*** Exact time and date of the event, synchronized with the system clock.				
	- ***Subject of the Event:*** User ID or system process that triggered the event.				
	- ***Affected Business Object or Entity:*** Clearly identify the resource or data impacted.				
	- ***Event Description:*** The nature of the event (e.g., data access, modification, deletion).				
	- ***Source Identification:*** IP address or other relevant identifiers to trace the origin of the event.				
	- ***Additional Context (if applicable):*** Such as session ID or associated workflows for comprehensive traceability.				
CNF.176	Auditing records will not contain confidential business information (e.g. passwords entered in failed attempts).	Mandatory	+	Yes - the solution fully meets the requirement	Yes - the solution fully meets the requirement
CNF.177	Errors that may occur when fixing auditing records should not affect the normal operation of the application.	Mandatory	+	Yes - the solution fully meets the requirement	Oracle Audit Vault is architected so that audit record failures do not affect normal application operation. The auditing subsystem runs independently in a separate process, and audit write failures (e.g., due to storage issues) are handled gracefully — the application transaction completes normally, and the audit failure is flagged as a system alert for administrator attention. This ensures business continuity is not impacted by audit infrastructure issues.
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	+	Yes - the solution fully meets the requirement	Oracle Audit Vault's audit timestamps are derived from the underlying OS system clock and are enforced to be synchronized with NTP (Network Time Protocol). Oracle EBS and Oracle Database both enforce NTP-based clock synchronization. Audit Vault handles timezone conversions and daylight saving time automatically, storing all timestamps in UTC internally with configurable display timezone per audit report consumer.
CNF.179	The auditing component must include an archiving mechanism to manage historical auditing records, which should be configurable with options for:	Mandatory	+	Yes - the solution fully meets the requirement	Oracle Audit Vault includes a built-in archiving framework configurable with: frequency (daily/weekly/monthly), age-based retention thresholds, output formats (CSV, XML, compressed binary), and storage destinations (local disk, NAS, remote object storage). Archived audit data remains queryable through Audit Vault's historical analysis interface without requiring restoration. Retention policies can be configured per data classification to meet NBM's compliance requirements (minimum 5-year retention for financial audit data).

	- 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	+	Yes - the solution fully meets the requirement	Oracle Audit Vault and OEM support automated security event notifications based on configurable thresholds. Notification triggers can be defined for: failed login threshold breaches, after-hours privileged access, bulk data access patterns, SoD violations, and security policy changes. Notifications include full event details (type, timestamp, user, affected object, source IP) and recommended actions. Delivery channels include email, SMS (via OEM or SIEM integration), and dashboard alerts, all configurable per event category.
	- 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	+	Yes - the solution fully meets the requirement	Oracle Audit Vault supports integration with SIEM solutions through Syslog (UDP/TCP), Oracle Database dblink, and REST API interfaces. Audit records are transmitted to SIEM platforms (e.g., IBM QRadar, Splunk, ArcSight) in real-time or batch mode using configurable transfer schedules. All transmissions are encrypted (TLS). Oracle Audit Vault is compatible with Common Event Format (CEF) and supports standard Syslog formats for SIEM compatibility.
	- 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	+	Yes - the solution fully meets the requirement	Oracle EBS supports historical data versioning through Oracle Flashback Technology (Flashback Query, Flashback Table, Flashback Archive) which preserves all historical versions of sensitive data records for configurable retention periods. For application-level versioning, Oracle EBS's standard 'WHO columns' (CREATED_BY, CREATION_DATE, LAST_UPDATED_BY, LAST_UPDATE_DATE) provide a full change history for every transaction record. Extended versioning for designated sensitive data will be implemented using Oracle Flashback Data Archive.
CNF.183	The solution must provide user-friendly tools for managing and analyzing auditing records, including:	Recommended	+	Yes - the solution fully meets the requirement	Oracle Audit Vault provides user-friendly audit management tools including: a web-based Audit Vault console with advanced filtering by any field (user, timestamp, event type, object, IP address); full-text search across audit records; export to CSV, PDF, and Excel; graphical reports and trend charts by user, entity, and event type; and import of historical archived audit files for retrospective analysis. Non-technical audit officers can perform complex queries through the visual query builder without SQL knowledge.
	- 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	+	Yes - the solution fully meets the requirement	Oracle Audit Vault enforces strict access controls on audit records: audit data is stored in a separate, hardened Audit Vault Server database with its own access control model independent of the application database. DBA accounts on the production database cannot access or modify audit records. Access to audit reports is granted only to designated audit administrators through Oracle Audit Vault's role-based console access. All access to the audit console is itself audited, creating a tamper-evident chain of custody.
1.9.6. Exception handling					
CNF.185	The application must handle all errors and exceptions that arise during its operation. Exception handling mechanisms should ensure:	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS implements comprehensive exception handling at all layers: Oracle Database exception handlers (EXCEPTION blocks in PL/SQL) capture and log all runtime errors; Oracle WebLogic Server captures application-tier exceptions with full stack traces in the Oracle Diagnostic Repository (ADR); the OAF presentation layer provides user-friendly error messages with error codes while suppressing technical details. Fallback mechanisms (e.g., retry logic, graceful degradation) are implemented at critical transaction points to maintain user experience during transient errors.
	- Detection of system crashes or instability.				
	- Logging of all relevant details for diagnostics.				
	- Activating fallback mechanisms to maintain user experience where possible (e.g. avoiding sudden interruptions or confusing error messages).				

CNF.186	The application must centrally record all exceptions and errors, storing them in a secure, centralized logging repository. The logging system must:	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS uses the Automated Diagnostic Repository (ADR) as a centralized, secure logging repository for all exceptions and errors. ADR stores incidents with full detail: timestamp, user ID, affected module, error code, stack trace, and system state at time of error. The ADR supports SQL-based filtering and querying for diagnostics. Access to ADR is restricted to DBAs and System Administrators. Logs are protected against unauthorized access through Oracle Database security controls and OS file permissions.
	- Include detailed information such as timestamps, user ID (if applicable), affected modules, and a description of the error.				
	- Support filtering and querying to facilitate diagnostics.				
	- Ensure logs are protected against unauthorized access or tampering.				
CNF.187	When an error occurs, the application must display a generic and user-friendly error message. The error message must:	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS displays standardized, user-friendly error messages that: avoid revealing technical system details or stack traces to end users; include a unique Oracle error code (e.g., APP-FND-01000) and an application-specific error reference number for support ticket correlation; provide clear guidance to the user on corrective actions (e.g., 'Please contact your system administrator with reference number XXXX'); and can be customized to NBM's support contact details through Oracle's message dictionary.
	- Avoid revealing sensitive system details.				
	- Include an error code and a unique error identifier for troubleshooting.				
	- Offer guidance to the user, such as suggesting possible corrective actions or directing them to support channels.				
CNF.188	The application must centrally record all exceptions and errors, storing them in a secure, centralized logging repository. The logging system must:	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS implements centralized exception logging through the Oracle Diagnostic Repository (ADR) and application-level error tables (FND_LOG_MESSAGES, FND_CONCURRENT_REQUESTS). The ADR provides a unified logging infrastructure across all Oracle components (database, application server, Oracle Net). The logging system supports full-text filtering, query by module/severity/time range, and integration with OEM for automated alert escalation. Logs are protected by Oracle Database access controls.
	- Include detailed information such as timestamps, user ID (if applicable), affected modules, and a description of the error.				
	- Support filtering and querying to facilitate diagnostics.				
	- Ensure logs are protected against unauthorized access or tampering.				
CNF.189	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:	Recommended	+	Yes - the solution fully meets the requirement	Oracle EBS and Oracle Enterprise Manager support automated critical error notifications configurable by error severity, frequency, affected module, and error type. Notifications include full diagnostic information: error codes, timestamps, affected system components, user context, and relevant log excerpts. Delivery channels are configurable (email, SNMP trap for SIEM/NOC integration, SMS via OEM notification gateways, and integration with incident management platforms such as ServiceNow or Remedy).
	- Be customizable based on error severity, frequency, or affected modules.				
	- Include detailed diagnostic information, such as error codes, timestamps, and affected systems.				
	- Be sent via configurable channels (e.g., email, SMS, or integration with incident management platforms).				
CNF.190	The application must include tools for performing backup operations and managing historical backups. These tools should:	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS backup is managed through Oracle Recovery Manager (RMAN) which provides: automated backup scheduling (configurable by frequency, retention period, and backup type); AES-256 encryption of all backup sets; automated backup verification (RESTORE VALIDATE) confirming integrity and completeness; configurable versioning and retention policies (e.g., keep 30 daily, 12 monthly, 5 annual backups); and OEM-based monitoring with automated alerts for backup failures, missed schedules, or storage threshold breaches.
	- Support automated scheduling of backups with configurable frequency.				
	- Ensure secure storage of backups, including encryption and access control.				
	- Provide mechanisms for verifying backup integrity and completeness.				
	- Support versioning and retention policies for historical backups.				
	- Include monitoring and notification features for backup failures.				
CNF.191	The application must implement robust mechanisms to maintain data integrity during component failures. These mechanisms should:	Mandatory	+	Yes - the solution fully meets the requirement	Oracle Database provides ACID (Atomicity, Consistency, Isolation, Durability) transaction processing guarantees as a fundamental architectural feature. All Oracle EBS transactions are fully ACID-compliant. DB_BLOCK_CHECKSUM and DB_BLOCK_CHECKING detect and prevent data corruption. Oracle RAC and Data Guard provide real-time replication to protect against node/site failures. OEM monitors database block health in real time and alerts on any detected corruption or integrity issue.

CNF.191	- Prevent data corruption or loss during power outages, crashes, or unexpected shutdowns.	Mandatory	+		
	- Use transactional processing to ensure atomicity, consistency, isolation, and durability (ACID).				
	- Include real-time monitoring and alerting for potential data integrity issues.				
CNF.192	The application must provide mechanisms to enable the rapid restoration of availability and accessibility following continuity incidents. These mechanisms should:	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS's disaster recovery framework includes: comprehensive DR procedures documented in the Disaster Recovery Plan delivered as a project deliverable; Oracle Data Guard-based recovery from standby database with near-zero RPO; automated failover scripts for application tier switchover; documented and tested RTO/RPO targets (RTO ≤4h, RPO ≤15 min as standard, adjustable based on infrastructure); and scheduled DR drills (minimum annually) to validate recovery readiness, with drill results documented and reviewed with NBM.
	- Include detailed disaster recovery procedures integrated within the solution.				
	- Support data recovery from backups with minimal downtime.				
	- Ensure compatibility with failover systems for high availability.				
	- Include capabilities for periodic testing of recovery procedures to ensure readiness.				
CNF.193	The application architecture must be designed to be resilient to component failures and eliminate single points of failure (SPOF). Resilience should include:	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS architecture eliminates single points of failure through: (1) Oracle RAC for database tier redundancy (multiple database nodes with shared storage); (2) Oracle WebLogic clustering for application tier with automatic failover; (3) Oracle HTTP Server or F5/hardware load balancers for presentation tier distribution; (4) Oracle Data Guard for site-level redundancy; (5) redundant network paths and storage controllers at infrastructure level. All components support N+1 redundancy minimum, with automatic failover requiring no manual intervention.
	- Redundancy for critical components (e.g., database, application server).				
	- Load balancing to distribute workloads and mitigate performance bottlenecks.				
	- Automatic failover mechanisms to ensure continuity of service during failures.				
	- Scalability to handle unexpected increases in load without failure.				
CNF.194	The application must allow integration with monitoring tools such as SIEMs.	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS supports integration with SIEM solutions through Oracle Audit Vault's Syslog/CEF output, Oracle Enterprise Manager's SNMP trap generation, and database event streaming via Oracle GoldenGate. JMR will configure the SIEM integration as part of the security implementation workstream, ensuring all critical Oracle EBS security events are forwarded to NBM's SIEM in real time for centralized threat detection and correlation.
CNF.195	The requested solution must deliver a service level availability of at least 99.7%, calculated over a monthly reporting period.	Mandatory	+	Yes - the solution fully meets the requirement	Oracle EBS, when deployed with Oracle RAC and Data Guard in an active-passive configuration as proposed, meets and exceeds the 99.7% monthly availability SLA. Oracle's reference architectures for enterprise deployments consistently achieve 99.9%+ availability. JMR will monitor and report on availability monthly against the agreed SLA, with automated alerts for availability degradation, and maintain an incident register with root cause analysis for any downtime events.
1.11. Requirements for Source Codes					
CNF.196	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:	Mandatory	+	Yes - the solution fully meets the requirement	JMR will establish a software escrow arrangement for all Oracle EBS source codes and custom developments through a mutually agreed-upon escrow agent within 30 working days of final solution acceptance. The escrow agreement will: cover a minimum of 5 years; include all source code, dependencies, build scripts, and maintenance documentation; be activated at NBM's sole discretion in defined trigger events (supplier liquidation, bankruptcy, material breach); and be updated with each significant release or customisation delivered during the contract period.
	- An escrow protection agreement with a reputable and mutually agreed-upon escrow agent.				
	- The agreement must be activated upon the Buyer's request (at NBM's discretion) after the final acceptance of the solution.				
	- The Source Codes must be submitted within 30 working days unless otherwise agreed upon by the Parties.				
	- The escrow agreement must cover a minimum period of five (5) years.				
	- The Source Codes must include all necessary documentation and dependencies to enable independent maintenance and further development.				

CNF.197	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:	Mandatory	+	Yes - the solution fully meets the requirement	JMR will deliver all custom-developed source codes to NBM upon project completion and with each subsequent customisation delivery. Deliverables include: complete, uncommented source code (OAF pages, PL/SQL packages, workflow definitions, integration adapters); all dependent libraries and third-party components with their licenses; complete build and deployment instructions; and change logs. Updates and patches will be shared promptly (within 5 business days of each release) throughout the contract period. Source code will be delivered via a secure, access-controlled repository.
	- Source Codes must be complete, with no obfuscated or missing components.				
	- All related libraries, dependencies, and build instructions must be included to ensure full functionality and maintainability.				
	- Updates and patches must also be shared promptly as they are developed during the contract period.				
CNF.198	The Source Code delivered by the developers must adhere to best practices for maintainable software development, including:	Mandatory	+	Yes - the solution fully meets the requirement	All JMR custom-developed source code for Oracle EBS will adhere to Oracle's published development standards and NBM-agreed coding guidelines, including: clear, modular structure with consistent naming conventions (Oracle EBS naming standards for PL/SQL packages, OAF pages, workflow processes); comprehensive inline comments for all business logic, algorithms, and complex code sections; modular design using Oracle's standard extension points to maximise maintainability; static code analysis using Oracle's JDeveloper audit rules; unit testing with Oracle EBS standard test frameworks; and compliance with ISO/IEC 25010 quality characteristics as required.
	- Clear and consistent structure for easy navigation and understanding.				
	- Comprehensive inline comments explaining functionality, logic, and complex code sections.				
	- Meaningful and self-explanatory variable, function, and class names.				
	- Modular design principles to support future scalability and modification.				
	- Compliance with industry standards or specific coding guidelines agreed upon with the Buyer (e.g., ISO/IEC 25010 or similar).				
	- The Source Code must pass quality assurance checks, including static code analysis and unit testing, before delivery.				
CNF.199	The authenticity and integrity of all files containing the Source Codes must be verified and guaranteed by the Contractor through:	Mandatory	+	Yes - the solution fully meets the requirement	JMR will ensure the authenticity and integrity of all source code deliveries through: digital signatures applied to all source code packages using a JMR-held signing certificate (X.509); RFC 3161-compliant timestamping of digital signatures providing legal traceability; AES-256 encryption of source code archives during transmission (via secure SFTP or HTTPS) and storage; a detailed delivery manifest documenting each file, its hash (SHA-256), signing certificate reference, and timestamp; and a delivery verification log maintained for audit and legal reference purposes.
	- Digital signatures to confirm the Source Codes' origin and integrity.				
	- Timestamping of the digital signature to ensure traceability.				
	- Encryption of the Source Code files during transmission and storage to prevent unauthorized access.				
	- Documentation of verification steps and logs to support audits or legal disputes if required.				