VANUATU NATIONAL PROVIDENT FUND

EXPRESSION OF INTEREST (EOI)

Transformation of the Employer Contribution Ecosystem

Employer Portal | Contribution Clearing House | Payment Orchestration | Banking Integration

Procurement intent

This EOI seeks a complete transformation of VNPF's employer contribution ecosystem. It is not a cosmetic redesign of the existing Employer Portal. The target solution must provide an end-to-end digital service for contribution schedule submission, validation, member matching, payment initiation through banking payment gateway, clearing, reconciliation, reporting, security and operational support at scale.

Document status	EOI – Market Engagement / Vendor Prequalification
Issued by	VANUATU NATIONAL PROVIDENT FUND (VNPF)
Issue date	2nd November 2026
EOI reference	VNPFEMPLOYERPORTAL2026
Closing date/time	30th November 2026
Contact	Richard.Edwin@vnpf.com.vu Reynold.Amkori@vnpf.com.vu

Document Control

Field	Details
Document title	Expression of Interest – Transformation of the VNPF Employer Contribution Ecosystem
Owner	Vanuatu National Provident Fund
Business sponsor	VNPF Board of Trustee
Procurement lead	Director, Member and Employer Services Division
Version	1.0
Classification	Procurement / Controlled
Status	For EOI issue
Approval	Paul Kaun, CEO

Revision History

Version	Date	Prepared by	Description
1.0	27th October 2026	VNPF	Initial EOI for market engagement and vendor prequalification

Purpose of this EOI

VNPF invites suitably qualified technology firms, system integrators, fintech providers, superannuation/pension technology specialists and consortiums to express interest in designing, implementing, integrating and supporting a modern Employer Contribution Ecosystem. This EOI will assist VNPF to validate the market, assess solution capability and delivery maturity, shortlist capable vendors, refine requirements and determine the most appropriate procurement pathway for the subsequent stage.

Executive Summary

VNPF intends to replace the limitations of its current Employer Portal with a secure, scalable and user-centred digital contribution platform. Employers must be able to prepare or upload contribution schedules (CS), validate employee/member data, resolve exceptions, submit contribution transactions, initiate payments through supported banking/payment channels, track settlement, reconcile payments to schedules and maintain a complete historical record from anywhere in the world.

The solution must support employers ranging from very small organisations to large employers with approximately over 4,000–5,000 employees per contribution cycle, without degraded usability or unreliable processing. It must also provide VNPF with operational controls, clearing capability, auditability, cyber security, data quality services, APIs, dashboards and exception-management tools required for a modern superannuation environment.

Transformation principle

The project shall be treated as an end-to-end contribution ecosystem transformation spanning employer experience, data quality, contribution processing, payment orchestration, banking connectivity, clearing, reconciliation, security, analytics and support—not as a front-end portal refresh.

Target Outcomes

- One secure employer identity and portal experience accessible through modern browsers from Vanuatu and overseas.
- Fast and reliable submission of contribution schedules for 1 employee through at least 5,000 employees or more in a single employer payment cycle.
- Configurable validation rules that identify errors before a schedule is accepted.
- Automated member matching, duplicate detection and controlled data-cleansing workflows.
- End-to-end contribution transaction request, payment initiation, clearing and reconciliation.
- Integration with banking/payment gateways without VNPF storing employer banking credentials.
- Real-time or near-real-time status visibility, receipts, exception handling and audit trails.
- API-first architecture supporting future VNPF digital services, banks, payroll providers and government/third-party systems.
- Strong security, privacy, resilience, monitoring and compliance controls.
- Reduced manual intervention, fewer rejected schedules, faster allocation of contributions and improved employer/member service.

1. Background and Current-State Problems

The Vanuatu National Provident Fund receives mandatory employer and employee contribution information and payments from employers. The existing Employer Portal provides a digital channel, but its current design and operating model do not adequately support VNPF's future service, scale, integration and control requirements.

1.1 Current-State Pain Points

- The portal is not sufficiently intuitive or user-friendly, creating avoidable employer effort and support demand.
- The current process lacks integrated banking/payment gateway capability for a seamless schedule-to-payment journey.
- Large employee contribution schedules can be difficult to submit and process reliably.
- Validation and error feedback are insufficiently automated, consistent or easy to resolve.
- Member matching and data-quality issues can create manual intervention, unmatched records and delayed allocation.
- Employers do not have a sufficiently unified view of schedules, payments, exceptions, receipts and historical records.
- Operational teams require stronger clearing, reconciliation, exception-management and audit capabilities.
- The current solution requires modernization to meet contemporary expectations for cyber security, resilience, integration, observability, mobile-responsive access and digital service delivery.

1.2 Scale and Access Context

The target platform must support the full range of VNPF employers, including employers with only a few employees and high-volume employers with approximately 4,000–5,000 employees or more. Employers must be able to securely access the service and transmit contribution schedules from anywhere in the world, subject to VNPF security policies, identity controls and applicable legal requirements. Operational manuals must also be produced and made available to all end users.

2. Project Objectives

- Design and implement a modern, accessible and secure Employer Contribution Ecosystem.
- Enable end-to-end digital contribution processing from schedule creation/upload through payment, clearing, reconciliation and posting readiness.
- Improve contribution data quality at source through configurable validation and member-matching services.
- Provide seamless and secure integration with participating banks and payment service providers.
- Enable reliable high-volume processing and transparent exception handling.
- Provide employers with complete self-service visibility of submissions, payments, receipts, corrections and history.
- Provide VNPF operations with real-time work queues, dashboards, audit trails and reconciliation tools.
- Establish an API-led and modular platform that can evolve without excessive vendor dependency.
- Meet robust security, privacy, business continuity, disaster recovery and service-management requirements.
- Build VNPF internal capability through documentation, training and knowledge transfer.
- Operational manuals and system documentation must be built not the system and be made available to all end users.

3. Strategic Rationale

The transformation is intended to strengthen contribution collection as a core VNPF business capability. It should reduce friction for employers, improve the quality and timeliness of member records, reduce operational risk and manual handling, improve payment traceability, and establish a platform for future digital integration with payroll systems, banks and other authorised ecosystem participants.

3.1 Design Principles

Principle	Required interpretation
Employer-first	Simple workflows, clear status, actionable errors, minimal re-keying and responsive design.
Straight-through processing	Automate valid transactions while routing exceptions to controlled work queues.
API-first and modular	Expose governed services through documented APIs; avoid tightly coupled proprietary dependencies.
Security by design	Identity, least privilege, encryption, secure coding, logging, monitoring and privacy embedded from inception.
Data quality at source	Validate and match before acceptance to reduce downstream corrections.
Resilient by design	High availability, recoverability, monitoring, capacity management and tested continuity.
Auditability	Every material action and status change must be traceable to actor, time, source and outcome.
Future-ready	Architecture must accommodate additional banks, payment rails, payroll providers and service channels.

4. Detailed Scope of Services

The selected vendor will be expected to provide all professional services, software, configuration, integration, testing, migration, implementation, training, documentation and support required to deliver the target solution. Vendors may propose a single platform or a well-integrated solution stack, provided accountability, security, data ownership and support are clear.

4.1 In-Scope Workstreams

- Discovery, process mapping, requirements validation and target operating model.
- User experience and service design for employer and VNPF operational users.
- Employer organisation, user, role and delegation management.
- Contribution schedule creation, upload, API submission, validation and correction.
- Member matching, data cleansing and exception management.
- Contribution Transaction Request creation and lifecycle management.
- Contribution clearing house services and allocation controls.
- Payment orchestration and banking/payment gateway integration.
- Automated reconciliation and exception management.
- Integration with VNPF core/member systems (VNPF Membership and Contribution System) and other authorized systems.
- Reporting, analytics, audit and operational dashboards.
- Data migration and historical record transition.
- Cyber security, privacy, monitoring, logging and compliance controls.
- Performance engineering, load testing, POC and 5,000-employee stress testing.
- Deployment, cutover, hypercare, support, SLA, knowledge transfer and continuous improvement.

5. Functional Requirements

5.1 Employer Registration, Identity and Access

- Employer onboarding and activation using VNPF-approved verification workflows.
- Multi-user employer accounts with role-based access (e.g., preparer, reviewer, approver, finance/payment user, administrator, read-only).
- Segregation of duties and configurable approval workflows for schedule submission and payment initiation.
- Multi-factor authentication (MFA), secure passwordless/federated options where approved, session controls and account recovery.
- Delegated access for authorised payroll agents/accountants with explicit employer consent and expiry controls.
- Employer profile, contacts, contribution settings, payment preferences and authorised users.
- Global browser access with responsive desktop/tablet/mobile experience and clear support for low/variable bandwidth conditions.

5.2 Contribution Schedule Management

- Create a contribution schedule manually for small employers, upload standard files for larger employers, or submit via API.
- Support VNPF-approved CSV/XLSX templates and future machine-to-machine formats.
- Pre-upload template validation, schema validation and human-readable error reporting.
- Save draft, resume, clone prior period, amend before submission and maintain version history.
- Bulk processing without requiring row-by-row interaction for valid records.
- Clear totals for employee contributions, employer contributions, other permitted components and overall payable amount.
- Employer declaration/attestation before final submission.
- Unique schedule ID, timestamp, status, period and immutable submission history.

5.3 Employer Submission and VNPF Verification Model

- Employers enter and submit employee Contribution Schedules through the Portal.
- Schedules go into a VNPF verification queue and are approved automatically, rejected or returned with reasons.
- Only approved schedules go on to clearing and reconciliation.
- Automated validation clears valid records, so VNPF officers only review exceptions and sampled items.
- Employers see live status and get notifications
- Returned schedules are corrected and resubmitted by the employer, with a full audit trail.
- Dashboards track verification workload and turnaround

6. Validation Rules Engine

The platform must include a configurable rules engine so VNPF can define, activate, deactivate, version and audit contribution validation rules without requiring source-code changes for routine policy configuration.

Rule category	Illustrative controls
File/schema	Required columns, format, data type, duplicate rows, malformed values, file size, encoding.
Employer	Employer ID/status, contribution period, duplicate schedule, permitted filing period.
Member	Member number format/status, name/DOB consistency, employment relationship, duplicate member entry.
Contribution	Permitted rates, minimum/maximum or policy thresholds, arithmetic consistency, zero/negative values, rounding.
Payment	Schedule total equals payment request, currency, reference integrity, duplicate payment prevention.
Business policy	Effective-dated rules, exemptions, special employer/member categories, grace/late logic where configured.

Each validation result must return a rule identifier, severity (error/warning/information), affected row/member, plain-language explanation, recommended correction and whether the issue blocks submission. VNPF must be able to report on recurring validation failures by employer and rule.

7. Member Matching & Data Cleansing

The solution must reduce unmatched contributions by combining deterministic matching, configurable fuzzy matching and controlled human review. Matching logic must be transparent, scored where appropriate and fully auditable.

- Exact matching using VNPF member number and other authoritative identifiers.
- Configurable secondary matching using combinations of name, date of birth, employer history and other approved attributes.
- Fuzzy matching with confidence thresholds and no automatic merge where confidence is below VNPF-approved levels.
- Detection of duplicates, transposed fields, formatting differences and common data-quality defects.
- Exception queue for possible matches, unmatched records and suspected duplicates.
- Controlled correction workflow that preserves source data, corrected data, user, timestamp and reason.
- Ability to return actionable data-quality feedback to employers before final acceptance where appropriate.
- Bulk cleansing and matching for migrated/historical records with reconciliation totals.

8. Contribution Transaction Request (CTR)

Following successful schedule validation, the system must create a controlled Contribution Transaction Request representing the financial obligation associated with the accepted schedule. The CTR should be the traceable link between the contribution schedule, payment request, settlement, clearing and reconciliation.

- Generate a unique, non-reusable CTR reference and payment reference.
- Bind employer, contribution period, schedule version, amount, currency and expiry/status rules.
- Support statuses such as Draft, Validated, Awaiting Approval, Payment Pending, Payment Initiated, Settled, Failed, Cancelled, Reconciled and Posted/Completed.
- Prevent duplicate payment or duplicate settlement against the same obligation.
- Allow controlled regeneration/replacement where a transaction expires or fails, preserving full history.
- Expose CTR status through portal, APIs and VNPF operational dashboards.

9. Contribution Clearing House

VNPF seeks a clearing capability that controls the relationship between contribution obligations, payment events and allocation-ready contribution data. The clearing house may be implemented as a dedicated module or service within the proposed architecture.

- Receive validated contribution obligations and associated payment references.
- Receive payment initiation and settlement events from the orchestration layer/banks.
- Match and clear settled funds against the correct employer, period and schedule.
- Handle partial, short, over, duplicate, late, reversed or unmatched payments according to VNPF rules.
- Maintain suspense/exception states and operator work queues with ageing.
- Produce allocation-ready records for downstream VNPF member/core systems.
- Maintain an immutable financial and operational audit trail.
- Provide end-of-day and period-based control totals for schedules, payments, cleared items, exceptions and postings.

10. Payment Orchestration Gateway

The payment orchestration layer must provide a 100% secure abstraction between the VNPF contribution platform and participating banks/payment channels. It should enable VNPF to add or change payment providers with minimal impact to the core contribution service.

- Create payment intents/requests from approved CTRs.
- Route transactions to an employer-selected or VNPF-configured supported bank/payment channel.
- Support redirect, hosted payment, bank API, account-to-account or other approved flows without exposing banking credentials to VNPF.
- Use idempotency controls to prevent accidental duplicate payment requests.
- Receive signed/authenticated callbacks, webhooks or status messages and verify authenticity.
- Normalize provider-specific statuses into a common VNPF payment status model.
- Support retries, timeouts, expiry, cancellation and controlled recovery from interrupted journeys.
- Provide a provider adapter pattern so new banks can be onboarded without redesigning the entire platform.
- Maintain transaction-level logs, correlation IDs and reconciliation references.

11. Banking Integration

Vendors must describe proven methods for integrating with commercial banks and payment providers. Final integration will depend on participating bank capabilities and agreements. The architecture must support multiple banks and payment methods over time.

Requirement	Expected capability
Authentication	OAuth 2.0/OIDC, mTLS, signed requests or bank-required equivalent; secrets managed securely.
Payment initiation	Create payment request or redirect to bank-controlled authentication/authorisation journey.
Status	Query and/or receive asynchronous payment status notifications.
Settlement evidence	Receive bank reference, value date, amount, payer reference and settlement status.
Reconciliation data	Consume statements, transaction feeds, APIs or approved files with strong controls.
Security boundary	VNPF must not collect or store employer internet-banking passwords, PINs or equivalent credentials.
Multi-bank model	Standard internal interface with provider-specific adapters and clear onboarding process.

12. Automated Reconciliation

The solution must automate reconciliation between accepted contribution schedules, CTRs, payment transactions, bank settlement records, clearing outcomes and downstream posting results.

- Automatic exact matching using unique references, amount, employer, period and settlement data.
- Configurable matching rules and tolerance controls approved by VNPF.
- Exception categories for missing payment, unmatched payment, amount mismatch, duplicate, reversal, partial payment and stale transaction.
- Operator work queues with ownership, notes, evidence, ageing and escalation.
- Controlled manual match/adjustment with maker-checker approval where required.
- Daily reconciliation summary and signed-off control totals.
- Full audit trail from original schedule through payment and posting.

13. Security & Compliance

Security must be designed into the platform, delivery process and operating model. Vendors must identify the security standards, certifications and control frameworks applicable to their organisation, cloud/service providers and proposed solution, and clearly distinguish certified controls from planned controls.

- MFA and role-based access control; least privilege; privileged access management for administrators.
- Encryption in transit using current secure protocols and encryption at rest using industry-standard cryptography.
- Secure secrets/key management with rotation, access controls and audit.
- Secure SDLC including code review, dependency management, SAST/DAST, vulnerability scanning and remediation.
- Independent penetration testing before go-live and periodically thereafter.
- Centralised security logging, tamper resistance, monitoring, alerting and integration capability with SIEM/SOC services.
- Protection against common web/API threats, rate limiting, bot/abuse controls and DDoS mitigation appropriate to the hosting model.
- Data minimisation, retention controls, secure disposal and privacy-by-design.
- Segregation of production/non-production environments and prohibition on uncontrolled production data use in lower environments.
- Incident response plan with defined notification, containment, investigation and evidence preservation processes.
- Compliance mapping to recognised standards such as ISO/IEC 27001, ISO/IEC 27017/27018 where applicable, OWASP guidance, PCI DSS only where the proposed payment architecture brings components into PCI scope, and other applicable legal/regulatory obligations.

Vendor obligation

Vendors must not state that a solution is “compliant” merely because a cloud provider holds a certification. The response must identify which party, component and service boundary is certified or assessed, the current validity of evidence, and any customer responsibilities.

14. Technical / Non-Functional Requirements

Area	Minimum expectation
Availability	Vendor to propose production SLA; target architecture should support high availability and removal of single points of failure.
Performance	Interactive pages and APIs designed for responsive operation; bulk processing must be asynchronous where necessary with visible progress/status.
Scalability	Demonstrate capacity for 5,000-employee or more schedules and concurrent employer usage, with horizontal/elastic scaling where appropriate.
Reliability	Idempotent financial operations, retry controls, transaction integrity and safe recovery from partial failures.
Maintainability	Modular architecture, automated deployment, configuration management, documented code/configuration and support procedures.
Observability	Central logs, metrics, traces, correlation IDs, dashboards, alerting and business transaction monitoring.
Accessibility	Responsive, keyboard-accessible, clear error handling; vendor to state alignment with WCAG 2.1 AA or later applicable standard.
Compatibility	Current supported versions of major browsers; no dependence on obsolete plugins or desktop-only components.
Localization	Support Vanuatu date/time/currency conventions and configurable labels/content; Unicode throughout.
Audit	Immutable or tamper-evident logs for authentication, schedule, rule, approval, payment, reconciliation and administrative actions.

15. Data Migration

The vendor must provide a migration approach that preserves integrity, traceability and business continuity. The final migration scope will be confirmed during discovery.

- Profile existing employer, user, contribution schedule, payment, receipt and relevant reference data.
- Define source-to-target mapping, transformation, cleansing and deduplication rules.
- Perform trial migrations and reconcile record counts, financial totals and key relationships.
- Provide exception reports and business sign-off checkpoints.
- Preserve historical records required for employer self-service, audit and regulatory purposes.
- Encrypt migration files and use controlled transfer/storage with defined retention and secure deletion.
- Provide rollback/contingency approach for cutover.
- The plan must include the following:
    - **Data Completeness:** Verify that all required employer, member, contribution, and transaction records have been successfully migrated without omissions or duplication.
    - **Data Accuracy:** Ensure that migrated data accurately reflects the original source records, including employer details, member information, contribution histories, and financial transactions.
    - **Data Reconciliation:** Conduct reconciliation between the legacy and new systems to identify and resolve any discrepancies before go-live.
    - **Data Integrity and Security:** Ensure that data relationships, formats, and security controls are maintained throughout the migration process.
    - **User Acceptance Testing (UAT):** VNPF's designated business and ICT teams must validate the migrated data against agreed acceptance criteria.
    - **Final Sign-Off:** The system must not proceed to go-live until all critical data migration issues have been resolved and formal acceptance has been provided by VNPF and signed off by the Chief Executive Officer (CEO).

16. API & Integration Requirements

- API-first design using well-documented REST/JSON and/or other standards justified by the vendor.
- OpenAPI specifications, versioning policy, authentication/authorization model and sandbox/test capability.
- Idempotency for transaction-creating APIs and correlation IDs across distributed services.
- Webhook/event interfaces for status changes where appropriate, with signature verification and replay protection.
- Integration with VNPF core/member systems, identity services, notification services, banks/payment providers and future payroll systems. The successful vendor will be responsible for designing, developing, testing, implementing, and supporting all necessary integration interfaces (APIs) between the proposed Employer Portal and VNPF's existing systems.
- Bulk APIs or secure file interfaces where API integration is not available, with equivalent validation, integrity and audit controls.
- Rate limiting, throttling, monitoring, API gateway controls and lifecycle management.
- No undocumented proprietary interface may be essential to VNPF’s ability to retrieve its own data or integrate future services.

17. Reporting & Analytics

- Employer dashboard: schedules by period/status, amount due/paid, validation issues, payment status, receipts and history.
- VNPF operations dashboard: volumes, values, success/failure rates, unmatched members, unreconciled payments, ageing and workload.
- Management dashboard: contribution collection trends, channel usage, employer compliance indicators and service performance.
- Data-quality analytics: top validation failures, matching confidence, recurring employer issues and correction trends.
- Payment analytics: provider performance, settlement time, failed/expired transactions and reconciliation exceptions.
- Export to common formats and controlled scheduled reports.
- Role-based access to reports and audit of sensitive report access/export.
- Ability to feed VNPF enterprise analytics/data platform through governed APIs or extracts.

18. Business Continuity and Disaster Recovery

Vendors must propose measurable resilience objectives and demonstrate that the solution can recover from infrastructure, application, data, integration and regional/service-provider failures appropriate to the selected hosting model.

- Proposed Recovery Time Objective (RTO) - the successful vendor must ensure that critical Employer Portal services can be restored within a maximum of **4 hours** following a major system disruption.
- Recovery Point Objective (RPO) - the solution must support data recovery with a maximum potential data loss window of **1 hour**, with additional transaction safeguards to prevent the loss or duplication of confirmed financial transactions.
- Automated backups with encryption, retention, integrity checks and periodic restore tests.
- Redundancy across failure domains and documented failover/failback procedures.
- Disaster recovery exercise at least annually or at a frequency agreed with VNPF, with evidence and remediation tracking.
- Business continuity arrangements for critical vendor support and third-party dependencies.
- Defined degraded-mode/manual contingency for contribution receipt and later reconciliation if critical external banking services are unavailable.

19. Mandatory Technical Requirements Matrix

Vendors must complete the following matrix using: C = Comply (available/configurable), PC = Partially Comply, R = Requires development, NC = Does Not Comply. Every PC/R/NC response must explain the gap, proposed remediation, cost/timeline impact and dependency. “Comply” responses must include a concise evidence reference.

ID	Requirement	Class	Vendor response	Evidence / comments
MTR-01	Secure web portal accessible internationally using supported modern browsers	Mandatory		
MTR-02	MFA, RBAC, employer-level segregation and segregation of duties	Mandatory		
MTR-03	Manual, file-upload and API-based contribution schedule submission	Mandatory		
MTR-04	Process a single employer schedule containing at least 5,000 employees	Mandatory		
MTR-05	Configurable validation rules engine with versioning and audit	Mandatory		
MTR-06	Member matching, duplicate detection, cleansing and exception workflow	Mandatory		
MTR-07	Unique Contribution Transaction Request and lifecycle controls	Mandatory		
MTR-08	Contribution clearing capability linking obligation, payment and allocation	Mandatory		
MTR-09	Payment orchestration abstraction supporting multiple banks/providers	Mandatory		
MTR-10	Secure banking integration without storing employer banking credentials	Mandatory		
MTR-11	Automated reconciliation and controlled exception management	Mandatory		
MTR-12	End-to-end audit trail with user/time/source/status history	Mandatory		

ID	Requirement	Class	Vendor response	Evidence / comments
MTR-13	API-first integration with documented, versioned interfaces	Mandatory		
MTR-14	Encryption in transit and at rest; secure key/secrets management	Mandatory		
MTR-15	Secure SDLC, vulnerability management and independent penetration testing	Mandatory		
MTR-16	Central logging, monitoring, alerting and correlation IDs	Mandatory		
MTR-17	Backup, restore and DR capability with defined RTO/RPO	Mandatory		
MTR-18	Data export and exit capability in open/documented formats	Mandatory		
MTR-19	Separate non-production environments and controlled deployment pipeline	Mandatory		
MTR-20	Performance/load test evidence and participation in VNPF POC	Mandatory		
MTR-21	Complete technical, operational, API and security documentation	Mandatory		
MTR-22	Face-to-face knowledge transfer and administrator/operations training	Mandatory		
MTR-23	Configurable notifications for validation, approval, payment and exceptions	Mandatory		
MTR-24	Historical schedule/payment/receipt search and download	Mandatory		
MTR-25	No critical dependency on unsupported/obsolete software components	Mandatory		

20. Proof-of-Concept (POC) Requirements

Shortlisted vendors may be required to complete a time-boxed POC using a VNPF-approved test environment and synthetic or appropriately protected test data. The POC is intended to demonstrate working capability, not presentation-only mock-ups. VNPF may refine scenarios before invitation.

20.1 Mandatory POC Scenarios

Scenario	Demonstration
POC-01	Employer login with MFA; demonstrate roles, preparer/approver separation and employer data isolation.
POC-02	Upload a valid contribution schedule and show validation, totals, acceptance and unique schedule reference.
POC-03	Upload a schedule containing at least 10 deliberate data errors and demonstrate row-level, actionable validation feedback.
POC-04	Demonstrate exact and fuzzy member matching, confidence handling and an unmatched-member work queue.
POC-05	Create a CTR from an approved schedule and demonstrate lifecycle/status history.
POC-06	Initiate a payment through a simulated or sandbox bank/payment provider and demonstrate secure handoff and return.
POC-07	Receive a simulated settlement event and automatically reconcile it to the correct CTR/schedule.
POC-08	Demonstrate partial/mismatched payment exception and controlled operator resolution.
POC-09	Show employer receipt/history and VNPF operational dashboards.
POC-10	Demonstrate audit trail, logs/correlation IDs and administrator configuration of one validation rule.
POC-11	Demonstrate API documentation and submit/query a schedule or status through API.
POC-12	Execute the 5,000-employee or more high-volume test defined below.

20.2 POC Evidence

- Architecture diagram and component inventory used for the POC.
- Test results with timestamps, record counts, processing times, error rates and resource observations.
- Security control demonstration relevant to identity, API authentication, secrets and audit.
- List of any POC functions that are simulated, manually assisted, roadmap-only or require additional licensed products.
- Known limitations, dependencies and estimated production remediation.

21. 5,000-Employee or more Stress / High-Volume Test

The high-volume test is mandatory for shortlisted vendors. Its purpose is to prove that the proposed solution can reliably process a large employer contribution cycle and remain operationally usable.

Test element	Minimum requirement / evidence
Dataset	One employer schedule containing 5,000 employee or more contribution rows with realistic identifiers, names, amounts and a controlled mix of valid/invalid records.
Upload	Demonstrate upload or API submission without browser timeout, data loss or manual file splitting.
Validation	Execute all applicable validation rules and produce a complete error/warning result set.
Matching	Run member matching and report exact, probable and unmatched outcomes.
Correction	Correct/re-submit selected invalid rows without re-keying the entire schedule.
CTR	Create a CTR for the accepted schedule and prove total integrity.
Payment	Initiate a sandbox/simulated payment request for the full accepted amount.
Reconciliation	Process simulated settlement and reconcile to the correct schedule/CTR.
Performance evidence	Record end-to-end elapsed time, server-side processing time, API response times, queue times, error rate, resource utilisation and any throttling.
Concurrency	Vendor to demonstrate or provide repeatable test evidence for concurrent employer activity and explain tested concurrency level.
Resilience	Demonstrate safe retry/recovery from at least one interrupted/duplicate request scenario without duplicate financial transaction.
Target	Vendor must state guaranteed or committed production service levels and capacity. VNPF will evaluate actual POC performance against the vendor's stated commitments and usability.

Important

VNPF is deliberately not prescribing an arbitrary processing-time number at EOI stage. Vendors must state measurable performance commitments and prove them. VNPF may set pass/fail thresholds for the shortlisted POC after reviewing market responses and the final hosting/integration design.

22. Vendor Response Template

Responses should follow the structure below to enable consistent evaluation. Marketing material may be appended but must not replace direct responses.

Section	Required response
A	Executive response and understanding of VNPF's transformation objective
B	Proposed solution overview and architecture
C	Completed Mandatory Technical Requirements Matrix
D	Functional requirements response and gaps
E	Payment orchestration, clearing, real banking integration and reconciliation approach
F	Security, privacy, compliance and assurance evidence
G	Hosting options, resilience, DR, monitoring and service management
H	Data migration and integration approach
I	POC readiness and proposed high-volume test method
J	Implementation plan, resources, governance and timeline
K	Training, change management and knowledge transfer
L	Support/SLA and continuous improvement
M	Vendor experience, references and key personnel
N	Data ownership, licensing, IP, exit and lock-in position
O	Commercial response using the required template
P	Assumptions, dependencies, exclusions and risks
Q	Signed declaration

23. Vendor Project Experience Requirements

- Demonstrated delivery of comparable pension, provident fund, superannuation, payroll contribution, clearing, banking, fintech or high-volume financial transaction platforms.
- At least three relevant reference projects preferred, including client, country, scope, scale, go-live date, technology, vendor role and reference contact (subject to client permission). Relevant project experience and client references are mandatory evaluation requirements.
- Experience integrating with banks/payment gateways and reconciling financial transactions.
- Experience with high-volume batch/file and API transaction processing.
- Established cyber security, software engineering, QA, DevOps and service-management practices.
- Named project manager, solution architect, security lead, integration lead, data/migration lead, test lead and change/training lead with relevant CV summaries.
- Ability to provide on-site engagement in Vanuatu at key phases and face-to-face knowledge transfer.
- Financial and organisational capacity to support the solution for the proposed contract term.

24. Evaluation Methodology

VNPF may use a staged evaluation. Responses that fail material mandatory requirements, provide materially incomplete information or do not accept participation in the POC may be excluded from further consideration. VNPF reserves the right to seek clarification, verify references and request demonstrations.

24.1 Proposed Evaluation Stages

1. Stage 1 – Administrative compliance and completeness.
2. Stage 2 – Mandatory technical requirement compliance and material exceptions.
3. Stage 3 – Qualitative technical, delivery, security, experience and commercial evaluation.
4. Stage 4 – Shortlisted vendor POC, including 5,000+ employee test, 100% pass target.
5. Stage 5 – Reference checks, due diligence, clarification and procurement recommendation / next-stage invitation.

24.2 Evaluation Matrix

Criterion	Weight	Evaluation focus
Solution fit & functional capability	20%	End-to-end employer contribution ecosystem, usability, validation, matching, CTR, clearing, reconciliation and reporting.
Architecture, integration & scalability	15%	API-first design, modularity, bank integration, 5,000+ employee scale, 100% performance target and observability.
Security, compliance & resilience	15%	Security controls, assurance evidence, privacy, DR/BCP and secure SDLC.
POC & high-volume test	20%	Working demonstration, correctness, usability, performance, resilience and transparency of limitations.
Delivery approach & implementation capability	10%	Methodology, governance, migration, testing, cutover, timeline and resource quality.
Relevant experience & references	8%	Comparable implementations and proven banking/financial transaction experience.
Training, support & knowledge transfer	5%	On-site training, documentation, SLA, support model and internal capability uplift.
Commercial & total cost of ownership	7%	Transparent implementation and recurring costs, licensing, third-party charges and five-year TCO.
Total	100%	VNPF may refine weightings in the next procurement stage.

VNPF may apply pass/fail gates for mandatory security, data ownership, POC participation, 5,000+ employee or more processing, real banking integration architecture and critical functional requirements before weighted scoring.

25. Implementation Phases and Indicative Timeline

Vendors must propose an achievable implementation plan. The following is an indicative planning framework and may be refined after EOI market feedback and detailed discovery.

Phase	Indicative duration	Key outputs
1. Mobilisation & discovery	3–4 weeks	Governance, requirements validation, process maps, delivery plan, environments, risk register.
2. Solution design	4–6 weeks	Target architecture, UX, security design, integration specs, data model, migration and test strategy.
3. Build/configuration & integrations	10–16 weeks	Portal, rules, matching, CTR, clearing, orchestration, bank adapters, APIs, dashboards.
4. Migration & system/integration testing	6–8 weeks	Trial migration, SIT, security testing, performance testing, defect remediation.
5. UAT, POC confirmation & readiness	4–6 weeks	UAT, 5,000-employee or more production-like test, training, operational readiness, cutover rehearsal.
6. Go-live & hypercare	2–4 weeks	Cutover, production launch, monitoring, rapid support and stabilisation.
7. Managed support & optimisation	Ongoing	SLA support, enhancements, capacity/security reviews and continuous improvement.

Vendors should identify critical-path dependencies, especially bank onboarding/certification, VNPF core-system interfaces, data availability, security approvals and third-party lead times.

26. Training and Change Management

- Role-based training for VNPF operations, finance, ICT, security, service desk, administrators and management.
- Employer-facing guides, quick-reference materials, FAQs and optional webinar/onboarding content.
- Face-to-face technical and operational knowledge transfer in Vanuatu for relevant VNPF teams.
- Administrator training covering rules, user management, configuration, monitoring and reporting.
- Technical training covering architecture, APIs, deployment, troubleshooting, logs, backup/restore and support procedures.
- Train-the-trainer capability and editable source materials for future VNPF use.
- Change impact assessment, communications plan, employer migration/onboarding strategy and adoption measures.
- Complete as-built documentation and handover before final acceptance.

27. Service Levels, Support and Maintenance

Vendors must propose a support model covering production operations, incident/problem management, security response, patching, upgrades and continuous improvement. Support hours must reflect the criticality of contribution and payment processing.

Severity	Illustrative definition	Target vendor response required
P1 Critical	Service unavailable, financial processing blocked, major security incident or material data integrity risk.	State 24x7 availability, response, restoration/workaround and escalation commitments.
P2 High	Major function degraded; significant employers/users affected; no reasonable workaround.	State support window, response and restoration target.
P3 Medium	Limited function affected; workaround available.	State response/resolution target.
P4 Low/Request	Minor defect, query, service request or enhancement.	State response/fulfilment target.

- Monthly SLA reporting and service review.
- Defined maintenance windows and advance notification.
- Security patch/vulnerability remediation timelines by severity.
- Problem management and root-cause analysis for major incidents.
- Release notes, regression testing and rollback procedures.
- Capacity monitoring and proactive scaling recommendations.

28. Data Ownership, Intellectual Property and Vendor Lock-In

- All VNPF and employer/member data remains the property of VNPF or the relevant data owner as determined by applicable law and agreements.
- VNPF must be able to export its data, transaction history, audit records and configuration in documented, usable formats throughout the contract and at exit.
- The vendor must disclose all proprietary components, third-party licences, open-source dependencies and restrictions material to operation or transition.
- APIs and data schemas required for VNPF integrations must be documented and available under the agreed licence/contract.
- Vendors must surrender to VNPF all source-code ownership/licensing, configuration ownership and any escrow arrangement proposed for critical bespoke components.
- Exit assistance must include data extraction, documentation, knowledge transfer, credential/key transition and reasonable cooperation with a replacement provider.
- No contract or technical design should make VNPF dependent on the vendor for routine access to its own data or create avoidable barriers to future integration.

29. Commercial Response Template

At EOI stage, vendors should provide indicative pricing in Vanuatu Vatu (VUV) and clearly state taxes, foreign-currency assumptions and validity period. Detailed binding pricing may be requested at the next procurement stage.

Cost category	One-off (VUV)	Annual/Recurring (VUV)	Basis / assumptions
Discovery & solution design			
Software/platform licenses			
Implementation/configuration			
Employer Portal & UX			
Validation/matching/clearing modules			
Payment orchestration & bank integrations			
API/integration development			
Data migration			
Security testing/assurance			
Performance/POC testing			
Training & change management			
Hosting/cloud/infrastructure			
Support & maintenance			
Third-party products/services			
Optional enhancements			
Exit/transition services			

29.1 Five-Year Total Cost of Ownership

Vendors must provide an indicative five-year TCO showing separate data implementation, licensing, hosting, support, transaction fees, bank/payment-provider charges under vendor control, mandatory upgrades and all material third-party costs. Any volume-based pricing must state thresholds and unit rates.

30. EOI Submission Instructions

Item	Instruction
EOI reference	VNPFEMPORTAL2026
Submission deadline	30th November 2026 at 4:30pm, Vanuatu time
Submission method	My E-mail to: Paul.Kaun@vnpf.com.vu CC to: Richard.Edwin@vnpf.com.vu & Reynold.Amkori@vnpf.com.vu By Mail to: **Mr. Paul Kaun** Vanuatu National Provident Fund PO BOX 420 Port Vila Vanuatu
File format	Searchable PDF plus editable response schedules where requested.
Subject / package label	EOI – VNPF Employer Contribution Ecosystem Transformation – [Vendor Name]
Contact for clarification	Reynold.Amkori@vnpf.com.vu
Clarification deadline	25th November 2026
Validity	Response to remain valid for at least 30 days from closing date.

30.1 Submission Conditions

- VNPF may amend, suspend or cancel the EOI process and is not bound to accept any response or proceed to a subsequent procurement.
- Costs of preparing and submitting an EOI, attending demonstrations or participating in due diligence are the vendor's responsibility unless VNPF expressly states otherwise.
- VNPF may request clarification, additional evidence, reference checks, security due diligence, demonstrations and a POC from shortlisted vendors.
- Vendors must identify actual or potential conflicts of interest and any subcontractors/consortium members.
- Confidential information must be clearly marked. Vendors must also respect the confidentiality of VNPF information provided during the process.
- Any material assumptions, exclusions, deviations or dependencies must be explicitly stated; silence may be treated as acceptance of the stated requirement for evaluation purposes.

31. Vendor Declaration

The undersigned, being duly authorised to represent the Respondent, declares that the information provided in this EOI response is true and complete to the best of its knowledge; that all material assumptions, exceptions and dependencies have been disclosed; that the Respondent is willing to participate in clarification, due diligence and the required proof-of-concept if shortlisted; and that no undisclosed conflict of interest exists that would materially affect the proposed engagement.

Declaration field	Vendor completion
Legal entity name	
Registered address	
Authorised representative	
Title/position	
Email / telephone	
Signature	
Date	
Conflict of interest disclosure	None / Attached (delete as applicable)

Appendix A – Detailed Functional Response Schedule

ID	Requirement	C/PC/R/NC	Standard / Config / Custom	Comments / evidence
FR-01	Employer onboarding and profile management			
FR-02	Multi-user roles and delegated authority			
FR-03	MFA and secure account recovery			
FR-04	Manual schedule entry for small employers			
FR-05	CSV/XLSX bulk schedule upload			
FR-06	API schedule submission			
FR-07	Draft/save/resume/clone prior schedule			
FR-08	Validation rules and actionable errors			
FR-09	Member exact/fuzzy matching			
FR-10	Data cleansing and exception workflow			
FR-11	Maker-checker schedule approval			
FR-12	CTR generation and lifecycle			
FR-13	Payment initiation and multi-bank routing			
FR-14	Payment callback/status processing			
FR-15	Clearing and allocation controls			
FR-16	Automated reconciliation			
FR-17	Partial/over/short/duplicate payment handling			
FR-18	Receipts and employer history			
FR-19	VNPF work queues and dashboards			
FR-20	Notifications and reminders			
FR-21	Audit trail and evidence export			

ID	Requirement	C/PC/R/NC	Standard / Config / Custom	Comments / evidence
FR-22	Operational/admin configuration			
FR-23	Reporting/export			
FR-24	API/webhook integration			
FR-25	Historical data search and retrieval			

Appendix B – Technical Architecture Information Requested

- Logical and physical architecture diagrams, including trust boundaries and data flows.
- Hosting model, cloud regions/data residency options, availability zones and major managed services.
- Application/service architecture, technology stack, supported versions and end-of-life management.
- Database/storage architecture, encryption, backup and recovery approach.
- Identity and access architecture for employer users, VNPF users and privileged administrators.
- API gateway, integration, messaging/event and batch/file components.
- Payment orchestration and bank adapter architecture.
- Logging, monitoring, tracing, SIEM/SOC integration and operational dashboards.
- DevSecOps pipeline, environment strategy, infrastructure/configuration as code and release controls.
- Security architecture including WAF, DDoS, secrets, keys, certificates, vulnerability management and penetration testing.
- Data retention, archival, disposal and exit/export architecture.
- Capacity model, tested performance envelope and scaling strategy.

Appendix C – Indicative End-to-End Process

Step	Target process
1	Employer signs in securely and selects contribution period.
2	Employer creates/uploads/submits contribution schedule.
3	Platform performs schema, business, contribution and member validation.
4	Member matching and cleansing services resolve or route exceptions.
5	Employer corrects blocking issues and submits final schedule.
6	Authorised approver confirms schedule; platform creates CTR.
7	Employer selects supported payment channel; orchestration gateway initiates secure payment journey.
8	Bank/provider authenticates employer and processes payment outside VNPF credential boundary.
9	Payment status/settlement evidence returns to orchestration and clearing services.
10	Clearing house matches settled funds to CTR and contribution schedule.
11	Reconciliation validates totals and routes exceptions for controlled resolution.
12	Allocation-ready contribution data is transmitted to VNPF core/member system.
13	Employer receives receipt/status; VNPF dashboards and audit trail are updated.

Appendix D – Key Definitions

Term	Definition for this EOI
Contribution Schedule (CS)	Employer-submitted detail of member/employer contributions for a contribution period.
CTR	Contribution Transaction Request: controlled financial obligation generated from an accepted contribution schedule.
Clearing House	Service that links contribution obligations, settlement events, exceptions and allocation-ready records.
Payment Orchestration	Layer that creates/routes payment requests and normalises status across supported banks/payment providers.
Member Matching	Process of associating employer-submitted employee data with the correct VNPF member record.
Straight-through processing	Automated processing of valid transactions without unnecessary manual intervention.
Idempotency	Control ensuring repeated submission of the same transaction request does not create duplicate financial outcomes.
POC	Proof of Concept demonstration using defined VNPF scenarios and test data.