Annexure 3: Reporting Requirements and Performance Management

1. Reporting and Monitoring

The Vendor shall establish a structured reporting and monitoring mechanism to ensure transparent, timely, and verifiable tracking of project progress, deliverable status, quality, risks, and issues throughout the engagement. Reporting obligations apply separately to each Lot. Where a Vendor holds more than one Lot, it may combine reports only with the written agreement of the PA Project Manager, provided each Lot is reported separately within the combined report.

1.1 What Shall Be Reported

The Vendor shall submit reports covering, at minimum, the following:

- **Progress and Milestone Status:** Activities completed during the reporting period, work-in-progress, upcoming activities, and status of each deliverable/gate against the Deliverable–Gate–Timeline–Payment Matrix (ToR Section 5.2) and the approved Milestone Plan.
- **BRD Requirement Implementation Status:** Status of each BRD requirement assigned to the Lot, traced in the Requirements Traceability Matrix (RTM), including requirements completed, in progress, deferred, or changed by an approved Change Request.
- **Deliverable and Acceptance Status:** Status of each deliverable against the acceptance criteria defined in ToR Sections 5.3 and 5.4, including pending sign-offs, conditional acceptance items and their completion dates.
- **Cross-Lot Dependency and Interface Status:** Status of the Vendor's entries in the Cross-Lot Dependency Register (ToR Section 3.5), including Interface Specifications published, approved or changed, mock services in use, dependencies on other Lots, GA systems and national platforms, and any delay notified under ToR Section 3.5.
- **Risks and Issues:** A maintained Risk and Issue Register capturing identified risks/issues, likelihood, severity/impact, mitigation or corrective action, responsible owner, target resolution date, and current status (open/in progress/closed).
- **Schedule Deviations:** Any delays or deviations from the agreed timeline, root cause, impact on downstream deliverables and on other Lots, and the proposed recovery plan.

- **Quality and Testing Status:** Status of unit, integration, system, performance, accessibility (WCAG 2.1 AA), and User Acceptance Testing (UAT), including defect counts by severity (Section 1.7), defect ageing, and resolution status.
- **Security and Code Quality Findings:** Findings from the independent VAPT, SAST, DAST, Software Composition Analysis (SCA), container scanning, and code quality tools, together with remediation status and the currency of the SBOM and CBOM.
- **Source Code and Configuration Status:** Repository activity, branching/release status, and version control compliance in the PA Git repository (ToR Section 4.1), including CI/CD pipeline status.
- **Resourcing Status:** Deployment status of Key Professional Staff (ToR Section 4.3), including the Thimphu presence of the Project Manager and Technical Lead, and any proposed substitutions and their justification.
- **Change Request Status:** Status of each Change Request and the cumulative value of approved Change Requests as a percentage of the Contract Price (ToR Section 13).
- **Financial/Invoicing Status:** Status of invoices raised against completed and accepted deliverables, hosting charges where applicable, and any liquidated damages, tied to the payment terms in ToR Section 12.

1.2 Reporting Types and Frequency

1.2.1 Reporting Overview

The table below summarises the seven report types required under this Contract. Minimum content for each report type is set out in Section 1.2.3.

Report Type	Frequency	Format	Prepared By	Submitted To	Submission Deadline

R1 Weekly Status Update	Weekly, for the Lot Project Working Group; fortnightly cross-Lot input for the cross-Lot Project Working Group (ToR Section 7.3)	Status template (R1) or call minutes	Vendor Project Manager / Technical Lead	PA Project Manager / PA GovStack Technical Lead	At least 1 working day before each Project Working Group meeting; minutes within 1 working day after it
R2 Monthly Progress Report	Monthly	Structured report (R2) + updated schedule	Vendor Project Manager	PA Project Manager	Within 5 working days after month-end
R3 Deliverable Completion Report (Gate Report)	At each gate (ToR Section 5.2)	Gate report (R3) + evidence annexes	Vendor Project Manager & Technical Lead	PA GovStack Technical Lead and PA Project Manager (and the PSC for the Integration with Ready Services and the Source Code, Documentation, Training and Knowledge	5 working days before gate event; final report with the invoice (ToR Section 12.3) within 2 working days after sign-off

				Transfer deliverables)	
R4 Risk and Issue Register	Continuous; reviewed at each status meeting	Live register (R4)	Vendor Project Manager (technical items verified by Technical Lead)	PA Project Manager	Updated at least 1 working day before each status meeting
R5 Security and Quality Findings Report	Per scheduled scan cycle, at least monthly, and after each independent VAPT; Critical/High findings within 24 hours of discovery	Findings report (R5) + tool output	Vendor DevOps / Security Engineer / Technical Lead	PA GovStack Technical Lead and PA security officer / Cyber Security Division	Within 2 working days of each scan cycle; Critical/High within 24 hours

R6 Steering Committee Report	Monthly, and at each milestone (ToR Section 7.3)	Executive brief (R6)	PA Project Manager (consolidating Vendor input)	Project Steering Committee	Vendor input at least 5 working days, and the consolidated report at least 3 working days, before the scheduled PSC meeting
R7 Hypercare and Warranty SLA Report	Weekly during Hypercare; monthly from Go-Live until the end of the Warranty Period	SLA report (R7), in the format set out in Annexure 8	Vendor Project Manager	PA Project Manager and PA GovStack Technical Lead	Within 3 working days after each week (Hypercare) or month-end (Warranty)

1.2.2 General Reporting Provisions

- All reports shall be prepared and submitted in English.
- Every report shall be version-controlled (version number, date, author) and submitted through the agreed project collaboration platform, with source files (Word/Excel/PowerPoint) retained alongside the PDF version.
- Reports shall be reviewed by the PA GovStack Technical Lead and PA Project Manager. Technical issues are verified by the PA's technical team; risks, delays, and major decisions are managed by the PA Project Manager (ToR Section 7.1).
- The Vendor shall implement corrective actions per review feedback; further activities proceed only upon PA Project Manager approval (ToR Section 7.1).

A single late or incomplete report shall be addressed by written reminder in the first instance. A second late or incomplete submission within any rolling three-month period, or any pattern of non-conforming reports, shall constitute failure to meet a material contractual requirement and may result in a Notice to Correct under ToR Section 7.2.2 and Section 3.1 of this Annexure.

Report content that reveals non-compliance with KPIs, SLAs, or GovStack conformance requirements shall be addressed through the Notice to Correct and Corrective Action Plan process (Section 3), and repeated failure may support Termination for Default (ToR Section 7.2.3 and Section 4.1).

1.2.3 Report Content Requirements

Format, frequency, preparer, recipient, and submission deadline for each report type are as set out in the table at Section 1.2.1. Minimum content requirements for each report type are set out below. Review and sign-off, and treatment of non-compliance, follow the general provisions at Section 1.2.2 and are not repeated per report type.

Report Type	Minimum Content Requirements
R1 Weekly Status Update	Activities completed and planned; % completion against work plan; blockers/dependencies/decisions required from the PA; cross-Lot dependency status; key personnel and resource status; milestones due in the next four weeks.
R2 Monthly Progress Report	Executive summary (RAG rating); progress against each active deliverable (D1 to the final deliverable of the Lot); BRD requirement status from the RTM; schedule variance analysis; payment milestone status; Risk and Issue Register summary and trend; Cross-Lot Dependency Register status; security and quality findings summary; KPI results and Project Success Rate (Section 2); staffing/resource utilisation; change request status and cumulative value; plan for next period.

R3 Deliverable Completion Report (Gate Report)	Deliverable reference and description; applicable acceptance criteria/trigger (ToR Sections 5.2 to 5.4); evidence of completion (test results, UAT sign-off, demo minutes, VAPT report, WCAG 2.1 AA report and DPIA where required, SBOM and CBOM); BRD/specification compliance checklist traced in the RTM; outstanding defects with remediation plan; recommendation (accept / conditional accept / reject).
R4 Risk and Issue Register	Risk/issue ID, description, category; likelihood and impact rating and resulting score (Section 1.6); owner, mitigation/contingency plan, target closure date; status (open/in progress/closed/escalated); change log since previous version.
R5 Security and Quality Findings Report	Scan/test type performed; findings by severity with CVSS or equivalent rating; Building Block/component affected; remediation status and target closure date; retest/verification results; compliance status against the security and quality KPIs in Section 2.1.
R6 Steering Committee Report	Overall project health by Building Block (RAG); milestone and payment status; key decisions required from the PSC; top risks/issues requiring PSC intervention (including items escalated under ToR Section 7.3); budget and contract status; Vendor performance summary against KPIs/SLAs and the Project Success Rate.
R7 Hypercare and Warranty SLA Report	Incidents and service requests by severity; response and resolution times against the SLAs in Annexure 8; availability achieved against Annexure 2; open incidents and root-cause analyses; security patches applied; SLA breaches and service credits, if any.

1.2.4 Report Template Index

Standard templates (R1–R7) shall be issued by the PA at Inception and maintained in the project repository referenced below. The Vendor shall use the current version of each template unless a variation is agreed in writing with the PA Project Manager.

Report Type	Template Code	Delivered As	Repository / Annexure Reference
Weekly Status Update	R1	Word / PDF, 1–2 pages	Project collaboration platform, folder: /Reports/Status
Monthly Progress Report	R2	Word / PDF + MS Project/Gantt	Project collaboration platform, folder: /Reports/Monthly
Deliverable Completion Report (Gate Report)	R3	Word / PDF + UAT sign-off, test logs, demo minutes	Project collaboration platform, folder: /Deliverables/[D#]
Risk and Issue Register	R4	Excel / shared tracker	Project collaboration platform, folder: /Reports/RIR
Security and Quality Findings Report	R5	Word / PDF + raw scan/tool output	Project collaboration platform, folder: /Reports/Security
Steering Committee Report	R6	Slide deck or 5-page brief	Project collaboration platform, folder: /Reports/PSC
Hypercare and Warranty SLA Report	R7	Word / PDF + ticket system extract	Project collaboration platform, folder: /Reports/SLA; format per Annexure 8

1.3 Reporting and Submission Channels

- Formal reports shall be submitted through the agreed project management/collaboration tool (e.g., Jira, Azure DevOps, or equivalent) designated for the engagement.
- Status meetings shall be held weekly for each Lot and fortnightly for cross-Lot matters (ToR Section 7.3), with minutes circulated to all parties.
- Formal deliverable submissions and sign-offs shall be made in writing (email or the designated document management system) to the PA Project Manager.

- Source code and related technical artefacts shall be committed to and maintained in the PA Git repository from the first day of development (ToR Section 4.1). No parallel private repository shall be used for deliverable code.
- Escalations outside routine reporting shall be raised immediately to the PA GovStack Technical Lead and PA Project Manager through the agreed escalation channel, rather than held for the next scheduled report. Security incidents shall be reported to the PA within 24 hours of discovery (ToR Section 10).

1.4 Monitoring Tools and Mechanisms

- A shared project management/tracking tool for milestones, deliverables, and task-level progress, accessible to both the Vendor and PA officials.
- Automated code quality and security scanning tools (e.g., SonarQube, SAST/DAST and SCA tools, container scanners) integrated into the CI/CD pipeline, with read access for the PA.
- A live/shared Risk and Issue Register accessible to relevant stakeholders.
- Integration with the national Observability platform for Production and Staging monitoring (ToR Section 4.1 and Annexure 2).
- Dashboards or periodic extracts summarising deliverable status, defect status, and SLA compliance (ToR Section 7.2.1 and Section 2 of this Annexure).

1.5 Review, Escalation, and Resolution of Risks/Issues

- All reports shall be reviewed by the PA GovStack Technical Lead (for technical matters) and the PA Project Manager (for schedule, risk, and contractual matters).
- Risks and issues shall be classified by severity (Critical/High/Medium/Low) with the response and escalation times in Section 1.6.
- Technical findings (e.g., defects, security vulnerabilities, code quality issues) shall be reviewed and verified by the relevant technical team; project-level risks, delays, and decisions requiring escalation shall be managed by the PA Project Manager.
- Where a risk or issue is not resolved by the Project Working Group within ten (10) working days, or by its target closure date if earlier, it shall be escalated to the Project Steering Committee (ToR Section 7.3).

- The Vendor shall implement corrective actions based on review feedback, and any dependent downstream activities shall proceed only upon written approval from the PA Project Manager.

The PA shall respond to any such approval request within five (5) working days of submission; any delay beyond this period shall not be counted against the Vendor's Deliverable Timeliness KPI (Section 2.1) or treated as a Vendor-caused schedule deviation, provided the Vendor has notified the delay in accordance with ToR Section 3.5.

1.6 Risk and Issue Severity

Severity	Definition	Reporting to PA	Escalation
Critical	Threatens a Go-Live date, a contractual milestone, data protection, security, or another Lot's critical path	Immediately, and in writing the same working day	PSC, if not resolved within 5 working days
High	Likely to delay a deliverable or materially affect quality or cost if not addressed	Within 2 working days	PSC, if not resolved within 10 working days
Medium	Limited impact that can be managed within the Lot's plan	At the next status meeting	Project Working Group
Low	Minor impact; monitored	In the Risk and Issue Register	None unless severity rises

1.7 Defect Severity Levels (Implementation and UAT)

The following defect severity levels apply to testing and UAT before Go-Live, and to the UAT Bug Resolution KPI in Section 2.1. For incidents in Production, including during Hypercare and the Warranty Period, the classification and response and resolution times in Annexure 8 apply.

Severity	Definition	Maximum resolution time

Critical	Core function unavailable, data loss or corruption, security vulnerability rated Critical, or no workaround; blocks testing or UAT	24 hours
High	Major function impaired with no acceptable workaround, or security vulnerability rated High	3 working days
Medium	Function impaired with an acceptable workaround	10 working days
Low	Cosmetic or minor issue with no functional impact	Next scheduled release

1.8 Independent Quality Assurance Review

The PA may appoint an independent quality assurance party, through internal staff or external resources, to review the Vendor's reports and deliverables (ToR Section 7.1). The Vendor shall give that party access to the PA repository, environments, reports and evidence, attend its review sessions, and respond to its written findings within five (5) working days. The appointment of such a party shall not affect the Vendor's reporting obligations under Section 1, nor extend any Vendor delivery timeline.

2. Key Performance Indicators and Project Success Rate

Performance of the Vendor shall be measured against a defined set of Key Performance Indicators (KPIs) tied to deliverables, quality, and responsiveness. Sustained or critical underperformance against these KPIs shall trigger a formal performance review and, where unresolved, may lead to termination of the engagement. Aggregate KPI performance, measured milestone by milestone, shall constitute the Vendor's Project Success Rate under ToR Section 7.2.1.

2.1 Performance KPIs

The following KPIs apply to each Lot, irrespective of the solution architecture proposed by the Vendor.

KPI Category	Metric	Target	Measurement
Deliverable Timeliness	% of deliverables accepted on or before the agreed gate date in the Milestone Plan (ToR Section 5.2)	≥ 90% on-time acceptance	Cumulative, at each gate; delays notified under ToR Section 3.5 and PA review time excluded
Deliverable Quality	% of deliverables accepted without requiring rework/resubmission	≥ 85% first-pass acceptance (accepted or conditionally accepted at first submission)	Cumulative, at each gate
UAT Bug Resolution SLA (tiered by severity)	Time to resolve defects identified in UAT, by severity (Section 1.7)	≥ 95% of defects resolved within the times in Section 1.7	Per release, from the defect tracker
Code Quality	Unit test coverage / static analysis compliance (ToR Section 5.3)	≥ 80% unit test coverage and all quality gates passed	Per release, from the CI/CD pipeline
Security Findings Closure	Time to remediate Critical/High vulnerabilities identified by VAPT/SAST/DAST/SCA scans	Critical within 7 days, High within 15 days; none open at release acceptance	Monthly, from R5

Service Availability (from Go-Live, including Hypercare and the Warranty Period, per ToR Section 14)	System uptime	As specified in Annexure 2, and not less than 99.5% per month, excluding approved maintenance windows	Monthly, from the Observability platform (R7)
Reporting Compliance	Timely submission of required reports (ToR Section 7.1 and Section 1)	100% on-time submission	Monthly
Interface Compliance	Changes to approved Interface Specifications made without TRB approval (ToR Section 3.5)	Zero	Per release

Note: The PA may adjust a target during Inception, for a specific Building Block, where the BRD or Annexure 2 sets a stricter requirement. The adjusted target shall be recorded in the approved Milestone Plan.

2.2 Project Success Rate

The Project Success Rate is the percentage of KPI measurements in Section 2.1 that met their target during the period assessed:

Project Success Rate (%) = (Number of KPI measurements meeting target ÷ Total number of KPI measurements) × 100

The **Project Success Rate** shall be calculated at each deliverable gate, cumulatively for the implementation period, and for the Warranty Period, and reported in R2 and R6. It shall be applied as follows:

Project Success Rate	Rating	Consequence
85% or above	Satisfactory	Normal monitoring. For the Warranty Period, eligible for an AMC (ToR Section 14.2).
70% to below 85%	Needs improvement	The PA may issue a Notice to Correct (Section 3.1).
Below 70%	Unsatisfactory	Formal Performance Review (Section 3.2). For the Warranty Period, not eligible for an AMC.

3. Notice to Correct, Formal Performance Review and Corrective Action Plan

3.1 Notice to Correct

Where the Vendor fails to meet a material contractual requirement, KPI, SLA, milestone, acceptance criterion, or GovStack conformance requirement, the PA may issue a Notice to Correct specifying the deficiency and required corrective action (ToR Section 7.2.2). A Notice to Correct may also be issued for unapproved replacement of a Key Expert (ToR Section 4.3) and for failure to close a conditional acceptance item by its date (ToR Section 5.3).

The Vendor shall remedy the deficiency within the cure period stated in the Notice to Correct. Unless the Notice states otherwise, the cure period is fifteen (15) working days, or the resolution time in Section 1.7 or Annexure 8 where the deficiency is a Critical or High defect or incident.

3.2 Formal Performance Review

A formal performance review shall be triggered where any of the following occur:

- **Uncured Notice to Correct:** The deficiency in a Notice to Correct is not remedied within the cure period.
- **Consecutive Missed Deliverables:** Failure to achieve acceptance for two (2) or more consecutive deliverables/gates within their agreed timelines, without an approved schedule extension.
- **Unresolved Critical Findings:** Any Critical-severity defect, security vulnerability, or quality finding remaining unresolved beyond its defined SLA (Section 1.7, Section 2.1 or Annexure 8).
- **Repeated SLA Breaches:** Breach of the same KPI or SLA on three (3) or more occasions within a rolling three (3)-month period.
- **Low Project Success Rate:** A Project Success Rate below 70% (Section 2.2).
- **Material Non-Compliance:** Failure to submit required reports (Section 1), maintain source code in the PA Git repository, or comply with agreed governance and review processes.
- **Key Personnel Issues:** Unauthorised or repeated replacement of Key Professional Staff (ToR Section 4.3) without prior approval, materially affecting delivery.

3.3 Corrective Action Plan (CAP) Procedure

1. The PA Project Manager shall issue a written Notice of Formal Performance Review, specifying the KPI(s) or requirements breached and supporting evidence.
2. The Vendor shall submit a Corrective Action Plan (CAP) within ten (10) working days, detailing root cause, remedial actions, responsible persons, measurable targets and a revised timeline.
3. The PA shall approve the CAP, or return it with comments, within five (5) working days. The Vendor shall resubmit a returned CAP within five (5) working days.
4. The PA Project Manager/Technical Lead shall monitor performance against the approved CAP over a cure period of thirty (30) days from CAP approval, unless the PA sets a different period in writing.
5. If performance is restored to acceptable levels, the review is closed and normal monitoring resumes. If not, the matter is escalated under ToR Section 7.2.3 and Section 4.1.

If the Vendor fails to submit an acceptable CAP, or fails to meet the CAP's agreed remedial timeline, this shall constitute expiry of the cure period for the purposes of ToR Section 7.2.3 (failure to remedy a Notice to Correct within the cure period). The Vendor shall not be entitled to a separate or additional cure period before termination proceedings under ToR Section 7.2.3 commence.

A Vendor that disputes a performance review finding, KPI breach determination, or a decision to terminate may raise such dispute in accordance with the Dispute Resolution provisions of the Contract (ToR Section 7.3). Raising a dispute shall not, by itself, suspend the cure period or the PA's right to proceed under ToR Section 7.2.3, unless otherwise directed by the dispute resolution body or agreed in writing by the PA.

4. Termination

4.1 Termination for Default

The PA may terminate the Contract, in whole or in part, for default in accordance with the Contract and PRR 2025 where the Vendor:

- fails to remedy a Notice to Correct or material breach within the prescribed cure period;
- repeatedly fails to meet agreed KPIs, SLAs, deliverables, acceptance criteria, or GovStack requirements;
- fails to satisfactorily implement an approved Corrective Action Plan;
- materially fails to meet security, quality, interoperability, performance, or data integrity requirements;
- engages in fraud, corruption, or other prohibited practices;
- becomes insolvent or otherwise unable to perform its contractual obligations; or
- fails to comply with material source-code, documentation, intellectual property, or handover obligations.

Procedure. The PA shall issue a written notice of intention to terminate, stating the grounds. The Vendor may respond in writing within ten (10) working days. If the PA is not satisfied with the response, it may issue a notice of termination stating the effective date. Termination shall be subject to the applicable notice and cure requirements, except where the nature of the breach

warrants immediate termination under the Contract or applicable law. On termination for default, the PA may forfeit the Performance Security (ToR Section 12.4) and apply liquidated damages already accrued (ToR Section 12.5), in accordance with the Contract and PRR 2025.

4.2 Termination for Convenience

The PA may terminate the Contract, in whole or in part, for convenience by providing sixty (60) days' written notice to the Vendor.

In such cases, the PA shall pay for accepted work and deliverables completed up to the effective date of termination, and for work in progress that is delivered to the PA, valued in accordance with the Contract. The Vendor shall have no entitlement to payment for unperformed work except as expressly provided in the Contract.

5. Exit and Handover

On expiry or termination for any reason, the Vendor shall comply with the exit and transition requirements in Annexure 8 (ToR Section 7.2.4) and shall promptly hand over all relevant GovStack Building Block artefacts, including:

- source code and repositories;
- build, deployment, CI/CD, and infrastructure-as-code scripts;
- technical, functional, architecture, API, security, and operational documentation, including the SBOM and CBOM;
- GovStack conformance and testing evidence;
- databases, migration scripts, data-mapping documents, and related data artefacts;
- administrator accounts, credentials, certificates and keys, transferred to the PA, with all Vendor access revoked;
- escrow details for any COTS component whose source code cannot be transferred (ToR Section 12.7); and
- configurations and other materials required for continued operation, maintenance, or migration.

The Vendor shall provide reasonable knowledge-transfer and transition support to the PA or its nominated successor for up to sixty (60) days (ToR Section 7.2.4). The Vendor shall return all PA

data, securely destroy any copies it holds, and provide a certificate of destruction (ToR Section 10.1). All deliverables and artefacts developed specifically under the Contract shall be made available to and owned by the Royal Government of Bhutan in accordance with ToR Section 12.7, irrespective of the underlying architecture or technology stack used. The PA shall retain applicable audit rights over Contract-related records for five (5) years following expiry or termination.