Annexure 2: Non-Functional Requirements (NFR)

GovStack Foundation Building Blocks

Part 1: Common NFRs Across All Building Blocks | Part 2: Building-Block-Specific NFRs

Table of Contents

Building Blocks in Scope **3**
Introduction **4**
Part 1: Common Non-Functional Requirements **4**
1.1. Performance Efficiency 4
1.2. Reliability & Availability 6
1.3. Security 8
1.4. Data management and privacy 11
1.5. Usability & Accessibility 12
1.6. Maintainability 13
1.7. Portability & Architecture 14
1.8. Interoperability 15
1.9. Compliance & Legal 16
1.10. Service Levels 17
1.11. Organisational & Delivery 17
1.12. Environment Strategy 20
Part 2: Building-Block-Specific Non-Functional Requirements **20**
2.1 Single Sign-On (SSO) 21
2.2 Identity Conversion Block (IDCB) 22
2.3 Master Data Management Block (MDMB) 24
2.4 Feedback Block (FDBKB) 25
2.5 Public Service Registry (PSR) 28
2.6 Unified Client Support (UCS) 29
2.7 IT Asset Repository (ITAR) 30
APPENDICES **31**
Appendix A: Glossary of Abbreviations 31

Building Blocks in Scope

Code	Building Block	Primary Domain
SSO	Single Sign-On	Authentication, session, federation, token lifecycle
PSR	Public Service Registry	Service & system catalogue, taxonomy, search
MDMB	Master Data Management Block	Golden-record matching, survivorship, master data distribution
FDBKB	Feedback Block	Feedback collection, analytics, dashboards
IDCB	Identity Conversion Block	Pseudonymised identity conversion, mapping lifecycle
UCS	Unified Client Support	Citizen support services
ITAR	IT Asset Repository	Single product portal of GovStack building blocks

Introduction

This document consolidates the Non-Functional Requirements (NFRs) of the BRDs of the seven GovStack Foundation Building Blocks listed above into a single specification, structured in two parts:

Part 1: Common NFRs: quality attributes and targets that apply, as a floor, across all seven Building Blocks. These were derived by comparing the NFR sections of the BRDs and extracting the requirements that recur across most or all of them, harmonised to a single consistent target where the source documents used different wording or thresholds for materially the same outcome.

Part 2: Building-Block-Specific NFRs: requirements that are unique to a block's domain (e.g. pseudonymisation guarantees for IDCB, golden-record match latency for MDMB).

Part 1: Common Non-Functional Requirements

The following twelve sections state the Non-Functional Requirements that apply, as a binding minimum, to all seven Building Blocks. Where Part 2 sets a stricter target for a block, the Part 2 target applies; a Part 2 target shall not be weaker than Part 1. Where this specification conflicts with the ToR, the ToR prevails (ToR Section 3.3).

1.1. Performance Efficiency

ID	Requirement	Common Target	Verification
CP-PERF-01	Synchronous API response time	95% ≤ 300 ms read, ≤ 500 ms write; 99%≤ 2× the 95% target	Load Test
CP-PERF-02	Page/dashboard load time	95% ≤ 3 s to interactive on the reference client	Synthetic monitoring / Real user monitoring (RUM)
CP-PERF-03	Database query performance	95% ≤ 100 ms for indexed single-table reads	Load Test
CP-PERF-04	Provisioned capacity	Each block provisioned to its peak concurrency and throughput, sustained for 60 minutes with all other targets met	Load Test
CP-PERF-05	Scalability headroom	Architecture shall sustain 10× the peak by horizontal scaling alone, without	Design review plus scaled load test

		redesign, re-platforming, or schema change	
CP-PERF-06	Capacity headroom in operation	≥ 20% spare capacity maintained at observed peak; breach triggers a capacity review within 10 business days	Capacity report
CP-PERF-07	Auto-scaling response	Scale-out decision to serve traffic ≤ 5 minutes; scaling linear to at least 4× baseline instance count	Load test
CP-PERF-08	Behaviour beyond capacity	Under overload, the system shall shed non-critical load, queue, or return HTTP 429/503 with Retry-After. It shall not fail uncontrolled, lose accepted writes, or cascade to callers. Entry to and exit from a degraded state shall be logged and alerted	Stress test to 150% of peak
CP-PERF-09	Batch and asynchronous processing	Bulk, long-running, and report work shall run asynchronously and shall not degrade interactive 95% by more than 10% while running	Load test
CP-PERF-10	Caching effectiveness	Where a block caches data (e.g. PSR catalogue, MDMB code lists): ≥ 85% hit ratio, with invalidation on state change. Time-based expiry alone is not sufficient for state-changing data	Metrics review
CP-PERF-11	Endurance	72-hour soak at normal load with no memory growth trend, connection-pool exhaustion, or 95% degradation beyond 10%	Soak test
CP-PERF-12	Capacity plan	A capacity plan covering users, transactions, API calls, data volume, peak profile, and 3-year growth shall be maintained and reviewed at each major release	Document review
CP-PERF-13	Search index freshness	For blocks with search: ≥ 95% of published or updated records searchable within 5 min; 100% of withdrawn or expired records removed within 5 min	Integration test

1.2. Reliability & Availability

ID	Requirement	Common Target	Verification
CP-REL-01	Service availability (baseline, monthly)	≥ 99.9%, excluding pre-announced maintenance windows.	Synthetic monitoring, Real user monitoring
CP-REL-02	Resilience tiering	Every block is assigned a tier. Tier 1: RTO ≤ 30 min, RPO ≤ 15 min. Tier 2: RTO ≤ 1 h, RPO ≤ 15 min. Tier 3: RTO ≤ 2 h, RPO ≤ 15 min. Tier 4: RTO ≤ 4 h, RPO ≤ 30 min	Document review, DR drill
CP-REL-03	Mean Time To Recovery (MTTR)	P1 (Critical) incidents: service restored within the block's resilience-tier RTO (CP-REL-02) and not later than the P1 restoration time in Annexure 8, Section 5.2	Incident Records
CP-REL-04	Backup baseline	Database backups ≥4×/week, application backups ≥2×/week, minimum 7-day retention, with at least one immutable/offline (WORM or air-gapped) copy per backup set; off-site storage alone does not satisfy immutability	Configuration review
CP-REL-05	Backup restoration testing	Tested at minimum quarterly; each test verifies recoverability and integrity and records actual restoration time	Restore drill report
CP-REL-06	Disaster Recovery drills	Conducted at least annually (service, node, and site recovery scenarios); pre-go-live site-recovery exercise mandatory.	DR drill report
CP-REL-07	Multi-zone / multi-facility deployment	Development, QA, Staging and Production deployed as separate zones within Bhutan, in the interim hosting environment and later GovCloud (Section 1.12); Production spread	Architecture review

		across at least two availability zones where the hosting environment provides them.	
CP-REL-08	Monitoring detection latency	A qualifying failure (one that would breach availability or RTO targets) shall generate an alert to the responsible operations team within 5 minutes of occurrence	Monitoring and Alert test
CP-REL-09	Graceful degradation	Core functions remain available in read-only/cached mode if a downstream dependency is unavailable; user-facing error messages during partial outage	Dependency failure test, Design review
CP-REL-10	Dependency recovery planning	Recovery plans cover application, database, storage, messaging, identity and every other critical dependency	Document review
CP-REL-11	Recovery testing and evidence	Recovery tests demonstrate the tier's RTO and RPO; results of backup and DR tests are retained and available for verification	Test evidence review
CP-REL-12	Planned maintenance	≤ 4 h/month, between 22:00 and 06:00 Bhutan time, with ≥ 72 h notice to consuming blocks and users. Blocks with zero-downtime deployment incur no user-visible outage. Unnotified maintenance counts as downtime	Maintenance records
CP-REL-13	Timeouts and circuit breakers	Every outbound synchronous call has a timeout (≤ 3 s unless documented), retry with exponential backoff and jitter, and a circuit breaker	Dependency failure test
CP-REL-14	Audit-sink resilience	If JLB is unavailable, audit events are queued durably and replayed in order on recovery, with zero loss. A backlog older than 15 min raises an alert	Failure test
CP-REL-15	Messaging reliability	Event publishing is at-least-once with acknowledged, idempotent delivery; consumers are idempotent; a dead-letter queue with alerting catches failures; zero loss of accepted events	Integration and failure test

CP-REL-16	Idempotent (same request) submission	Create and submit APIs accept an idempotency key, so client retries never create duplicates	Integration test

1.3. Security

ID	Requirement	Common Target	Verification
CP-SEC-01	Encryption at rest	AES-256 for all databases, object storage, and message queues holding personal or transaction data	Configuration review, Technical Test
CP-SEC-02	Encryption in transit	TLS 1.2 minimum; TLS 1.3 mandatory for new integrations; no unencrypted service-to-service traffic	TLS scan
CP-SEC-03	Key and certificate management	Keys rotated every 90 days; HSM-backed key storage for signing and pseudonymisation keys; no software-only keys and no expired certificates in production	Configuration review
CP-SEC-04	Vulnerability management	Vulnerability scans; Critical ≤ 7 days, High ≤ 15 days (Annexure 3, Section 2.1; Annexure 8, Section 5.2); annual (minimum) third-party penetration testing	Scan reports, remediation tracker
CP-SEC-05	Audit logging	100% of security-relevant events (authN/authZ, data access, config change) logged to the Journaling/Logging Block (JLB); logs tamper-evident/immutable; retained ≥ 7 years	Log review
CP-SEC-06	Security Standard	OWASP Top 10 verification; OWASP ASVS Level 2 for every block and Level 3 for SSO and IDCB; ISO/IEC 27001 control alignment; SOC 2 Type II readiness; NIST alignment where cited.	Audit

CP-SEC-07	In-country hosting / data residency	All Development, QA, Staging and Production, backup, replication and DR processing occurs exclusively within Bhutan, in environments approved by the PA (ToR Section 10.1; Section 1.12); no data or metadata is processed or cached outside Bhutan	Architecture and configuration review
CP-SEC-08	Independent penetration testing	Third-party test before go-live, after each major release, and at least annually; findings remediated within the CP-SEC-04 timelines	Pen-test report
CP-SEC-09	API protection	API gateway with per-consumer rate limiting (HTTP 429 with Retry-After); in-country DDoS mitigation; API keys stored hashed (SHA-256 or stronger)	Security test
CP-SEC-10	Input validation & injection prevention	All inputs validated & sanitised; SQL-injection, XSS, and CSRF prevention; schema validation	SAST, DAST
CP-SEC-11	Software and cryptographic bills of materials	SBOM and CBOM shall cover applications, libraries, packages, containers, and third-party components and be updated throughout the lifecycle.	SBOM and CBOM review
CP-SEC-12	Container security shall be enforced.	Container images shall be scanned and hardened; only approved images shall be deployed to production.	Pipeline review
CP-SEC-13	Secrets shall be securely managed.	Passwords, API keys, certificates, tokens, and other secrets shall not be stored in source code and shall use approved secrets management.	Code scan
CP-SEC-14	Privileged access shall be controlled.	Least privilege, MFA where applicable, access review, logging, and attributable administrative access shall be enforced.	Access review records

CP-SEC-15	Security testing in CI/CD	SAST, DAST, dependency, container, API, penetration, and other applicable security testing shall be performed.	Pipeline review
CP-SEC-16	Authentication shall be secured.	Approved enterprise/national authentication mechanisms shall be used where applicable, with secure credential and session handling.	Integration test
CP-SEC-17	Authorization shall be enforced.	RBAC and/or policy-based access control shall follow least privilege and deny-by-default principles.	Access-control test
CP-SEC-18	Sessions and tokens shall be protected.	Token/session lifetime, expiration, revocation, secure storage, and replay protection shall be implemented.	Security test
CP-SEC-19	Service-to-service authentication	Mutual TLS for all internal service calls, using certificates issued by the RGoB PKI	Configuration review
CP-SEC-20	Web application hardening	CSP, HSTS and frame-ancestors headers; Secure, HttpOnly and SameSite cookies; CSRF tokens on every state-changing request	Header scan, DAST
CP-SEC-21	Bot and abuse protection	Public submission forms protected by an in-country CAPTCHA or equivalent; no third-party service that sends user data outside Bhutan	Bot-detection test
CP-SEC-22	File uploads	Type allow-list and size limit per block (Part 2); every file malware-scanned before it can be listed, previewed, downloaded, shared or attached; infected files quarantined and the user told. A 10 MB file is scanned in $\leq$ 30 s; the upload acknowledgement does not wait for the scan	Security test
CP-SEC-23	Multi-tenant isolation	No tenant can read or write another tenant's data through any interface (UI, API, export or search); a load spike in one tenant causes no measurable degradation in another	Isolation and load test

CP-SEC-24	Incident and breach notification	Security incidents reported to the PA (GovTech) within 24 h of discovery (ToR Section 10); personal-data breaches notified to the regulator and affected people within 72 hours	Incident records
CP-SEC-25	SIEM integration	Security events forwarded to the government SIEM within 60 s	Integration test

1.4. Data management and privacy

ID	Requirement	Common Target	Verification
CP-DATA-01	Data classification	Data classified and handled per the Government-approved classification scheme	Data inventory review
CP-DATA-02	Data integrity	Data protected against unauthorised or unintended change throughout its lifecycle	Security test
CP-DATA-03	Data quality	Critical data meets defined accuracy, completeness, consistency and validity rules, checked on write	Data-quality report
CP-DATA-04	Retention schedules	Data retained per approved retention schedules and legal requirements	Retention audit
CP-DATA-05	Secure deletion	Data securely deleted when retention expires; deletion auditable	Deletion test
CP-DATA-06	Non-production data	No production data in non-production environments unless authorised and masked, anonymised or otherwise protected	Environment review
CP-DATA-07	Data export	All Government data exportable in open, documented, non-proprietary formats (JSON, CSV, XML)	Export test
CP-DATA-08	Controlled migration	Migration includes mapping, transformation, validation, reconciliation, rollback and approval procedures	Migration plan review
CP-DATA-09	Data-subject rights	Access, rectification, erasure and portability fulfilled within 30 days. After erasure, individual data is	Functional test

		unrecoverable except records the law requires and anonymised aggregates; every erasure is logged	
CP-DATA-10	Privacy impact assessment	DPIA completed before go-live and on every material change to personal-data processing	DPIA review
CP-DATA-11	Consent and cookies	Consent recorded, versioned and withdrawable; non-essential cookies set only after consent; web analytics hosted in-country	Cookie and consent test
CP-DATA-12	Minimisation and purpose limitation	Only necessary personal data collected; the purpose and legal basis recorded for every personal-data flow; optional fields clearly marked	Data-flow review
CP-DATA-13	Concurrency control	Concurrent edits to the same record are never silently overwritten (e.g., optimistic locking with version check)	Concurrency test

1.5. Usability & Accessibility

ID	Requirement	Common Target	Verification
CP-USE-01	Accessibility standard	WCAG 2.1 Level AA on all user-facing interfaces, including citizen-facing screens, admin screens and embeddable widgets; keyboard navigation; screen-reader support; contrast ≥ 4.5:1. Both automated and manual accessibility testing before acceptance.	Accessibility testing
CP-USE-02	Responsive design	The system must be mobile-friendly from 320px and above, adapt to different screen sizes, have easy-to-tap buttons (≥44×44px), and avoid horizontal scrolling. Where required, citizen-facing systems should be installable as PWAs (like an app).	Device testing
CP-USE-03	Usability acceptance	The system should be easy to use: SUS score of 70 or higher, at least 85% of tasks completed successfully, and less than 5% user errors.	User testing

CP-USE-04	Learnability	First-time/novice users should be able to complete the primary task without training within a block-appropriate time bound	User testing
CP-USE-05	Error handling	Error messages should be clear and helpful without showing technical system or developer errors to users.	UI review
CP-USE-06	Browser compatibility	Support and document the latest Government approved/supported versions of Chrome, Firefox, Safari, and Edge.	Compatibility testing
CP-USE-07	Design system conformance	All user interfaces built from the Unified Design System(UDS) as published by GovTech Agency.	Design review
CP-USE-08	Error prevention	The system should quickly validate user inputs with feedback < 100 ms, ask for confirmation before deleting or other destructive actions, warn users about unsaved changes, and clearly mark required and optional fields.	UI testing
CP-USE-09	Web standards	The website must use proper, standards-compliant HTML5 and CSS3 code.	W3C validator

1.6. Maintainability

ID	Requirement	Common Target	Verification
CP-MAINT-01	Automated test coverage	≥ 80% coverage for new code; regression suite executed in CI on every merge	CI report
CP-MAINT-02	Deployment and rollback	Zero-downtime (e.g., blue-green or rolling) deployment; automated rollback ≤15 minutes	Deployment and rollback test
CP-MAINT-03	Code quality	The code should undergo static analysis in CI, maintain a technical-debt ratio < 5% (SonarQube or equivalent), enforce linting, and have every change reviewed by at least one independent reviewer.	Static analysis report
CP-MAINT-04	Documentation	API documentation should be automatically published using OpenAPI, and all architecture, runbook, admin, and user	Document review

		documentation should be updated with every release.	
CP-MAINT-05	Observability	Structured logs, metrics, and distributed traces with correlation identifiers, compatible with the government observability stack (e.g., OpenTelemetry / Prometheus or equivalent)	Observability review
CP-MAINT-06	configuration-driven change	New configuration (e.g. a form field, a reference-code value, a new domain) deployable via admin UI without core code changes	Configuration test
CP-MAINT-07	Horizontal scalability & stateless design (Kubernetes / HPA)	Stateless, containerised services; Kubernetes HPA auto-scaling on CPU / queue-depth; no shared instance state	Design review, load test
CP-MAINT-08	Automated testing shall be implemented.	Unit, integration, regression, API, security, and end-to-end tests shall be automated where applicable and integrated with CI/CD.	Pipeline review
CP-MAINT-09	Database change control	Schema and data migrations shall be version-controlled, repeatable, traceable, and reversible where technically feasible.	Migration review
CP-MAINT-10	Deployment rollback shall be supported.	Production releases shall have a tested rollback mechanism and recovery to the previous stable version.	Demonstration and rollback testing
CP-MAINT-11	Health endpoints	Liveness and readiness endpoints on every service, used by the orchestrator and monitoring	Configuration review

1.7. Portability & Architecture

ID	Requirement	Common Target	Verification
CP-PORT-01	Containerisation	All services packaged and deployed as containers (Docker/Kubernetes); Helm charts or equivalent manifests published	Deployment test

CP-PORT-02	Stateless services	Application-tier services are stateless; session and state held in a shared store; horizontal scaling through Kubernetes HPA on CPU, memory, or queue depth, with no sticky sessions.	Design review/load testing
CP-PORT-03	Cloud/infrastructure independence	No mandatory dependency on a specific proprietary cloud provider beyond the Government-provided baseline infrastructure	Architecture review
CP-PORT-04	Environment parity	The system has four separate environments, consistently configured: Development, QA, Staging, and Production environments	Environment review
CP-PORT-05	Infrastructure portability shall be supported.	Applications shall be deployable on approved Government Kubernetes/container environments without significant redesign.	Deployment testing
CP-PORT-06	Infrastructure as code	Deployment, infrastructure and application configuration maintained as code in the Procuring Agency's repository	Repository review
CP-PORT-07	Transferability	Source code, configurations, documentation, deployment artefacts, and operational knowledge shall be transferable to the Government or another supplier.	Exit-plan review

1.8. Interoperability

ID	Requirement	Common Target	Verification
CP-INTOP-01	API standard	OpenAPI 3.0 or later specification for every API; RESTful design; no mandatory proprietary SDK to consume an API	API review/integration testing
CP-INTOP-02	Event standard	All event-driven integration through the Message Broker / Event Bus shall use CloudEvents-compliant payloads with standardized event metadata.	Integration testing

CP-INTOP-03	Error format	All building blocks shall use standardised error responses based on RFC 7807 Problem Details or equivalent format.	API / integration testing
CP-INTOP-04	GovStack alignment	Conformance with the applicable GovStack Building Block API specification for the block's domain	API conformance testing
CP-INTOP-05	Data exchange formats	All data import, export, and bulk interfaces must use open, documented, non-proprietary formats (JSON/XML/CSV)	Interface testing
CP-INTOP-06	API versioning and deprecation	Semantic versioning; breaking changes only in a new major version; during implementation, interfaces between Building Blocks follow ToR Section 3.5 (previous version supported for at least one release or 90 days, whichever is longer); after Go-Live, the previous major version is supported for ≥ 6 months after ≥ 6 months' notice to all registered consumers	API lifecycle review
CP-INTOP-07	Platform integration	Authentication through NDI/SSO, and events through the Event Bus; data sharing with other agencies through NDE where applicable. No block duplicates a platform service	Architecture review

1.9. Compliance & Legal

ID	Requirement	Common Target	Verification
CP-COMP-01	Data protection	Compliance with the Information, Communications and Media Act of Bhutan 2018, the National Digital Identity Act of Bhutan 2023, e-Governance Policy for the Royal Government of Bhutan 2019, RGoB information security policies, the data-protection legislation in force (currently the Draft Data Protection Bill), and GDPR principles (data minimisation, purpose	Legal review

		limitation, consent, right to erasure/portability) where applicable	
CP-COMP-02	Accessibility compliance	WCAG 2.1 AA with a published accessibility statement and periodic (minimum quarterly) audit	Accessibility audit report
CP-COMP-03	Audit/record retention	Minimum 7-year retention for audit logs; retention schedules per national records-management requirements for master/reference data (should be configurable)	Retention audit
CP-COMP-04	Standards alignment	ISO/IEC 27001:2022 (security); CPSV-AP and ISO 15836 Dublin Core (service metadata, where applicable); NIST SP 800-63B and SP 800-162 (identity and access, where applicable)	Compliance review
CP-COMP-05	License inventory	Consolidated inventory of every open-source and third-party component and its licence, reviewed with each release.	Inventory review
CP-COMP-06	Continuous compliance review	Changes to applicable laws, regulations, standards, and Government policies shall be monitored and addressed.	Compliance report
CP-COMP-07	Licence restrictions	No licence restricts Government ownership, use, modification, deployment, or redistribution	Legal review
CP-COMP-08	Third-party component approval	New third-party components shall undergo security, licensing, technical, and Government approval where required.	Approval records

1.10. Service Levels

Incident severity levels and response, restoration and resolution times for Production are set out in Annexure 8, Section 5.2, which is the single source for these figures. Defect severity levels for testing and UAT are set out in Annexure 3, Section 1.7. The availability, recovery and performance targets in this specification apply in addition.

1.11. Organisational & Delivery

ID	Requirement	Common Target	Verification
CP-ORG-01	Milestone delivery	Delivery in defined milestones, each closed by User Acceptance Testing sign-off against this specification.	UAT sign-off
CP-ORG-02	Change management	All production changes are tracked in a change log; no Change Request proceeds to implementation without written approval in accordance with ToR Section 13 and Annexure 4, recorded prior to any code or configuration change reaching the production environment.	Change-log audit
CP-ORG-03	Operational readiness	An Operational Readiness Checklist (runbooks, monitoring, support handover, DR drill evidence, training completion) is signed off before production go-live	Checklist sign-off
CP-ORG-04	Support tiers	As set out in Annexure 8, Section 5.1: L1 by the PA/GovTech helpdesk; L2 and L3 by the Vendor; working-hours support for P2–P4 and 24/7 for P1	Support records
CP-ORG-05	Training and documentation handover	Administrator training and end-user documentation delivered before go-live, in English and where the BRD requires, Dzongkha (ToR Sections 15.2 and 16.3)	Training records, document review
CP-ORG-06	Reporting cadence	Reports submitted to the PA (GovTech) as set out in Annexure 3, Section 1.2	Document review
CP-ORG-07	Source Code Management	All source code, configuration, and infrastructure-as-code artifacts maintained in a version-controlled repository maintained by the Procuring Agency; branching strategy documented; no direct commits to the release/production branch — all changes via reviewed pull/merge request with a minimum of one independent approver; full commit history and release tags preserved for the contract's duration and handed over in full upon exit	Repository audit

CP-ORG-08	Defect Lifecycle	Every defect tracked through a defined state machine (New → Assigned → In Progress → Fixed → Retest → Closed, with Reopened/Rejected as exit states); state transitions timestamped and attributable; defect status queryable against the severity levels in Annexure 3, Section 1.7 (testing and UAT) and Annexure 8, Section 5.2 (Production) at any time, not only at resolution	Tracker audit
CP-ORG-09	Knowledge transfer shall be provided	Government technical and operational teams shall receive sufficient training and documentation to operate and maintain the solution.	Competency sign-off
CP-ORG-10	Security handover shall be completed	Security configurations, certificates, secrets ownership, open vulnerabilities, and security documentation shall be transferred to the PA (GovTech).	Handover record
CP-ORG-11	Operational runbooks shall be provided.	Runbooks for deployment, monitoring, backup, recovery, troubleshooting, administration, incident response, and handling each dependency outage.	Runbook review
CP-ORG-12	Architecture decisions shall be documented.	Significant architectural decisions, rationale, alternatives, and consequences shall be maintained as ADRs or equivalent.	ADR review
CP-ORG-13	Exit and transition	Exit Plan delivered with the Source Code, Documentation, Training and Knowledge Transfer deliverable and updated as set out in Annexure 8, Section 20; on exit, full handover of code, data, configuration and documentation, with up to 60 days of transition support (ToR Section 7.2.4)	Exit-plan review
CP-ORG-14	Warranty	Defects corrected at no additional cost from Go-Live until the end of the 12-month Warranty Period starting on Final Acceptance (ToR Section 14.1; Annexure 8)	Contract review

1.12. Environment Strategy

ID	Requirement	Common Target	Verification
CP-ENV-01	Environments	Four separate, consistently configured environments per Lot: Development, QA, Staging, and Production (CP-PORT-04)	Environment review
CP-ENV-02	Interim hosting	Until GovCloud is ready, Building Blocks are hosted in the interim environment [provided by the PA / provided by the Vendor within Bhutan, as approved by the PA]. Any part the Vendor provides meets this specification and is priced separately (ToR Section 12.3)	Architecture review, R7 SLA report
CP-ENV-03	Staging parity	Staging mirrors Production in topology, versions, and configuration, scaled down only where the PA approves; used for performance testing and pre-release verification	Environment review
CP-ENV-04	Non-production data	As CP-DATA-06 and ToR Section 10.1	Environment review
CP-ENV-05	GovCloud readiness	Every block deployable to GovCloud through IaC and Helm charts without code change; migration plan, data reconciliation and rollback documented before migration (ToR Section 5.1)	Migration plan review
CP-ENV-06	Decommissioning	Vendor-provided parts of the interim environment decommissioned and data destroyed after migration (ToR Sections 5.4 and 10.1)	Certificate of destruction

Part 2: Building-Block-Specific Non-Functional Requirements

For each building block, this Part lists only (a) domain-specific NFRs that are materially different from, or add precision to, the Part 1 common baseline, and (b) NFRs added during this consolidation because a Functional Requirement had no corresponding NFR, or because a

quality attribute was absent from that block's BRD. Requirements not repeated here are governed by the Part 1 common baseline.

2.1 Single Sign-On (SSO)

ID	Requirement	Target / Note
1. NDI Fallback Resilience		
SSO-NFR-1.1	Failure-domain independence from NDI	No shared hosting, network path, DNS, database, cache, identity store, or certificate chain with NDI; verified by architecture review
SSO-NFR-1.2	NDI outage detection time	Outage detected and login page switched to fallback within ≤60 s (2 health-check intervals)
SSO-NFR-1.3	NDI recovery switch-back	NDI route restored within one health-check interval of recovery, with no forced logout of fallback sessions
SSO-NFR-1.4	Fallback drills	Failover to fallback mode tested at least quarterly in production-like conditions, with results reported
SSO-NFR-1.5	Availability during NDI outage	SSO fallback route ≥99.95% available during any NDI outage period
2. Dependency Resilience		
SSO-NFR-2.1	OTP delivery availability	NTFB OTP delivery ≥99.9%; SMS delivered in ≤30 s (95%). Because MFA is mandatory, an NTFB outage blocks all fallback logins
SSO-NFR-2.2	Multi-channel OTP	At least two independent SMS providers or channels; TOTP always usable without NTFB
SSO-NFR-2.3	Circuit breakers and timeouts	Every external call has timeout ≤3 s, retry with backoff and a circuit breaker; failures never cascade to the login page
SSO-NFR-2.4	JLB outage buffering	Audit events buffered durably and replayed when JLB is unavailable; zero audit event loss
3. Observability and Monitoring		
SSO-NFR-3.1	Metrics and dashboards	Real-time metrics for login success/failure per route, OTP delivery, NDI status, latency, and error rate
SSO-NFR-3.2	Alerting	Alert operations within ≤1 minute for NDI down, fallback activated, error rate >5% or OTP failure spike

SSO-NFR-3.3	Distributed tracing	Correlation ID carried end-to-end across SSO, NDI, NTFB, JLB and SPs
SSO-NFR-3.4	SIEM integration	Security events forwarded to SIEM within ≤60 s
4. Maintainability and Operability		
SSO-NFR-4.1	Zero-downtime deployment	Rolling releases with no session loss
SSO-NFR-4.2	Environment separation	Separate Development, QA, Staging, and Production; no production data in lower environments without masking
SSO-NFR-4.3	Configuration without code change	Timeouts, policies, SP restrictions, and health-check intervals configurable at runtime
SSO-NFR-4.4	Documentation	Operations runbooks, including an NDI-outage playbook, OpenAPI 3.0 specs and an SP integration guide
SSO-NFR-4.5	Automated testing	Unit, integration, load and security tests in CI/CD; minimum coverage threshold (e.g. 80%)
5. Portability and Vendor Neutrality		
SSO-NFR-5.1	Open standards	Uses only open protocols (OIDC, OAuth 2.0, SAML 2.0) with no proprietary SP client libraries required

2.2 Identity Conversion Block (IDCB)

ID	Requirement	Target / Note
1. Performance		
IDCB-NFR-1.1	Conversion latency	95% of synchronous conversions shall complete within <50 ms, from request receipt to pseudonym returned.
IDCB-NFR-1.2	Reverse resolution	95% of reverse-resolution requests shall complete within <50 ms, from request to domain reference returned.
IDCB-NFR-1.3	Temporary token generation	95% of temporary-token requests shall complete within <30 ms.
IDCB-NFR-1.4	Explainability overhead	When explain=true, the additional processing time shall be ≤20 ms for 95% of requests.
IDCB-NFR-1.5	Admin and consumer UIs	Admin dashboard cold load shall be **<2 s** and consumer self-service dashboard load **<1 s**.

2. Availability and Resilience		
IDCB-NFR-2.1	Resilience tier	Tier 1 resilience with RTO <30 min and RPO <5 min for the identity graph and mapping store; audit logs shall have RPO = 0.
IDCB-NFR-2.2	Degraded mode	When upstream registries are unavailable, cached conversions for registered domain pairs shall continue to work, and responses shall be clearly marked as degraded.
3. Security		
IDCB-NFR-3.1	Pseudonymisation guarantee	Original/base identifiers shall never appear outside IDCB, including in APIs, logs, traces, metrics, error messages or dashboards.
IDCB-NFR-3.2	Domain unlinkability	Pseudonyms from different domains shall not be linkable without IDCB; domain identifiers shall use protected cryptographic methods.
IDCB-NFR-3.3	Key versioning	Keys shall be rotated every 90 days without changing existing pseudonyms; every mapping shall record its key version.
IDCB-NFR-3.4	Consumer tokens	Every request shall use a JWT with a maximum lifetime of 1 hour; long-lived API tokens shall not be used.
IDCB-NFR-3.5	Scope enforcement	Consumers shall have least-privilege scopes; violations shall trigger a security alert and may automatically suspend the caller.
4. Privacy, Data Governance and Compliance		
IDCB-NFR-4.1	Purpose limitation	Every conversion shall use a registered and authorised purpose; unauthorised resolution requests shall be refused.
IDCB-NFR-4.2	Legal-basis traceability	Every active conversion context shall reference a legal authority, and legal_basis_ref shall be mandatory before publishing a rule.
IDCB-NFR-4.3	Response minimisation	Responses shall contain only the fields permitted by the registered rule and declared purpose.
IDCB-NFR-4.4	Citizen rights	Citizen-facing systems shall support subject-access requests, and incorrect conversion results shall be able to be disputed.

IDCB-NFR-4.5	Mapping retention	Expired or revoked mappings shall be retained for ≥3 years for forensics; active mappings shall be retained for the policy lifetime + 1 year.
5. Operations and Onboarding		
IDCB-NFR-5.1	Consumer onboarding	A new consumer shall be registered and complete its first successful conversion within ≤5 business days.

2.3 Master Data Management Block (MDMB)

ID	Requirement	Target / Note
1. Performance and Scalability		
MDMB-NFR-1.1	Lookup/match latency	95% of single-record lookups and real-time matches within 2 seconds under peak load. Batch ingestion shall complete within 5 seconds for 95% of batches of up to 1000 records.
MDMB-NFR-1.2	Scalability	The system shall support 50 tenants, 1 million golden records and 80 peak lookups per second, and shall scale to 10× (CP-PERF-05) this baseline without breaching MDMB-NFR-1.1.
2. Availability and Recoverability		
MDMB-NFR-2.1	Availability	The system shall be available ≥ 99.9% monthly, excluding scheduled maintenance windows notified to tenants at least 72 hours (CP-REL-12) in advance.
MDMB-NFR-2.2	Recoverability/ freshness	RPO ≤ 15 minutes and RTO ≤ 1 hour. A change to a golden record shall be reflected in each consuming system within its agreed synchronization SLA. Search index refresh ≤ 5 minutes.
MDMB-NFR-2.3	Change notification delivery	Notifications of a create, amend, deactivate, merge, or unmerge shall be delivered at least once to subscribed consuming systems within 60 seconds, with automatic retry on failure.
3. Security and Privacy		

MDMB-NFR-3.1	Encryption specifics	AES-256 at rest and TLS 1.3 (minimum TLS 1.2) in transit for all master-data stores and APIs, with encryption keys held in a managed key service.
MDMB-NFR-3.2	Tenant isolation	No tenant shall be able to read or write another tenant's unpublished or draft data through any interface (UI, API or export).
MDMB-NFR-3.3	No personal data	The system shall prevent storage of personal data. Field definitions shall be checked against a prohibited-attribute list (e.g., CID number, individual name, date of birth) before activation.
4. Data Integrity and Stewardship		
MDMB-NFR-4.1	Concurrency control	Concurrent amendments to the same record shall not silently overwrite each other (e.g., through optimistic locking).
MDMB-NFR-4.2	Steward review turnaround	95% of flagged match/survivorship conflicts shall be reviewed by a data steward within 2 business days. The system shall track task ageing and escalate overdue tasks to the tenant administrator.
MDMB-NFR-4.3	Data-quality reporting	The system shall report data-quality indicators per domain and per tenant, including completeness, duplicate rate, open steward tasks and task ageing.
5. Auditability and Monitoring		
MDMB-NFR-5.1	Audit delivery resilience	If JLB is unavailable, audit events shall be queued durably and delivered in order once JLB recovers, with zero loss. A change shall not be committed unless its audit event is persisted.
6. Maintainability and Compliance		
MDMB-NFR-6.1	Configurability	New entity domains, fields and hierarchy structures shall be configurable by an authorised administrator without a code release (FR-1.2, FR-1.3).

2.4 Feedback Block (FDBKB)

ID	Requirement	Target/Note

1. Performance		
FDBKB-NFR-1.1	API performance per Node	Each Node must respond quickly: 95% of submissions <500 ms and 99% <1,000 ms; 95% of retrieval requests <300 ms; 95% of searches <1,000 ms; 95% of analytics requests <2,000 ms.
FDBKB-NFR-1.2	Page-load performance	Pages must load quickly: FCP <1.5 s, LCP <2.5 s, TTI <3.5 s on 4G; dashboard initial load <2 s.
FDBKB-NFR-1.3	Database performance per Node	Simple indexed queries <50 ms; complex aggregations <500 ms; 95% of full-text searches <200 ms; report generation <5 s.
FDBKB-NFR-1.4	Live dashboard refresh	Feedback volume counter shall refresh within <30 s.
FDBKB-NFR-1.5	Federated query performance	Queries across up to 50 Nodes shall complete within ≤15 s for cached/scheduled views and ≤60 s for on-demand live queries.
2. Availability and Resilience		
FDBKB-NFR-2.1	Partial federated results	A Node that times out shall not block the overall response; the Node shall be reported as "data unavailable".
FDBKB-NFR-2.2	Node failure isolation	An outage, load spike or breach at one Node shall not affect the availability, performance or data of other Nodes.
FDBKB-NFR-2.3	Resilience tier	Each Node shall have RTO ≤4 hours and RPO ≤30 minutes.
FDBKB-NFR-2.4	Maintenance window	Planned maintenance shall be <44 minutes/month and performed between 22:00–02:00.
FDBKB-NFR-2.5	Local degradation	Feedback submission shall remain available if analytics fails; write failure shall trigger read-only mode; dependency failures shall not block local submission.
FDBKB-NFR-2.6	Client-side retry	Interrupted submissions shall be cached and retried after reconnection without creating duplicates; full offline mode is not required.
FDBKB-NFR-2.7	Backup and restore	Daily automated backups, 6-hourly incrementals and weekly full backups; retain 7 daily, 4 weekly

		and 12 monthly backups across ≥2 in-country locations; restore tested monthly.
FDBKB-NFR-2.8	DR drills	Each Node shall conduct 2 disaster-recovery drills per year.
FDBKB-NFR-2.9	Alert thresholds	Node downtime shall trigger an immediate alert; API error rate >5% shall alert within 5 min; latency degradation >20% shall alert within 15 min.
3. Security and Privacy		
FDBKB-NFR-3.1	Federated access control	Cross-Node queries shall use short-lived, purpose-scoped tokens with separate authorisation; Nodes may reject or rate-limit abnormal queries.
FDBKB-NFR-3.2	Encryption and key management	External connections shall use TLS 1.3; sensitive feedback shall use field-level encryption; each agency shall manage its own keys.
FDBKB-NFR-3.3	Security patching	Critical vulnerabilities shall be fixed within ≤72 hours and high-severity vulnerabilities within ≤7 days.
FDBKB-NFR-3.4	Rate limiting	Each Node shall support rate-limit tiers of 100, 1,000, and 10,000 requests/minute.
FDBKB-NFR-3.5	Attachment security	Only JPG, PNG and PDF files, each <2 MB, with a maximum of 5 files per submission; access restricted to authorised reviewers.
FDBKB-NFR-3.6	Agency data separation	Staff shall only be able to access their own agency's feedback.
FDBKB-NFR-3.7	Location privacy	Location shall be captured only at dzongkhag level; precise coordinates shall not be collected.
FDBKB-NFR-3.8	Disclosure control	Averages and demographic statistics below the proposed n≥10 minimum sample shall be suppressed; public statistics shall be anonymised and aggregated.
FDBKB-NFR-3.9	Erasure and aggregation	After erasure, individual data shall be unrecoverable, while permitted aggregated contributions may remain.
FDBKB-NFR-3.10	Data residency and CDN	Only static, non-personal assets may use an external CDN; feedback and PII shall remain within the

		Node/Bhutan.
4. Interoperability and Integration		
FDBKB-NFR-4.1	Submission acknowledgement	An acknowledgement containing the feedback ID and expected timeline shall be provided within ≤10 s after submission.
FDBKB-NFR-4.2	UCS handoff	95% of UCS handoff API calls shall complete within ≤2 s, with zero data loss and no duplicate records.
5. Feedback Intelligence and Analysis		
FDBKB-NFR-5.1	Duplicate and spam detection	Duplicate feedback shall be detected within 24 hours; spam and authenticity flags shall be sent for human verification rather than silently discarded.
FDBKB-NFR-5.2	Critical-sentiment alert	A spike in "Highly Critical" feedback shall trigger an alert to the owning agency within ≤15 min.
6. Usability and Accessibility		
FDBKB-NFR-6.1	Submission effort	Median feedback submission time shall be ≤2 minutes, with autosave every 30 seconds and a consistent experience across all Nodes.
FDBKB-NFR-6.2	Responsive design	The interface shall work correctly across screen widths from 320 px to 3,840 px.
7. Maintainability		
FDBKB-NFR-7.1	Per-Node rollback	Each Node shall support rollback to the previous working version within ≤5 minutes.
FDBKB-NFR-7.2	Code maintainability	Maintainability index shall be >70 and documentation coverage shall be >60%.

2.5 Public Service Registry (PSR)

ID	Requirement	Target
1. Performance		
PSR-NFR-1.1	Search response	95% of searches shall return results within <200 ms, measured from query receipt to results.

PSR-NFR-1.2	Service detail page	95% of service-detail pages shall fully render, including media, within <500 ms.
PSR-NFR-1.3	API response	95% of API requests shall complete within <100 ms.
PSR-NFR-1.4	Database query	95% of database queries shall complete within <50 ms.
PSR-NFR-1.5	Embeddable widget	95% of widget loads shall become interactive within <300 ms.
PSR-NFR-1.6	Auto-scaling	The system shall respond to increased load and scale within <3 min.
2. Availability and Resilience		
PSR-NFR-2.1	Resilience tier	Tier 3 resilience with RTO ≤2 h and RPO ≤15 min.
PSR-NFR-2.2	Critical-data restore	Critical data shall be restored within <1 h, verified through quarterly recovery drills.
3. Usability and Search Quality		
PSR-NFR-3.1	Learnability	New users shall find a target service within <3 min without assistance.
PSR-NFR-3.2	Task success	>90% of users shall successfully complete service discovery, with satisfaction of ≥4.0/5.
PSR-NFR-3.3	Search quality	≥90% of test queries shall return the correct service in the top 5 results, with a zero-result rate <5%.

2.6 Unified Client Support (UCS)

ID	Requirement	Target
1. Performance		
UCS-NFR-1.1	Case creation API response time	Under 500 ms at the 95% up to 1,000 concurrent users

ID	Requirement	Target
UCS-NFR-1.2	Page load	Under 2 s initial load on standard broadband; under 500 ms for in-session navigation
UCS-NFR-1.3	Case status lookup	Under 2 s at 95%, by reference number or CID
UCS-NFR-1.4	Attachment virus scan	Scan completes within 30 s for a 10 MB file; the submission acknowledgement does not wait for the scan
UCS-NFR-1.5	Notification dispatch latency	Handed to NTFB within 60 s of the triggering event
UCS-NFR-1.6	SLA timer accuracy	Alerts and breach events fire within 1 minute of the scheduled time; all servers NTP-synchronised
UCS-NFR-1.7	Report generation	Reports generated within 30 s
2. Capacity and scalability		
UCS-NFR-2.1	Peak concurrent users, all channels	5,000 or more with under 10% throughput reduction
UCS-NFR-2.2	Event throughput capacity	10,000 events per second sustained
UCS-NFR-2.3	Multi-tenant isolation under load	No measurable degradation in one tenant from a traffic spike in another
3. Audit		
UCS-NFR-3.1	Audit event delivery	100%, with local fallback queue and automatic replay; zero loss by design
4. Security and privacy		
UCS-NFR-4.1	Security assurance	OWASP ASVS Level 2 and RGoB ICT security policy; third-party penetration test before go-live and annually; critical vulnerabilities fixed in 7 days, high in 15 (CP-SEC-04)
UCS-NFR-4.2	Privacy	Privacy notice at submission; citizen access to own data; compliance with applicable Bhutanese law

2.7 IT Asset Repository (ITAR)

ID	Requirement	Target
ITAR-NFR-1.1	Keyword search performance	Results within 3 s
ITAR-NFR-1.2	Form and pop-up performance	Reads, saves, and pop-up loads within 2 s at 95%
ITAR-NFR-1.3	Auditability	Every record and configuration change produces a JLB event with user, time, and before/after values
ITAR-NFR-1.4	Configurability	Adding or changing fields, field types, and master data takes effect without code change or redeployment.
ITAR-NFR-1.5	Security	Complies with RGoB national ICT security policy and OWASP Top 10. Annual third-party penetration test.
ITAR-NFR-1.6	Concurrent edit integrity	Optimistic locking so concurrent edits are not silently overwritten
ITAR-NFR-1.7	Encryption	TLS 1.3 in transit, AES-256 at rest; column-level encryption for fields marked sensitive
ITAR-NFR-1.8	Browser support and usability	A trained user registers a system within a stated time
ITAR-NFR-1.9	Observability	Prometheus metrics, structured JSON logs, and health endpoints for the national Observability platform
ITAR-NFR-1.10	Portability	All records and configuration exportable in JSON and CSV
ITAR-NFR-1.11	Data migration	Bulk import from the existing inventory, with validation and an error report, before go-live

APPENDICES

Appendix A: Glossary of Abbreviations

Abbreviation	Meaning
ASVS	Application Security Verification Standard
DR	Disaster Recovery
EVTB	Event Bus

FDBKB	Feedback Block
GovCloud	The Government of Bhutan's national cloud hosting environment
IDCB	Identity Conversion Block
ITAR	IT Asset Repository
JLB	Journaling/Logging Block
MDMB	Master Data Management Block
MTTR	Mean Time To Recovery
NFR	Non-Functional Requirement
NTFB	Notification Block
PSR	Public Service Registry
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SBOM/CBOM	Software / Cryptographic Bill of Materials
SSO	Single Sign-On
UCS	Unified Client Support
WCAG	Web Content Accessibility Guidelines