TERMS OF REFERENCE

FOR

QUALITY ASSURANCE PROVIDER

INTEGRATED FINANCIAL MANAGEMENT INFORMATION SYSTEM (IFMIS)

'Testing Agency', 'Quality Assurance Provider' and 'QA Agency' will be used interchangeably. (ToR V.1)

1. Background

The Ministry of Finance, Royal Government of Bhutan has been implementing various reforms for strengthening and modernization of Public Financial Management (PFM) in the country. The modernization (or automation) journey for the PFM commenced two decades ago and most functions in PFM have been automated to varying degrees. Following systems are currently in use for PFM catering to specific needs of PFM functions and the stakeholders:

Multi-Year Rolling Budget (MYRB) - MRYB supports in preparation and finalization of the annual budget including its revisions (supplementary budgets, reappropriations etc.)

Electronic Public Expenditure Management System (e-PEMS) - e-PEMS supports budget execution, particularly for managing the public expenditure. The system supports the creation and the disbursement vouchers and releasing payments for all categories of expenditure including accounting and reporting for public expenditure. e-PEMS also has a payroll module for generation of payroll for all the government employees. The system is interfaced with the IT systems of the Bank of Bhutan to support e-payments to the payees. With the introduction of e-payments, a significant portion of public expenditure now is paid through electronic fund transfer to the bank accounts of payees.

FinDocs - the supporting documents for disbursement vouchers are captured in FinDocs in electronic format. Soft copies of the documents are tagged to the voucher number generated from e-PEMS. This system is used by the Cluster Finance Services, where the finance personnel are stationed in an office located away from the agency.

Electronic Daily Allowance & Travel System (e-DATS) - e-DATS Supports in processing the travel authorizations for the official travels of the staff in the government and is interfaced with the e-PEMS for payments for advances and for settling the expenditure incurred during such travels.

Meridian/ Commonwealth Secretariat Debt Recording Management System (CS-DRMS) - Is in use for managing the public debt, particularly for the external debt. The system supports recording the details of debt instruments, accounting for funds received and repayments for the external debt including generation of reports for debt monitoring and reporting.

The government implemented several other IT systems for automation of other related functions for PFM. Some of these systems have electronic data exchange mechanisms in place with the core IT systems in PFM as referred to above.

IT systems at Department of Revenue and Customs (DRC) - DRC has implemented several key systems for modernization of tax and customs administration and related revenue collection. Key systems at DRC include (a) Revenue Administration Management Information System (RAMIS)/Bhutan Integrated Taxation System (BITS) for collection of major taxes such as income tax, sales tax etc., (b) Property Tax System for administration and collection of property tax, (c) Electronic Customs Management System (e-CMS) for administration and collection of customs duties and taxes and (d) Bhutan Integrated Revenue Management System (BIRMS) for collection of non-tax revenues. These systems are interfaced with the banking systems to support online payments for tax and non-tax revenues.

E-Government Procurement (e-GP): the e-GP system is supporting various public procurement functions including creation of annual procurement plans, creation of tender documents through electronic bidding document creation facility in the system, publishing

bidding documents, receiving tenders/proposals, evaluation and award of contracts. e-GP is also interfaced with MYRB and e-PEMS.

Government Inventory Management System (GIMS) - Supports recording details of assets procure/constructed through public expenditure and tracking their allocation. GIMS is also interfaced with the e-GP system currently.

Zest System - The Royal Civil Service Commission has introduced the Zest system, which supports Human Resource Management for Government employees, for both permanent and contractual staff. The system supports recording details of staff, their qualifications, designation, pay grade and structure, details of training and certifications, processing payments for certain specific benefits extended to the employees etc.

Construction Manager Software(CMS) - System has been developed by the Ministry of Infrastructure and Transport and supports in managing the works contracts awarded by the Ministry. The system has key features such as preparation of estimates for the work contracts, capturing details of contracts and the contractors, monitoring the progress of the contracts, receiving and approval of the bills from contractors and interfacing with e-PEMS for sharing details of approved invoices. e-CMS development has been concluded recently, and the system is currently undergoing internal testing within the Ministry.

Through these modernization efforts over the years, the Government made some key achievements in improving PFM processes, systems and institutional capacities. Some of these achievements are as follows:

a. Critical functions in PFM are automated, which is supported in improving efficiency in managing the public expenditure and revenue collections. IT systems are already in place for budgeting, submission of monthly cash flow requirements and applying monthly cash ceilings, processing public expenditure, revenue collections, payroll, public procurement, inventory/asset management, debt management, contract management, accounting and reporting etc.

b. A significant portion of public expenditure is currently processed and paid through electronic payment channels with minimal dependency on cash payments, such as petty cash expenses and for expenditure needs in remote locations with minimal access to ICT infrastructure for day-to-day expenditure needs. Cheque based payments have been largely eliminated.

c. Approved payments are processed, and payment is released in real time with payment instructions sent to the bank every two minutes improving the speed in release of payments.

d. Most of the revenue administration functions, including revenue collections, are automated in the current environment.

e. Adopted Treasury Single Account (TSA) for revenue collections and public expenditure with a significant portion of public revenues pooled into treasury single account maintained at Royal Monetary Authority (RMA) through intermediary accounts maintained in Bank of Bhutan.

f. Established IT infrastructure and created good IT literacy in the finance cluster/section staff across the country, which created a positive culture for adoption of new systems or changes in existing IT systems.

The existing ICT systems for PFM are hosted in the Government Data Center being managed by the GovTech, an autonomous agency established by the Royal Government for providing

ICT systems and infrastructure planning, coordination, implementation and maintenance support for the whole of the Government in the country.

2. Challenges in the current ICT Systems in PFM

While several ICT systems have been introduced and most of the PFM functions have been modernized by the Government, certain critical gaps exist in the current environment leading to initiation of steps for introduction of a new Integrated Financial Management Information System (IFMIS) for the Government. The following summarizes the key gaps/challenges in the current environment:

a. Existing IT systems, such as MYRB, e-PEMS etc., were developed in 2010 in Microsoft .Net platform and system enhancements were undertaken over the years to add new features to cater to the emerging needs of the Government for PFM. The architecture and development approach for the systems has become redundant and adequate documentation has not been created to support continuity in systems development and maintenance.

b. While most of the PFM functions are currently automated, substantial scope exists for process improvement and minimizing the administrative burden in managing the PFM functions. Implementing such changes in the current environment would require substantial enhancements to the existing systems.

c. Most of the PFM functions are carried out at the implementing agency level and the current systems design and ICT enabled procedures do not include the implementing agencies as a stakeholder/user in the business processes. This is leading to implementing agencies relying on manual procedures and documentation for PFM. Such manually processed and approved records are shared with the finance section/finance cluster staff for recording the transactions in IT systems and their further processing for release of payments to the payees. Such an environment results in dependence on manual procedures and IT-enabled systems in parallel.

d. The integration of IT systems and automated data exchange among existing ICT systems needs substantial improvement. Data exchange with the banking systems for e-Payments is an exception, and most of the remaining data exchange among the systems requires manual interventions.

e. The ownership for maintenance and enhancements has been recently transferred from MoF to the GovTech, an autonomous agency created by the Royal Government for ICT systems development and maintenance across the Government. Lack of adequate documentation and inadequate knowledge transfer to GovTech is posing constraints in implementation of needed changes to the systems.

For addressing these critical challenges and for further improving the operational efficiencies in managing the public finances, the Government has initiated implementation of a new Integrated Financial Management Information System (IFMIS). The new system is envisaged to replace several of the existing systems in a phased manner during the project lifecycle.

3. Implementation & Procurement Approach for IFMIS

IFMIS is proposed to be implemented in two phases and the table below summarizes the specific functions/modules proposed to be covered in each phase:

3.1 Phasing Plan for implementation of PFM Functions in IFMIS

IFMIS system development for all the modules shall be performed in parallel and shall be completed as per the planned timelines. While system development for all the modules is expected to be done in parallel, system adoption by the national government agencies is planned in a phased manner.

Table 1: Proposed modules for IFMIS Phase 1 Launch

Scope of IFMIS	System Interfaces
a. Budget Management b. Commitments Management c. Cash Management (Part 1) d. Expenditure Management e. Payroll Management f. Accounting and Fiscal Reporting	a. ZEST (RCSC) b. Commercial Banks CBS IT System c. RMA IT System d. E-Government Procurement System (e-GP) e. Construction Manager Software (CMS) f. Government Inventory Management System (GIMS) g. Meridian (Debt Management System) h. Strategic Planning and Monitoring Evaluation (SPME)

Table 1: Proposed modules for IFMIS Phase 2 Launch

Scope of IFMIS	System Interfaces for IFMIS
a. Budget Preparation b. Cash Management (Part 2) c. Revenue Accounting d. Accounting and Fiscal Reporting (Part 2)	a. BITS (DRC) b. Audit Information Management System (AIMS) at RAA

3.2 Phasing of system implementation for Government Agencies

Rollout of new IFMIS for all the government agencies, despite extensive testing and quality assurance procedures, could pose severe challenges in case of any unforeseen developments during its implementation and rollout. It is also critical to pilot the system functionality to verify the adequacy, comprehensiveness and the completeness of the system prior to its rollout across the Government. Upon completion of the system stabilisation period successfully and addressing the gaps identified during this stage, the system shall be rolled out to all the users across the Government. Following summarises the proposed approach for rollout of IFMIS for the stakeholders:

a. System testing and certification by the designated user group from the IFMIS including technical testing and certification by GovTech or agency designated for this purpose.

b. Extend system access to the existing e-PEMS users for trial run/test transactions for 4-6 weeks along with system support for digitizing the data needed for IFMIS that is currently not available in e-PEMS, MYRB or other IT systems

c. Resolution of issues in trial run, data migration and production go-live of phase 1 functionality for all existing e-PEMS users at the same time.

d. Production system stabilization for 3-4 months, resolution of any issues in production go-live and system stabilization

e. Launch system access to other users in the Government agencies for capturing all financial transactions in IFMIS at source including system launch for external users (e.g. suppliers)

f. Launch phase 2 modules upon successful launch of phase 1 functionality and in the interim continue the use of MYRB for budget preparation related activities.

3.3 Procurement Approach for IFMIS

IFMIS implementation requires a wide array of goods and services across the project lifecycle including application software and related services, IT infrastructure and related services, quality assurance, capacity building and change management. Following summarizes the procurement approach adopted for the IFMIS:

a. **IFMIS Implementation Partner (IIP):** IIP was selected to provide IFMIS application software design, development, testing, implementation, data migration, training and warranty, maintenance and support services for IFMIS application software. The scope for IIP also includes supply, installation and maintenance of development, test and training instances for IFMIS and excludes the scope for IT infrastructure for production and DR instances.

b. **IFMIS IT Infrastructure Implementation Partner (IIIP):** IIIP contract focusses on supply, installation, commissioning, warranty and maintenance support for the IT infrastructure needed for the production and disaster recovery instance for IFMIS. The scope for IIIP excludes providing the physical space or data center hosting facility for the production and DR instance including network and security infrastructure for both the sites. Such hosting facilities are provided by GovTech through the Government Data Center and DR site.

The acceptance testing services to be provided by the QA Agency shall cover the goods and services delivered by both the IIP and IIIP referred above.

3.4 Deployment Site of IFMIS Application

Both the production and DR instances for IFMIS will be hosted in the data center facilities established and being maintained by the GovTech Agency (GovTech) of RGoB. Following provides information related to the DC and DR sites being managed by the GovTech and other related standards to be complied by the IIIP for deployment of IFMIS IT Infrastructure in these sites:

a. The RGoB uses the facilities of the National Primary and Recovery Data Centers that are administered by the GovTech Agency (GovTech). The IFMIS software solution shall be deployed and use the IT infrastructure platform within the Data Centers.

b. The GovTech will provide the following for the proposed IFMIS solution:
    a. Central Server Room for all IFMIS applications and data storage requirements.
    b. Core Network for the WAN connectivity to external networks (i.e. Government Network)
    c. Storage Area Network (SAN)
    d. Tape backup facility
    e. Firewall protection with internal, external, and DMZ zones and dedicated separate network/server equipment.
c. The Government has remote branch offices connected via the Government Network. Where the system is expected to connect to the internet, a De-Militarized Zone should be specified with a separate server, firewalls, and other intrusion detection systems provided by the GovTech to ensure that no unauthorized access to the system is possible.
d. The GovTech infrastructure supports servers with x86 architecture Linux (Ubuntu 24.04), virtualized servers, network administration, anti-virus software distribution, PostgreSQL relational database software, and the current ePEMS and MYRB applications used by the RGoB for PFM.
e. GovTech's Cloud Services Division (CSD) has the mandate to provide Platform as a Service (PaaS) to host the government system/applications. At present they provide Ubuntu 24.04 LTS. However, for those wishing to use the enterprise OS, the clients are required to bear the cost for license. New systems are provided with a staging environment. After meeting the BtCIRT's vulnerability assessment compliance, systems will be moved to the production environment and for servers that require global access a global IP is provided. The DNS entries for "systems.gov.bt" domains at GDC nameservers are available.
f. The infrastructure above is designed to be reliable with minimal downtime. Those servers with Storage or Hard Disks are structured with RAID 10. The SAN is structured with redundant arrays of storage and the ability to 'hot swap' the drives if one fails. The communication system has two means for connecting to the national network and can switch over automatically. The tape drive backs up the entire system, enabling the system to step back and then rebuild if necessary.
g. IFMIS is intended to be supported in a failover mode to the BDC (Backup Data Center) located in Bumthang. The QA Agency shall verify compliance with all ***Basic Minimum GovTech Standards***.

4. Scope of Work for Quality Assurance for IFMIS

The IFMIS project shall be subject to independent quality assurance, acceptance testing, and certification throughout its lifecycle, covering three phases: (i) the design and development phase, (ii) the implementation and testing phase, and (iii) the warranty and operations and maintenance phase. Payments to IIP at each phase shall be made only upon PMU's acceptance of the relevant QA deliverable as specified in the deliverables table at Section 15.

The QA Agency shall review all aspects of the IFMIS system - including software, hardware, and documentation - covering solution architecture design, system and sub-system design, coding, testing, documentation, version control, change management, security, performance, interoperability, scalability, and availability. The QA Agency shall verify compliance with all technical and functional requirements specified in the bidding documents (including addenda issued), subsequent negotiations, and the detailed requirements specifications signed off

between the Royal Government of Bhutan and IIP. PMU shall establish appropriate processes for notifying IIP of any deviations from defined requirements at the earliest instance to enable timely corrective action.

The QA Agency's involvement does not absolve IIP of its fundamental responsibility for designing, developing, installing, testing, and commissioning all components of the IFMIS system in conformity with the approved requirements. All services and deliverables of IIP shall be subject to QA audit and certification as specified in this TOR, and PMU reserves the right to request additional QA coverage beyond the defined scope where necessary to protect RGoB's interests.

The QA Agency's scope of work covers the following activities:

- Testing and Certification
- ISO Certification
- Warranty and Operations Phase
- Concurrent Activity Management
- Testing round, retesting and three round completion

4.1 Testing and Certification

4.1.1. Functional Requirements review

The IFMIS solution developed and implemented by the implementation partners shall be reviewed and verified by the testing agency (*also known as Quality Assurance Provider)* against the final Requirements signed off between the DTA and implementation partner. Any gaps identified as 'necessary for resolution prior to go-live' (includes SRS verification and proceed tab) by the procuring agency and the testing agency shall be addressed by implementation partners prior to the Go-live of the solution. The acceptance testing with regards to the functional requirements shall be performed by the testing agency as well as the select staff from the Government and the system has to satisfy both the testing agency's acceptance testing and internal user acceptance testing from the Government, upon which the system shall go-live.

For conducting the User Acceptance Testing (UAT), DTA shall identify the employees from respective agencies, who shall be responsible for day-to-day operations of the functions automated through the IFMIS solution. The system, during the functional requirements review, shall necessarily satisfy the user acceptance testing process. The acceptance testing agency and the other designated staff from oversight and spending agencies will also participate in the UAT.

Functional prototype review, including the UI/UX for the prototype, verifying core functionality against defined requirements to ensure intended operations work as expected, identifying usability issues, integration flaws that may impact user experience or system behaviors and provide actionable feedback on test findings to refine prototype before full-scale development or release

Functional testing of the system, including necessary integration testing within the IFMIS modules and external systems, shall be performed as per the signed-off functional requirements specifications, functional design and prototype for IFMIS.

4.1.2. Technical requirements and design review verification

The technical design of IFMIS solutions including the solution architecture, solution design, customization approach, source code for software customizations etc shall be reviewed by the QA Agency to ensure compliance with the technical requirements and standards defined for the project. Any non-compliance/gap identified in the design shall be reported to implementation partners, which shall be addressed and signed off prior to undertaking the next phase of activity in the project implementation.

The number of rounds of review of technical design related documents and related processes shall be the same as defined for the functional design review.

4.1.3. Infrastructure Compliance Review and verification

The QA Agency shall confirm the Government Data Center readiness, network, deployment environment, and availability of services in all defined locations. The QA agency shall perform the infrastructure compliance review to verify the conformity of the infrastructure supplied by implementation partners against the requirements and specifications provided in the bidding documents, as proposed in the proposal submitted by implementation partners and the final version of the specifications included in the contract documents and any subsequent amendments signed off between the Government and the implementation partners. Compliance review shall not absolve implementation partners from ensuring that proposed infrastructure meets the SLA requirements.

Such review shall be completed at three stages:

- upon delivery on site and unpacking of the boxes/items and their initial power on,
- installation and configuration of the infrastructure and,
- a final review to verify if the findings from the prior two reviews have been addressed.

4.1.4. Performance and scalability

The QA Agency shall test and verify the deployed IFMIS solution against the performance parameters defined in the SLA and bidding documents. The review shall cover:

- Request-response and workflow performance: response times for all key transactions and workflow processing times across all automated approval workflows.
- Concurrent user capacity: the number of simultaneous users the system can support without performance degradation.
- Stress and resilience: system behaviour under sustained peak load and at or beyond capacity.
- Backup, restoration, and disaster recovery: data backup and restoration procedures, completion times, and failover to BDC within the RTO and RPO defined in the SLA.
- Scalability: verification that the IFMIS architecture supports the phased expansion of PFM functions across government agencies without requiring fundamental redesign between phases.

A comprehensive load and stress test shall be conducted prior to each phase go-live. The system must meet all SLA performance thresholds under peak load conditions before the QA Agency issues a Go-Live Certificate. The QA Agency shall submit a Performance and Scalability Test Report to PMU as a mandatory deliverable before each go-live milestone.

4.1.5. Security Review

The IFMIS system and its supporting IT infrastructure shall be audited by the QA Agency from a security and controls perspective. The audit shall cover three domains:

- IT infrastructure and system software: servers, operating systems, database management systems, and middleware deployed for IFMIS.
- Application software and related components: all custom-developed modules, third-party integrations, and APIs, including vulnerability assessment, penetration testing, code review, user authentication and access control, user activity logging, audit logging mechanisms, workflow controls, data encryption, and data access privileges, retention periods, and archival mechanisms.
- GovTech shared infrastructure: network, security, and storage infrastructure provided by GovTech for IFMIS, verified through configuration review.

This list is indicative and not exhaustive. PMU reserves the right to require additional security testing as necessary to protect RGoB's interests, provided such testing is within the general scope of security assurance and cost at the RFP stage.

4.1.6. Manageability Review

The QA Agency shall verify the manageability of the IFMIS solution and its supporting infrastructure deployed for the system. Such review shall cover manageability requirements such as monitoring, administration, configuration, inventory management, fault identification etc.Manageability assessment - verifying that the system can be monitored, administered, and maintained effectively by RGoB and GovTech staff following handover.

4.1.7. Availability

IFMIS solutions should be designed to remove all single points of failures. Appropriate redundancy shall be built into all the critical components to provide the ability to recover from failures. The QA Agency shall perform various tests including network, server, security, DC/DR fail-over tests to verify the availability of the services in case of component/location failures. The QA Agency shall also verify the availability of IFMIS services to all the users in the defined locations.

4.1.8. Data quality and migration validation

The QA Agency shall perform the data quality assessment for the entire data migrated to the IFMIS as per the data quality definition prepared by the QA Agency and signed off between the Government and the QA Agency. Testing agencies shall also perform document quality assessment for documents uploaded into IFMIS on a sample basis to verify the quality and completeness of any supporting documents uploaded into the system. The errors/gaps identified during the data quality assessment shall be addressed by implementation partners before moving the data into the production environment, which is a key milestone for Go-live of the solution.

The Testing Agency shall submit reports separately for each of the above testing requirements and for each round of testing. The bidders shall quote separately for each of the above testing focus areas and shall be paid accordingly upon completion of testing for each of the above areas.

4.1.9. User acceptance testing support

The QA Agency shall support PMU in conducting User Acceptance Testing (UAT) by facilitating testing sessions with RGoB stakeholders from the relevant spending and oversight agencies. UAT shall verify that the system satisfies the day-to-day operational needs of the users who will work with IFMIS after go-live. The QA Agency shall document all UAT outcomes, record any functional gaps identified by users, and confirm that all gaps classified as necessary for resolution prior to go-live have been addressed by IIP before the Go-Live Certificate is issued.

Note: UAT shall be conducted under the joint supervision of DTA PFM TU

4.1.10. Project Documentation

The QA Agency shall review the project documents developed by implementation partners including source code documentation, software change management related documents, installation, training and administration manuals, version control etc. Any issues/gaps identified by the QA Agency in any of the above areas, shall be addressed by the implementation partners to the complete satisfaction of DTA.

Annual Documentation Review

The QA Agency shall conduct one annual documentation review commencing from the first anniversary of the Phase 1 Go-Live Certificate and annually thereafter, to verify that IIP's updated system documentation is current, complete, and consistent with the deployed system. For the purposes of this clause:

- Current means all documentation reflects the version currently running in production, with matching version numbers and release dates.
- Complete means all modules in scope are documented, covering at minimum: functional specifications, system architecture, user manuals, administration manuals, and source code documentation.
- Consistent means no material discrepancy exists between documented system behaviour and actual observed system behaviour as identified during the review.

The QA Agency shall submit a Documentation Review Report to PMU within five (5) working days of completing each review. Where gaps are identified, IIP shall resolve all gaps within fifteen (15) working days of receiving the report. Billing shall be at actual effort up to a ceiling of ten (10) person-days per annual review, supported by timesheets.

4.1.11. Knowledge transfer verification

The QA Agency shall verify that IIP has fulfilled its knowledge sharing obligations to RGoB throughout the project lifecycle. This includes confirming that IIP has conducted training for relevant RGoB staff on system operation, administration, and maintenance; transferred source code, technical documentation, and operational know-how to the designated RGoB personnel; and ensured that RGoB has the internal capacity to operate, administer, and maintain IFMIS independently following the end of the warranty period.

4.1.12. Change Management Spot-Check

The QA Agency shall conduct one change management spot-check per quarter, reviewing a sample of change requests processed by IIP during that quarter to verify compliance with the approved change management procedure. PMU shall select the sample, which shall comprise at least five (5) change requests and shall include at least one change request from each

severity category processed during the quarter. Where fewer than five change requests were processed during the quarter, all shall be reviewed. The QA Agency shall submit a Change Management Spot-Check Report to PMU within five (5) working days of completing each review. Billing shall be at actual effort up to a ceiling of three (3) person-days per quarter, supported by timesheets.

4.2 ISO Certification

The QA Agency shall obtain system-level ISO certifications for the IFMIS deployment at the Government Data Center on behalf of the Ministry of Finance, Royal Government of Bhutan. The certificates shall be issued to the Ministry of Finance as the system owner and shall remain the property of RGoB. These certifications are independent of and separate from any ISO certificates held by IIP as an organization.

The following four certifications are required:

#	Standard	Certification	Scope
1	ISO/IEC 27001:2022	Information Security Management	IFMIS deployment at Government Data Centre. ISO/IEC 27017 cloud security controls and ISO/IEC 27701 privacy information management controls shall be assessed as extensions within the same audit. The resulting certificate shall explicitly state that both ISO 27017 and ISO 27701 controls were included in the assessment scope.
2	ISO 9001:2015	Quality Management	IFMIS project delivery and operations processes.
3	ISO/IEC 20000-1:2018	IT Service Management	IFMIS service management and support operations at Government Data Centre.
4	ISO 22301:2019	Business Continuity Management	IFMIS service continuity including disaster recovery at BDC.

QA Agency Obligations

The QA Agency shall manage the end-to-end process of obtaining all four certifications on behalf of the Ministry of Finance, including the following activities:

a) Certification Programme Plan: The QA Agency shall prepare a Certification Programme Plan covering all four certifications and submit it to PMU as part of the Final Inception Report (Section 13, Item 1(b)). The Plan shall set out the timeline for each certification, including certification body engagement, gap assessment schedule, remediation window, Stage 1 and Stage 2 audit dates, first-year surveillance audit schedule, and resource requirements from IIP and PMU. The formal ISO certification process shall not commence until PMU has confirmed the Plan in writing. PMU shall

provide written confirmation within ten (10) working days of receiving the Final Inception Report.

b) Engage a Certification Body: The QA Agency shall engage one internationally accredited ISO certification body, approved by PMU, to conduct all four certification audits. The QA Agency shall propose at least two (2) accredited certification bodies for PMU's selection within thirty (30) calendar days of the Phase 2 Go-Live Certificate. Using a single certification body for all four audits is required to reduce cost and coordination. The certification body's fees for all four audits, including Stage 1, Stage 2, and first-year surveillance audits, shall be included in the QA Agency's bid price. PMU shall confirm at bid stage whether the certification body's fees will be paid through the QA contract or through GovTech's IFMIS project budget so that all bidders can price on a consistent basis.

c) Gap Assessments: The QA Agency shall conduct gap assessments of the IFMIS deployment against all four standards in parallel, commencing within five (5) working days of the Phase 2 Go-Live Certificate. Each assessment shall identify all non-conformances classified as Critical, Major, or Minor. The QA Agency shall submit a consolidated Gap Assessment Report covering all four standards to PMU within forty-five (45) calendar days of the Phase 2 Go-Live Certificate.

d) Remediation Oversight: The QA Agency shall prepare a consolidated Remediation Action Plan identifying which non-conformances IIP is responsible for remediating, and which PMU is responsible for addressing. IIP is responsible for non-conformances in the application software, deployment processes, and service management. PMU - through GovTech - is responsible for non-conformances in the data center infrastructure, network security, and hosting environment. The QA Agency shall verify each remediation item and confirm in writing to PMU before the formal certification audits are scheduled.

e) Manage the Formal Certification Audits: The QA Agency shall coordinate Stage 1 and Stage 2 audits for all four standards with the selected certification body, scheduling them to run in parallel where possible. The QA Agency shall prepare all scope statements, management system documentation, and evidence packages required for each standard. The QA Agency shall serve as the primary point of contact between PMU, IIP, and the certification body throughout the audit process.

f) Obtain the Certificates: The QA Agency shall obtain all four ISO certificates issued to the Ministry of Finance, Royal Government of Bhutan, scoped to the IFMIS deployment at Government Data Center, and deliver them to PMU no later than T[IFMIS]+30.

g) Surveillance Audit Support - First Year: The QA Agency shall support PMU through the first annual surveillance audit for each of the four standards. This support shall be included in the bid price and covers preparation of evidence, documentation review, and attendance at the surveillance audit. Subsequent surveillance audits are PMU's responsibility after the conclusion of the QA contract.

PMU Obligations

I. PMU shall provide the QA Agency with full access to the Government Data Center, all system documentation, infrastructure configuration records, security policies, and relevant staff for gap assessments and formal certification audits within five (5) working days of each request.

II. PMU shall ensure that IIP remediates all Critical and Major non-conformances identified in the Gap Assessment Report within thirty (30) calendar days of receipt.

III. PMU - through GovTech - shall remediate all Critical and Major non-conformances in the data centre infrastructure, network security, and hosting environment within thirty (30) calendar days of receipt of the Gap Assessment Report.

IV. Where the certification timeline is delayed because IIP has failed to remediate or PMU has failed to provide the required access or documentation, PMU shall formally document the delay and extend the QA Agency's T[IFMIS]+30 deadline by the number of days of delay directly attributable to IIP or PMU. No penalty shall apply to the QA Agency for the extended period.

Payment

The QA Agency's QA-PM 10 payment shall be released upon delivery of all four ISO certificates to PMU. Where the certification timeline is delayed for reasons attributable to IIP, PMU, or the certification body's scheduling, the QA-PM 10 payment deadline shall be extended proportionately, and no penalty shall apply to the QA Agency. The QA Agency shall notify PMU immediately upon identifying any risk of delay, providing the reason and a revised expected certificate delivery date.

Certification Deadline

All four ISO certificates shall be delivered to PMU no later than T[IFMIS]+30. This deadline assumes Phase 2 Go-Live at T[IFMIS]+28 and allows two (2) months for gap assessments, remediation, and formal certification audits conducted in parallel.

4.3 Warranty and Operations Phase

Following go-live of Phase 1 and Phase 2, the IFMIS system enters a warranty and operations period during which the Implementation Partner (IIP) is obligated under the IFMIS contract to maintain system performance, resolve defects, and support ongoing operations. During this period the QA Agency shall provide independent oversight to PMU, verifying that IIP is meeting its obligations. The QA Agency shall not manage or operate the IFMIS system; its role is solely to provide independent periodic assurance to PMU.

The QA Agency's activities during this phase are limited to the four activities set out below. Any activity requested by PMU beyond this defined scope shall be agreed in writing before commencement and shall be compensated at the actual man-month rate of the staff performing the work, agreed with PMU before work begins.

(a) Quarterly SLA Compliance Review

The QA Agency shall conduct one quarterly SLA compliance review per phase commencing from the date of the respective Go-Live Certificate - Phase 1 from the date of the PM7 Go-Live Certificate, and Phase 2 from the date of the PM12 Go-Live Certificate. Each review shall verify IIP's compliance with the service level commitments specified in Annex 2 of the

IFMIS TOR, covering system uptime, response times, incident resolution, and change management compliance. The QA Agency shall submit a Quarterly QA Compliance Report to PMU within five (5) working days of completing each review. Billing shall be at actual effort up to a ceiling of ten (10) person-days per review, supported by timesheets submitted with each invoice.

(b) Security Re-Assessment

The QA Agency shall conduct a security re-assessment of the IFMIS system upon the occurrence of either of the following trigger events:

(i) Major Release: A release by IIP that modifies authentication, authorization, encryption, or access control components; or adds, removes, or materially changes a system interface; or involves a change to the network or server security architecture at Government Data Center. PMU shall determine whether a release constitutes a major release within three (3) working days of IIP's release notification. Routine patches, bug fixes, and releases that do not meet the criteria above shall not constitute trigger events.

(ii) Security Incident: A Critical or High severity security incident notified to PMU by BtCIRT or IIP.

The trigger date shall be the date the qualifying event occurs - not the date of PMU's notification to the QA Agency. PMU shall notify the QA Agency of a trigger event within two (2) working days of its occurrence. The QA Agency shall complete the re-assessment and submit a Security Re-Assessment Report to PMU within fifteen (15) working days of the trigger date. Billing shall be at actual effort up to a ceiling of fifteen (15) person-days per re-assessment, supported by timesheets.

4.4 Concurrent Activity Management

Between T[IFMIS]+12 and T[IFMIS]+15, the QA Agency must carry out two separate workstreams at the same time: Phase 1 Round 1 testing (which begins at T[IFMIS]+12) and Phase 2 design document review (PM8 at T[IFMIS]+12 and PM9 at T[IFMIS]+15). This section sets out exactly what is expected of the QA Agency, IIP, and PMU during this window, and what happens if IIP submits Phase 2 documents late.

The QA Agency's Obligation

The QA Agency must assign two separate teams for the concurrent window — one team dedicated to Phase 1 Round 1 testing and a separate team dedicated to Phase 2 design review. The two teams must be made up of different named individuals. The QA Agency must identify these individuals by name in a Concurrent Activity Staffing Plan, submitted as part of the Final Inception Report. The QA Agency may not assign the same person to both workstreams during the concurrent window without written PMU approval.

The bid price must include all costs for running both teams during T[IFMIS]+12 to T[IFMIS]+15. No variation or additional payment will be accepted for this overlap because it is clearly visible in the project schedule at the time of bidding.

IIP's Submission Obligation

IIP must submit PM8 design documents to PMU no later than T[IFMIS]+12 and PM9 design documents no later than T[IFMIS]+15, in line with the IFMIS TOR milestone schedule. Early submission is encouraged. Late submission by IIP does not extend the QA Agency's Phase 1 Round 1 testing timeline or reduce the QA Agency's Phase 1 testing obligations in any way.

Phase 2 Document Handover - PMU Obligations

To protect the quality of both workstreams, PMU shall manage the timing of Phase 2 document handover to the QA Agency based on when IIP submits the documents. The rules below apply to both PM8 (due at T[IFMIS]+12) and PM9 (due at T[IFMIS]+15).

I. Where IIP submits Phase 2 documents on or before the milestone date: PMU shall forward the documents to the QA Agency within two (2) working days of receipt. The QA Agency's Phase 2 review period shall commence on the date of receipt from PMU. This is the expected and preferred scenario as it allows the QA Agency to complete Phase 2 design review before or alongside Phase 1 Round 1 testing without conflict.

II. Where IIP submits Phase 2 documents after the milestone date but before the QA Agency submits the Phase 1 Round 1 Test Report: PMU shall acknowledge receipt from IIP but shall hold the documents and not forward them to the QA Agency until two (2) working days after the QA Agency submits the Phase 1 Round 1 Test Report to PMU. The QA Agency's Phase 2 review period shall commence on the date of receipt from PMU. IIP's late submission shall be recorded as a milestone delay under the IFMIS TOR.

III. Where IIP submits Phase 2 documents after the QA Agency has submitted the Phase 1 Round 1 Test Report: PMU shall forward the documents to the QA Agency within two (2) working days of receipt. The QA Agency's Phase 2 review period shall commence on the date of receipt from PMU. No penalty shall apply to the QA Agency for any Phase 2 review deadline that falls after the commencement of the Phase 2 review period. IIP's late submission shall be recorded as a milestone delay under the IFMIS TOR.

Independent Assessment of Each Workstream

The QA Agency's performance on Phase 1 Round 1 testing is assessed independently of its Phase 2 design review work, and vice versa. A delay on one workstream cannot be used as a reason or excuse for a delay on the other. If the QA Agency believes the concurrent workload is affecting quality on either workstream, it must notify PMU in writing immediately with specific details. General references to concurrent workload shall not constitute grounds for penalty exemption.

1. *Review Period and Forwarding- Obligations and timelines*

i. Standard Review Period: The QA Agency shall complete review within ten (10) working days from the date of receipt from PMU (working days exclude Bhutanese public holidays). The QA Agency shall acknowledge receipt within one (1) working day.

ii. PMU Forwarding Obligation: PMU shall transmit deliverables to the QA Agency within two (2) working days of receipt from IIP. The QA Agency's review period commences on receipt from PMU, not on IIP's submission to PMU. Delays caused by PMU's forwarding shall not attract penalties against the QA Agency.

iii. Extended Review Period: For deliverables exceeding 150 pages of substantive technical content or full testing round reports covering all test categories, the review

period is fifteen (15) working days. The QA Agency shall notify PMU within two (2) working days of receipt if the extended period applies. PMU may agree to a further extension of up to five (5) additional working days for exceptional complexity, at no additional cost.

iv. Phase 2 Documents During the Concurrent Window: Where PMU holds Phase 2 design documents under the Concurrent Activity Management provision, the two (2) working day PMU forwarding obligation in (e)(ii) runs from the date the QA Agency submits the Phase 1 Round 1 Test Report to PMU - not from the date PMU received the documents from IIP. The QA Agency's standard review period under (e)(i) runs from the date of receipt from PMU. IIP's original submission date is recorded separately for the purpose of tracking IIP's milestone performance under the IFMIS TOR.

v. Penalty Rate: For delays attributable to the QA Agency, RGoB may levy a penalty of zero-point five percent (0.5%) of the fee applicable for the relevant milestone for every seven (7) calendar days or part thereof of delay. The total penalty for any single milestone shall not exceed ten percent (10%) of that milestone's fee. Penalties shall be deducted from the next payable milestone.

vi. Penalty Exemptions: No penalty applies where the delay is caused by: (a) late IIP deliverables required by the QAP; (b) PMU forwarding delay beyond the two-working-day obligation; (c) a force majeure event; or (d) a PMU-approved extension. Where delay is anticipated, the QAP shall notify PMU in writing at least three (3) working days before the due date with reasons and a revised date; approved extensions are not subject to penalty.

4.5 Testing Round, Re-Testing, and Three-Round Completion

A. Testing Round

A Testing Round is a structured cycle of:

(i) QA Agency review and testing of IIP deliverables or system components against the Requirements Traceability Matrix (RTM);

(ii) QA Agency submission of a formal Test Report to PMU documenting all findings by severity;

(iii) PMU forwarding findings to IIP;

(iv) IIP remediation; and

(v) IIP submission of a written Remediation Completion Notice to PMU confirming which findings have been addressed.

A new Testing Round shall not commence until PMU has transmitted the Remediation Completion Notice to the QA Agency.

B. Re-Testing of Fixes in the Subsequent Round

Where IIP submits a fix for a finding identified in Round N after the Round N Test Report has already been submitted to PMU, that fix shall be re-tested by the QA Agency within Round N+1 as part of that round's scope - not as a separate additional round. This ensures all testing and re-testing is completed within three rounds.

The QA Agency shall maintain a Defect Register throughout all testing rounds, tracking each finding's severity, remediation status, and the round in which it was re-verified and closed. All re-testing of prior round findings is included in the man-month pricing for Round N+1. If the volume of carry-forward re-testing exceeds twenty percent (20%) of the contracted Round N+1 effort, the excess shall be compensated at the contracted man-month rate, subject to PMU approval.

C. Three-Round Completion Obligation

The QA Agency and IIP shall together ensure all Critical and High findings from all rounds are re-verified and closed by the end of Round 3. The following rules apply:

End of Round 1: The QA Agency shall issue IIP a Remediation Priority List specifying (a) which findings must be closed before Round 2 commences, and (b) which findings may be carried into Round 2 for re-verification. This list shall be submitted to PMU alongside the Round 1 Test Report.

End of Round 2: All Critical findings must be closed. Any High findings not yet closed must have a PMU-approved remediation date. The Round 2 Test Report shall include a Carry-Forward Register listing all findings being carried into Round 3.

End of Round 3: The Defect Register must show zero open Critical or High findings before the QA Agency can issue a Go-Live Certificate. If any Critical or High finding remains open at the end of Round 3, the QA Agency shall issue a formal No-Go determination, and the matter shall be escalated to the Project Steering Committee.

D. Round 2 Commencement Condition

Round 2 shall not commence until IIP submits a Remediation Completion Notice. The QA Agency shall assess the remediation status of all Critical and High findings from Round 1 and classify readiness using the following framework:

Level	Condition	Decision
Highly Probable	≥90% of Critical and High findings remediated; no unresolved Critical findings	Commence Round 2
Probable	80%–89% remediated; no unresolved Critical findings	Proceed with written risk acceptance from the Project Director
Possible	60%–79% remediated; or Critical findings remain with documented mitigations acceptable to PMU	Commence with conditions specified in writing by PMU
Remote	Below 60% remediated; or unresolved Critical findings without acceptable mitigation	Do not commence

Notwithstanding the thresholds above, the QA Agency may adjust the readiness classification upward or downward by one level where the nature, severity, or systemic significance of outstanding findings warrants a different assessment, provided the adjustment is documented in writing with specific reasons.

E. No Additional Rounds Beyond Round 3

There shall be no Round 4 or beyond under the fixed contract price. If the system cannot be certified after Round 3, the QA Agency shall issue a formal No-Go determination and continue to support PMU through the Project Steering Committee escalation process at the contracted man-month rate, invoiced monthly, until PMU issues a written release notice. See payment clause (g) below.

a. The functional specifications documents (such as FRS, SRS, UI/UX designs, prototypes, etc) shall be subjected to the review of the QA Agency up to a maximum of three rounds of review for each deliverable/artifact.

b. It is expected that the implementation partner will address all the feedback within these three rounds of review.

c. Implementation partner shall ensure that the complete versions of the deliverables are submitted to the PMU established by the Procuring Agency, which in turn will forward the deliverables to the QA Agency for its review and feedback.

d. Any findings from the review shall be communicated by the QA Agency to the PMU, which shall forward the feedback to the implementation partner and/or facilitate a discussion between the QA Agency and the implementation partner.

5. Payment Schedule for IFMIS QA Agency

The bidders are required to quote for each category of testing separately as per the format provided in the bidding document. The quote for each category of testing shall also include necessary costs for tools required to undertake such testing and for phase 1 and phase 2 separately.

#	Trigger / Milestone	Payment (% of Quoted Cost)	Applicable Scope	Tentative Timeline
(a)	Signing of contract; submission and acceptance of Inception Report	5% of total contract value	Entire contract	T+4 Aligned to PM2 gate
(b)	Completion and submission of Round 1 Testing Report	30% of cost quoted for respective test category	Per test category, per phase (Phase 1 / Phase 2 separately)	Phase 1: T+14 Phase 2: T+25
(c)	Completion and submission of Round 2 Testing Report	25% of cost quoted for respective test category	Per test category, per phase (Phase 1 / Phase 2 separately)	Phase 1: T+17 Phase 2: T+26
(d)	Completion and submission of Round 3 / Final Testing Report	35% of cost quoted for respective test category	Per test category, per phase (Phase 1 / Phase 2 separately)	Phase 1: T+20 Phase 2: T+27
(e)	Completion of Round 2 where no further round of testing is required	60% of cost quoted for respective test category (applies in lieu of (c) and (d) combined)	Per test category, per phase—only if Round 2 is the final round	Phase 1: T+17 Phase 2: T+26

'Testing Agency', 'Quality Assurance Provider' and 'QA Agency' will be used interchangeably. (ToR V.1)

(f)	Final QA Certification Report per major milestone, containing Go/No-Go recommendation with supporting evidence; ISO compliance confirmed	5% of total contract value	Per major milestone	T+27 max. Upon completion of Phase 2
(g)	Excess Carry-Forward Re-Testing Variation: Where re-testing of carry-forward findings from Round N within Round N+1 exceeds twenty percent (20%) of the contracted Round N+1 effort, as certified by the QA Agency with supporting timesheets and approved in writing by PMU.	Man-month rate of staff performing the work	Per excess re-testing event, per phase	As incurred - PMU notified before excess occurs; PMU to respond within five (5) working days
(h)	Post-Round 3 Advisory Support (No-Go escalation only): Where the QA Agency issues a No-Go determination after Round 3 and the Project Steering Committee escalation is ongoing, the QA Agency shall provide advisory and oversight support to PMU. This provision does not constitute a fourth round of testing; it covers attendance at PSC meetings, review of IIP remediation evidence, and advisory support to PMU only.	Man-month rate, invoiced monthly with supporting timesheets	Per month until PMU issues written release notice	Monthly - from date of No-Go determination until PMU issues written release notice

Note on T: T[IFMIS] is the IFMIS Contract Commencement Date (date of signing the IFMIS implementation contract with IIP).

T[QA] is the QA Contract Commencement Date (date of signing the QA Agency contract, which is a separate contract with a separate party).

T[QA] should equal T[IFMIS]+3. All T+ timelines in this table are expressed relative to T[IFMIS] for alignment; QAP milestone obligations are measured from T[QA]. Where MOF or PMU delays the QA contract beyond T[IFMIS]+3, QAP milestone deadlines are extended proportionately per Section 4(f)(i).

Note on payment structure: Clauses (b), (c) and (d) apply per test category and per phase.

Together they account for ninety percent (90%) of the phase budget (Round 1 = 30%, Round 2 = 25%, Round 3 = 35%).

The remaining ten percent (10%) retention per phase is released with the Round 3 / Go-Live Certification payment. Clause (e) applies only where PMU and the QA Agency mutually agree that Round 2 is the final round; in that case the combined payment is sixty percent (60%) instead of clauses (c) and (d) separately.

6. Dispute Escalation Procedure

Level 1 (Working Level): QA Agency Representative and IIP Project Manager and PMU Technical lead shall attempt resolution within 2 working days.

Level 2 (Management Level): If unresolved, QA Agency Manager, IIP Project Director and PMU Project Manager shall attempt resolution within 3 working days.

Level 3 (PMU, IIP and QA): If still unresolved, the matter shall be escalated to the Project governance committee (PMU) with IIP and QA representatives. The decision shall be final and binding.

Technical Arbitration: For purely technical disputes, an independent technical expert may be appointed by mutual agreement with costs shared equally among the two (IIP & QAP).

7. Defect Severity Classification

The Defect Severity Classification framework shall be developed and proposed by the QA Agency within the Preliminary Inception Report and shall be subject to PMU approval before commencement of testing activities.

QAP Obligations:

(a) The QA Agency shall submit a comprehensive Defect Severity Classification framework as part of the Inception Report, including clear definitions, examples, and classification criteria for each severity level.

(b) The framework shall include, at minimum, four severity levels (Critical, High, Medium, Low) with objective, measurable criteria for each level.

(c) The framework shall specify expected remediation timeframes for each severity level.

(d) The QA Agency shall apply the approved framework consistently throughout all testing phases.

(e) Any proposed modification to the approved framework shall require written PMU approval.

Go-Live Gate Requirements:

(a) *"No go-live"* status shall be determined by QAP while any defect classified as Critical remains unresolved.

(b) *"No go-live"* shall be determined by QAP while any defect classified as High remains unresolved, unless a formal exception is approved in writing by the Project Director.

(c) All defects classified as Medium shall have a documented remediation plan with specific timelines approved by PMU before go-live certification.

(d) The QA Agency shall maintain a complete Defect Register with severity classifications, and any disputes regarding classification shall be escalated per Section 5 (Dispute Escalation Procedure).

Binding Effect: The approved Defect Severity Classification framework shall form part of the contract and shall be binding on all parties including IIP for remediation obligations.

Note: For security-specific findings, the classification and remediation timeframes as per GovTech standards, shall take precedence over this general framework.

8. Confidentiality and Data Protection

All information provided to the QA Agency as part of this assignment shall remain strictly confidential. Execution of a Non-Disclosure Agreement (NDA) is mandatory before commencement of work.

a) The QA Agency shall sign a Non-Disclosure Agreement during contract agreement.

b) All test data containing actual government financial information shall be masked or anonymized.

c) Security vulnerability findings shall be classified as Confidential and shared only with PMU and designated IIP security personnel.

d) Testing Agency personnel shall undergo background verification acceptable to the procuring agency.

e) All project materials shall be returned or certified destroyed within 30 days of contract completion.

f) Confidentiality obligations survive contract termination for 5 years.

9. Conflict of Interest

The QA Agency warrants that:

a) The QA Agency has no current contractual relationship with the Implementation Partner (IIP) or the IT Infrastructure Implementation Partner (IIIP).

b) No QA Agency personnel have been employed by IIP or IIIP in the past 2 years.

c) QA Agency has no ownership interest or investments in IIP or IIIP or vice versa.

d) QA Agency will not bid for any IFMIS-related implementation work during the contract period and for 2 years after completion.

e) QA Agency shall have no affiliation in any matter whatsoever that is deemed conflicting by the Ministry of Finance. Discovery of undisclosed conflict of interest shall be grounds for immediate termination with forfeiture of retention amounts.

10. Termination and Transition

Termination:

a. The Ministry of Finance may terminate this contract with thirty (30) days written notice, with or without cause. Payment for work satisfactorily completed up to the date of termination shall be made to the QA Agency.

b. DTA may terminate for material breach not cured within 30 days of notice, consistent failure to meet deadlines.

c. DTA may terminate immediately for fraudulent activity or discovery of conflict of interest.

Transition Obligations: Upon termination, QA Agency shall provide complete handover of all testing artifacts within 15 days, brief successor agency for up to 40 person-hours at no additional cost and continue critical testing activities for up to 30 days during transition at current rates.

The QA Agency's liability for defects in positively certified deliverables is limited to: (a) re-performance of the relevant QA activity at no additional cost; and (b) financial liability not exceeding the total fees received by the QA Agency under this contract. The QA Agency shall not be liable for consequential, indirect, or third-party losses, nor for defects arising from IIP's failure to implement the system in accordance with the approved SRS, or from data issues outside the scope of the approved data quality definition.

11. Intellectual Property

a) All test cases, test scripts, test data, and testing frameworks developed specifically for IFMIS shall be the property of the Royal Government of Bhutan.

b) QA Agency may retain rights to generic testing methodologies and proprietary tools brought to the engagement.

c) QA Agency shall provide complete documentation of all custom test artifacts upon contract completion.

d) The government shall have perpetual, royalty-free license to use all testing documentation and artifacts.

12. QA Certification as Mandatory Gate

The QA Agency certification shall be mandatory for all applicable ISO standards. The ISO standards in scope, the QA Agency's verification obligations, and the IIP's evidence submission requirements are fully specified in **Section 4(i) (ISO Certification of IFMIS)** of this TOR. QA Agency certification for any phase milestone shall be withheld until the ISO compliance verification activities specified in Section 4(i) are satisfactorily completed and the QA Agency has issued a formal ISO Compliance Verification Report.

No-Go Decision Authority: QA Agency shall recommend a No-Go decision when any of the following conditions exist:

a) One or more unresolved Critical defect,

b) More than three unresolved High defects without approved remediation plan and timeline,

c) Non-compliance with key non-functional requirements including system availability below 99.5%, response time exceeding SLA thresholds by more than 20%, unresolved Critical or High security vulnerabilities, or DR failover RTO/RPO not demonstrated,

d) Data migration validation failure rate exceeding 1% for critical financial data.

A No-Go recommendation shall be escalated to the Project Steering Committee within 48 hours for final decision. The PSC may override a No-Go recommendation only with documented risk acceptance signed by the Secretary, Ministry of Finance.

13. Mandatory QA Deliverables

QA Agency shall produce and submit deliverables as specified herein. The following list is indicative and not exhaustive; PMU reserves the right to request additional deliverables as may be necessary for comprehensive quality assurance of IFMIS.

Minimum Required Deliverables (including but not limited to):

1. Inception Report (two-stage delivery):

    a. Preliminary Inception Report - within 30 calendar days of T[QA]: QA Strategy, Resource Deployment Plan, Preliminary Defect Severity Classification

Framework, Risk Register, Communication and Reporting Protocol, ISO 27001 SoA Assessment Methodology. Does not require FRS/SRS inputs.

b. Final Inception Report - within 20 working days of PMU transmitting PM4 sign-off documents to the QA Agency. Content: Master Test Plan covering all test categories for both phases; Requirements Traceability Matrix baseline mapped to the approved SRS; ISO 27001 Statement of Applicability Assessment; Defect Severity Classification Framework (final, for PMU approval); and Certification Programme Plan covering all four ISO certifications, showing: certification body engagement timeline, gap assessment schedule, remediation window, audit dates for Stage 1 and Stage 2, first-year surveillance audit schedule, and resource requirements from IIP and PMU. PMU shall confirm written agreement to the Certification Programme Plan within ten (10) working days of receiving the Final Inception Report. The formal ISO certification process shall not commence until PMU has confirmed the Plan in writing.

2. Requirements Traceability Matrix (RTM) - updated with each testing round; 100% of requirements mapped to test cases.
3. Test Case Repository - submitted before each testing phase; shall cover all requirements per the RTM.
4. Test Execution Evidence - submitted with each testing report; shall include screenshots, logs, and data evidence.
5. Defect Register - maintained continuously throughout all testing phases; shall record severity classification, status, age, resolution details, and aging analysis.
6. Performance and Scalability Test Report - submitted before each go-live milestone; all SLA metrics shall be validated.
7. Security Testing Report - submitted before each go-live milestone; shall include VA/PT findings and re-test evidence.
8. DR/Failover Test Report - submitted before each go-live milestone; RTO/RPO shall be demonstrated.
9. Final QA Certification Report - submitted per major milestone; shall contain a Go/No-Go recommendation with supporting evidence.
10. Data Migration Strategy and Validation Report - submitted prior to data migration; 100% validation of data integrity required.
11. Any other deliverables may be reasonably requested by PMU for comprehensive quality assurance of IFMIS.

Minimum QA Deliveries aligned with IFMIS Deliverable

IFMIS Milestone	Tentative Date	IFMIS Deliverables (TOR Table 20)	QA Review Activity	QA Deliverable	QA-PM	QA Gate for IIP Payment Release	QA Payment Trigger
PRE-IMPLEMENTATION & DESIGN PHASE							
Contract Signing (T)	(T)	1.Signed agreement 2.Performance Bank Guarantee	QAP contract executed and team mobilised. No QA review of IIP deliverables- administrative milestone only.	QAP contract signed and effective. QAP team deployment plan confirmed. No QA deliverable at T.	-	None. This is an administrative milestone. No QA deliverable is required before IIP contract signing.	None. No QA payment at T.
PM 1	(T+1)	3.Detailed Project Plan 4.Project Management Approach Document	Project Plan reviewed and noted for information only. Inception Report deferred to PM2 (T+4) when design deliverables are available - no substantive QA review possible at T+1.	None at PM1. Inception Report submission and acceptance deferred to PM2. QA-PM 1 (5%) payment triggered at PM2 gate.	QA-PM 1 (paid at PM2)	None. The QA Agency reviews the project plan for information only. No QA deliverable is required before PM1 payment to IIP.	None at PM1. QA-PM 1 is deferred to the PM2 gate.

Process Design (T+3) [No PM]	(T+3)	5. As-Is study report for Phase 1 functions and services 6. To-Be report (process reengineering, process maps) 7. As-Is and To-Be validation workshops	QAP reviews As-Is and To-Be reports for alignment with functional requirements. Findings incorporated into SRS & UI/UX Verification Report (QA-PM 2) - no standalone payment deliverable at T+3.	As-Is & To-Be Review Findings Note - sub-section of SRS & UI/UX Verification Report (QA-PM 2). Not a standalone deliverable.	QA-PM 2 (included)	None. No IIP payment at this milestone. QA findings from As-Is/To-Be review are recorded as input to the PM2 Part A gate.	None.
PM 2 (Part A) System Design (T+3)	(T+3)	8. UI/UX Prototypes - Phase 1 processes 9. System Requirements Specification (SRS) - Phase 1 10. System Architecture & Design Document (SDD) 11. Training Plan for IFMIS 12. Data digitization	[QA-PM 1 - moved from PM1] Inception Report submitted and accepted by PMU: QA Strategy, Master Test Plan, Resource Plan, Defect Severity Framework, ISO 27001 SoA Assessment Protocol. [QA-PM 2 - Part A] Review SRS completeness against FRS; SRS proceed-tab sign-off. Review UI/UX Prototypes. Review SDD for architectural soundness. Validate IT	1. Inception Report - QA Strategy, Master Test Plan (all categories, both phases), Resource Plan, Defect Severity Classification Framework, ISO 27001 SoA Protocol, RTM baseline. 2. SRS & UI/UX Verification Report Phase 1 (Part A) - FRS/SRS sign-off (proceed-tab), UI/UX review, SDD technical review, IT Infrastructure Sizing verification.	QA-PM 1 + QA-PM 2 (Part A)	The following must be accepted by PMU before PM2 Part A payment is released to IIP: (1) Preliminary Inception Report accepted by PMU. (2) SRS and UI/UX Verification Report Phase 1 Part A, with FRS/SRS proceed-tab sign-off, accepted by PMU.	QA-PM 1 is released upon PMU acceptance of the Preliminary Inception Report. QA-PM 2 tranche 1 (3%) is released at the same PM2 gate alongside QA-PM 1.

		and migration strategy 13. IT Infrastructure sizing report (Production & DR)	Infrastructure Sizing Report.				
PM 2 (Part B) As-Is/To-Be Sign-off (T+4)	(T+4)	14. Sign-off on As-Is & To-Be Reports - updated based on RGoB feedback from T+3 workshops	[QA-PM 2 - Part B] Review updated As-Is & To-Be reports incorporating RGoB feedback. Verify alignment with SRS. Issue final sign-off on Phase 1 process design. Complete SRS & UI/UX Verification Report.	SRS & UI/UX Verification Report Phase 1 (Final) - complete report incorporating As-Is/To-Be review findings. PMU acceptance of the SRS & UI/UX Verification Report (Final) triggers QA-PM 1 (5%) and QA-PM 2 (5%) = 10% combined payment.	QA-PM 2 (Final)	SRS and UI/UX Verification Report Phase 1 (Final), incorporating As-Is/To-Be review findings, accepted by PMU.	No separate QA payment at Part B. Acceptance of the Final Report completes the PM2 IIP payment gate.
PM 3	(T+4)	15. IT Infrastructure delivery & installation report - development, test and training instances	Infrastructure Verification: physical installation check against IT Infrastructure Sizing Report; configuration compliance; GovTech Basic Minimum Standards; BDC/DR connectivity and failover configuration.	Infrastructure Verification Report - Pass/Fail determination, itemised findings, GovTech standards compliance, BDC/DR connectivity verification, open items list.	QA-PM 3	Infrastructure Verification Report accepted by PMU.	QA-PM 3 is released upon PMU acceptance of the Infrastructure Verification Report.

PM 4	(T+6)	16. Updated System Design reports (based on RGoB review) 17. Test Strategy, Test Plans, Test Cases - Phase 1 18. Templates for government agency data preparation	Review updated SDD for incorporation of RGoB feedback. Validate Phase 1 Test Strategy, Test Plans and Test Cases for SRS coverage adequacy. Sign-off addendum to SRS & UI/UX Verification Report. Triggers remaining 3% of QA-PM 2.	System Design & Test Strategy Sign-Off Note - addendum to SRS & UI/UX Verification Report confirming updated SDD adequacy and Phase 1 test case coverage. Triggers final 3% of QA-PM 2.	QA-PM 2 (extended 2%)	System Design and Test Strategy Sign-Off Note accepted by PMU.	QA-PM 2 final tranche (2%) is released upon PMU acceptance of the Sign-Off Note.
PHASE 1 TESTING (3 ROUNDS)							
PM 5	(T+12)	19. Developed IFMIS solution submitted for UAT 20. IIP internal test results 21. Preliminary review report confirming Phase 1 process coverage (prior to UAT acceptance)	Phase 1 Round 1 Testing commences: functional testing of all Phase 1 modules (SRS coverage); integration testing (RMA, e-GP, HRMIS, BITS/RAMIS, Meridian/CS-DRMS); security VA/PT; ISO 27001:2022 controls checklist Round 1; performance baseline.	Phase 1 Round 1 Test Report: • Functional Test Results (RTM pass/fail) • Integration Test Results (all interfaces) • Security Testing Report Round 1 (VA/PT, severity classified) • ISO 27001 Controls Checklist Round 1 • Defect Register (all findings classified) • RTM (updated)	QA-PM 4 (Ph.1 Rd.1)	None at PM5. IIP development completion milestone. Phase 1 Round 1 testing commences at this point. Phase 1 Round 1 Test Report is required before PM6, not PM5.	None at PM5. QA-PM 4 is triggered at the 3P Testing Reports milestone (T+14).

3P Testing Reports (T+14) [RGOB Milestone]	(T+14)	RGOB milestone - IIP has no deliverable. Deliverables are the responsibility of RGoB/QAP: Submission of third party and user acceptance testing reports. Note: QAP IS the designated third party QA Agency.	QAP submits Phase 1 Round 1 Test Report to PMU at T+14. This IS the third party acceptance testing report referenced in IFMIS TOR. PMU reviews and forwards to IIP for gap addressing.	Phase 1 Round 1 Test Report submitted at T+14 - this is the QA-PM 4 deliverable. Payment triggered upon PMU acceptance.	QA-PM 4 (payment at T+14)	Phase 1 Round 1 Test Report submitted to and accepted by PMU.	QA-PM 4 is released upon PMU acceptance of the Phase 1 Round 1 Test Report.
Gap Addressing (T+16) [No PM]	(T+16)	22. Action Taken Reports on acceptance testing gaps 23. Corrective actions documented	QAP reviews IIP's Action Taken Reports to verify Round 1 gaps have been addressed. Findings feed into Phase 1 Round 2 testing scope.	ATR Verification Note - QAP's written confirmation that IIP's ATRs adequately address Round 1 findings. Included as input section in Phase 1 Round 2 Test Report.	QA-PM 5 (input)	ATR Verification Note confirming IIP gaps from Round 1 have been adequately addressed, submitted to PMU.	None. ATR Verification Note is an input to Round 2. No separate QA payment.

Data Migration (T+16) [No PM]	(T+16)	24. Data Quality Assessment Reports (multiple stages) 25. Migration of corrected data into IFMIS 26. Data migration status reports 27. Escalation Reports for delays	QAP conducts Data Quality Assessment: record count reconciliation (100%), financial balance reconciliation (zero variance), data transformation mapping verification. Witnesses cutover dry run and signs off cutover readiness checklist.	Data Quality Assessment Report - record count reconciliation, financial balance reconciliation, data transformation validation, document attachment sampling. Input to Phase 1 Round 2 Test Report.	QA-PM 5 (input)	Data Quality Assessment Report submitted to PMU.	None. Data Quality Assessment Report is an input to Round 2. No separate QA payment.
PM 6	(T+18)	28. Fully tested, error-free IFMIS Phase 1 (source code, library files, DLLs, setup programs, documentation)	Phase 1 Round 2 Testing: regression testing (Round 1 defect fixes); Performance & Scalability (load, stress, BDC/DR failover - RTO/RPO); UAT support; ISO 27001:2022 controls checklist Round 2; Manageability review. Verify ≥80% Critical/High remediation from Round 1.	Phase 1 Round 2 Test Report: • Regression Test Results • Performance & Scalability Report (all SLA metrics) • DR/Failover Test Report (RTO/RPO demonstrated) • Security Testing Report Round 2 (re-test evidence) • ISO 27001 Controls Checklist Round 2 • ATR Verification + Data Quality Assessment • Updated Defect Register	QA-PM 5 (Ph.1 Rd.2)	Phase 1 Round 2 Test Report accepted by PMU.	QA-PM 5 is released upon PMU acceptance of the Phase 1 Round 2 Test Report.

Trial Launch (T+18) [No PM]	(T+18)	29. System Launch for trial phase (existing e-PEMS users; 4–6 weeks)	QAP observes trial launch; monitors production system behaviour; tracks user-reported issues. Findings documented as input to Phase 1 Round 3 testing.	Trial Phase Observation Report - summary of trial phase issues, user-reported defects, system behaviour findings. Included as input in Phase 1 Round 3 Final Test Report.	QA-PM 6 (input)	Trial Phase Observation Report submitted to PMU.	None. Observation Report is an input to Round 3. No separate QA payment.
System Stabilization (T+21) [No PM]	(T+21)	30. Updated reports for all deliverables (issues identified/resolved during stabilization) 31. Issue Log and Action Taken Report	QAP verifies all issues from trial phase and stabilization resolved. Reviews Issue Log and ATR. Confirms zero unresolved Critical/High defects. ISO 27001 controls final verification pass.	Final Issue Resolution Verification Note - QAP confirmation that Issue Log and ATR complete, all Critical/High resolved. Included in Phase 1 Round 3 Final Test Report as pre-condition for Go-Live Certificate.	QA-PM 6 (input)	Final Issue Resolution Verification Note confirming zero unresolved Critical or High defects, accepted by PMU.	None. Pre-condition for Go-Live Certificate. No separate QA payment.
PM 7 Go-Live Phase 1	(T+21)	32. Updated stabilization reports 33. Go-Live Certificate from RGoB 34. Issue Log and Action Taken Report (final)	Phase 1 Round 3 (Final): final regression pass; zero Critical/High confirmed; SLA Reporting System verification; Data Migration final validation; ISO 27001 controls Round 3 - all non-conformances resolved; Trial Phase and	Phase 1 Round 3 Final Test Report: • Final Regression Test Results • Phase 1 Go-Live Certificate (Go/No-Go + evidence) • SLA Reporting System Verification	QA-PM 6 (Ph.1 Rd.3)	The following must be accepted by PMU before PM7 Go-Live payment is released to IIP: (1) Phase 1 Round 3 Final Test Report accepted by PMU. (2) Phase 1 Go-Live Certificate issued by the QA Agency and accepted by PMU.	QA-PM 6 is released upon PMU acceptance of the Phase 1 Round 3 Final Test Report and the Phase 1 Go-Live Certificate.

			Stabilization findings verified resolved; QAP issues Phase 1 Go/No-Go Go-Live Certificate.	• Data Migration Validation (100% accuracy) • ISO 27001 Controls Sign-Off Phase 1 • Trial Phase Observation Report • Final Issue Resolution Verification Note • Defect Register (zero Critical/High open)			
Warranty Phase 1 (Quarterly)	From Phase 1 Go-Live	35. Warranty & AMC for Phase 1 products 36. Post-implementation support 37. Performance Monitoring Reports 38. Updated system design docs, source code, config files 39. Updated user/admin/training manuals	Periodic SLA compliance verification (quarterly); security re-assessment for major changes; change management documentation review; spot-check of updated deliverables.	Quarterly QA Compliance Report - SLA compliance evidence, change management review, security re-assessment findings (if triggered), spot-check findings on updated deliverables.	Warranty QA Scope	Quarterly QA Compliance Report submitted to PMU each quarter from the Phase 1 Go-Live Certificate date.	Included in contract price. No separate QA-PM payment for warranty activities.

		40. Software change logs					
PHASE 2 DESIGN							
PM 8	(T+12)	41. Phase 2 process and functional design sign-off (Same scope as Phase 1 process/functional design deliverables)	Review Phase 2 As-Is/To-Be reports and functional design applying Phase 1 review protocol. SRS proceed-tab sign-off for Phase 2. Issued as addendum to QA-PM 2.	SRS & UI/UX Verification Report Phase 2 - Part A: As-Is/To-Be and Functional Design sign-off, Phase 2 SRS proceed-tab. Addendum to QA-PM 2.	QA-PM 2 (extended)	SRS and UI/UX Verification Report Phase 2 Part A (As-Is/To-Be and functional design sign-off) accepted by PMU.	No additional QA payment. Phase 2 design review is within the QA-PM 2 scope, which has already been settled.
PM 9	(T+15)	42. Phase 2 system design (SDD, Test Plans, Test Cases) (Same scope as Phase 1 system design deliverables)	Review Phase 2 SDD and Test Plans/Cases. Validate test case coverage against Phase 2 SRS. Sign-off addendum to SRS & UI/UX Verification Report Phase 2.	SRS & UI/UX Verification Report Phase 2 - Part B: Phase 2 SDD review, test case coverage assessment. Final Phase 2 design sign-off addendum.	QA-PM 2 (extended)	SRS and UI/UX Verification Report Phase 2 Part B (SDD review and test case coverage adequacy) accepted by PMU.	No additional QA payment. Phase 2 design review is within the QA-PM 2 scope, which has already been settled.
PHASE 2 TESTING (3 ROUNDS)							

PM 10	(T+24)	43. Phase 2 development complete; submitted for third-party acceptance testing and QA (Same scope as Phase 1 development deliverables)	Phase 2 Round 1 Testing: functional testing of all Phase 2 modules; integration with Phase 1 live production; security VA/PT; ISO 27001:2022 controls checklist Phase 2 Round 1; performance baseline. QAP submits Phase 2 Round 1 Report at T+25.	Phase 2 Round 1 Test Report: • Functional Test Results Phase 2 (RTM Phase 2) • Integration Test Results (Phase 2 + Phase 1 live) • Security Testing Report Phase 2 Round 1 • ISO 27001 Controls Checklist Phase 2 Round 1 • Defect Register Phase 2	QA-PM 7 (Ph.2 Rd.1)	Phase 2 Round 1 Test Report accepted by PMU.	QA-PM 7 is released upon PMU acceptance of the Phase 2 Round 1 Test Report.
PM 11	(T+26)	44. Phase 2 acceptance testing and certification (Same scope as Phase 1 acceptance testing deliverables)	Phase 2 Round 2 Testing: regression; full Performance & Scalability (Phase 1+2 integrated); Data Quality Phase 2; UAT support; ISO 27001 controls checklist Phase 2 Round 2; verify ≥80% Critical/High remediation.	Phase 2 Round 2 Test Report: • Regression Test Results Phase 2 • Performance & Scalability Report (integrated Ph.1+2) • Security Testing Report Phase 2 Round 2 • ISO 27001 Controls Checklist Phase 2 Round 2 • Data Quality Assessment Report Phase 2 • Updated Defect Register Phase 2	QA-PM 8 (Ph.2 Rd.2)	Phase 2 Round 2 Test Report accepted by PMU.	QA-PM 8 is released upon PMU acceptance of the Phase 2 Round 2 Test Report.

PM 12 Go-Live Phase 2	(T+28)	45. Phase 2 Go-Live 46. All updated deliverables (same scope as PM7): stabilisation reports, Issue Log, Go-Live Certificate from RGoB	Phase 2 Round 3 (Final): final regression; zero Critical/High confirmed; full IFMIS SLA verification; Data Migration final validation (production); ISO 27001 controls Phase 2 Round 3 - all non-conformances resolved; Phase 2 Go-Live Certificate issued.	Phase 2 Round 3 Final Test Report: • Final Regression Test Results Phase 2 • Phase 2 Go-Live Certificate (Go/No-Go + evidence) • SLA Reporting System Verification (full IFMIS) • Data Migration Validation Phase 2 (100% accuracy) • ISO 27001 Controls Sign-Off Phase 2 • Defect Register Phase 2 (zero Critical/High open)	QA-PM 9 (Ph.2 Rd.3)	The following must be accepted by PMU before PM12 Go-Live payment is released to IIP: (1) Phase 2 Round 3 Final Test Report accepted by PMU. (2) Phase 2 Go-Live Certificate issued by the QA Agency and accepted by PMU.	QA-PM 9 is released upon PMU acceptance of the Phase 2 Round 3 Final Test Report and the Phase 2 Go-Live Certificate.
ISO CERTIFICATION VERIFICATION							
ISO Verification (Post-PM 10)	(T+27 max.)	47. ISO 9001:2015 certificate - IIP organisational (IFMIS project scope) 48. ISO 27001:2022 certificate - IIP organisational (IFMIS deployment security scope)	ISO Compliance Gap Assessment of IFMIS deployment at GovTech DC against ISO 27001:2022 Annex A; review of IIP certificates; verify remediation of all Critical/Major non-conformances from all testing rounds; issue	ISO Compliance Verification Report: • ISO 27001 Controls Summary (all rounds, Phase 1+2) • Gap Assessment Report (vs ISO 27001:2022 Annex A) • IIP certificate verification (validity and scope)	QA-PM 10	All four ISO certificates delivered to PMU: ISO/IEC 27001:2022 (with ISO 27017 and ISO 27701 extensions), ISO 9001:2015, ISO/IEC 20000-1:2018, and ISO 22301:2019.	QA-PM 10 is released upon delivery of all four ISO certificates to PMU.

			ISO Readiness Declaration.	• Evidence of remediation of Critical/Major non-conformances • ISO Readiness Declaration			
WARRANTY & OPERATIONS PHASE (PHASE 1 + PHASE 2)							
Warranty (Quarterly)	Ph.1: from Phase 1 Go-Live Ph.2: from Phase 2 Go-Live	49. Warranty & AMC for all IFMIS products 50. Post-implementation support 51. Performance Monitoring Reports 52. Updated system design docs, source code, config files 53. Updated user/admin/training manuals 54. Software change logs	Periodic SLA compliance verification (quarterly); security re-assessment for major changes; change management documentation review; spot-check of updated deliverables. Covers Phase 1 from Jan 2028, Phase 2 from Aug 2028.	Quarterly QA Compliance Report - SLA compliance review, change management review, security re-assessment findings (if triggered), spot-check findings on updated deliverables.	Warranty QA Scope	The following QA reports are required each period: Quarterly QA Compliance Report (each quarter); Security Re-Assessment Report (where a trigger event occurs); Change Management Spot-Check Report (each quarter); Annual Documentation Review Report (annually from first anniversary of Phase 1 Go-Live).	Included in contract price. No separate QA-PM payment for warranty and operations phase activities.

PMU Rights and Protections:

a. PMU reserves the absolute right to request additional deliverables, reports, or documentation as deemed necessary for quality assurance purposes, at no additional cost to RGoB provided such requests are within the general scope of QA services.

b. PMU Review Period: PMU shall communicate acceptance, conditional acceptance, or rejection (with written reasons specifying which acceptance criteria failed and the changes required) within ten (10) working days of receipt; fifteen (15) working days for full testing round reports covering all test categories.

c. Deemed Acceptance: Absence of PMU communication within the applicable review period constitutes deemed acceptance on the day following expiry of that period. Deemed acceptance carries the same legal effect as formal written acceptance for the purpose of triggering QAP payment.

d. Rejection Protocol: A rejection must specify with particularity which acceptance criteria the deliverable failed and the specific changes required. Vague or generic feedback shall not constitute a valid rejection. The QA Agency shall resubmit within five (5) working days of a valid rejection. A second rejection of the same deliverable shall be escalated under Section 6 (Dispute Escalation Procedure).

e. Partial Acceptance: PMU may issue partial acceptance for deliverables with separable components, releasing payment for accepted portions without withholding the entire milestone payment.

f. PMU may engage independent reviewers to assess deliverable quality at PMU's discretion, and QA Agency shall address any findings raised by such reviewers.

Quality Standards and Acceptance:

a) All deliverables shall be complete, accurate, professionally formatted, and free from material errors or omissions.

b) Deliverables shall be submitted in formats specified by PMU (MS Word, Excel, PDF as applicable) with version control.

c) PMU acceptance of any deliverable shall not constitute waiver of any defects subsequently discovered, and QA Agency remains liable for the accuracy and completeness of all deliverables.

Consequences of Non-Compliance:

a) Failure to submit mandatory deliverables within specified timelines shall result in withholding of corresponding milestone payments until satisfactory submission.

b) Deliverables rejected by PMU more than twice for quality deficiencies shall trigger penalty provisions under Section 17 (Consequences for QA Delays).

c) Persistent failure to meet deliverable quality standards (three or more instances) shall constitute grounds for termination for cause under Section 9.

d) QA Agency shall be liable for any losses, damages, or additional costs incurred by RGoB due to inaccurate, incomplete, or misleading deliverables, including but not limited to costs arising from defects not identified due to inadequate testing or reporting.

Binding Effect: This deliverables clause shall be strictly construed, and the enumerated list shall not limit PMU's right to require comprehensive quality assurance documentation as necessary to protect RGoB's interests in the IFMIS implementation.

14. Enhanced Security Assurance Requirements

Security Assurance Scope and Methodology: The QA Agency shall conduct comprehensive security assurance activities. The following list is indicative and not exhaustive; PMU reserves the right to require additional security testing as deemed necessary to protect IFMIS and RGoB's interests. Minimum required activities include, but are not limited to:

a) Vulnerability Assessment (VA) using industry-standard automated scanning tools and methodologies,

b) Penetration Testing (PT) covering critical functions including but not limited to authentication, authorization, payment processing, data access, and any other functions identified by PMU,

c) Code review for custom-developed components and any third-party integrations,

d) Configuration review for infrastructure components,

e) Any other security assessments required by PMU or mandated by applicable regulations and standards.

Security Finding Classification (Minimum Framework - QA Agency may propose additional severity levels):

Critical (Severity 1) - Actively exploitable vulnerability with immediate risk of unauthorized access, data breach, financial loss, or complete system compromise. Examples: SQL injection in payment module, authentication bypass, remote code execution, exposed credentials. Remediation: IMMEDIATE - IIP must acknowledge within 4 hours and implement a fix within 24 hours. System components may be taken offline if necessary.

High (Severity 2) - Significant vulnerability that could lead to unauthorized access or data exposure under specific conditions. Examples: Privilege escalation, insecure direct object references, cross-site scripting (stored), weak encryption, missing access controls. Remediation: IIP must acknowledge within 24 hours and implement a fix within 72 hours (3 days). Temporary mitigations must be in place within 24 hours.

Medium (Severity 3) - Moderate risk vulnerability with limited exploitability or impact, or where effective mitigations exist. Examples: Cross-site scripting (reflected), information disclosure, session management issues, missing security headers.

Remediation: IIP must acknowledge within 48 hours and implement a fix within 14 days. Documented mitigation plan required within 7 days.

Low (Severity 4) - Minor issues, defense-in-depth recommendations, or best practice deviations with minimal direct risk. Examples: Verbose error messages, outdated but non-vulnerable libraries, missing optional security headers.

Remediation: IIP must acknowledge within 7 days and implement a fix within 30 days or provide documented risk acceptance.

Mandatory Re-Testing:

All Critical and High findings shall be re-tested after IIP remediation. Re-test evidence shall be included in the Security Testing Report.

The QA Agency shall not certify go-live until re-test confirms successful remediation.

Zero Tolerance Policy:

a) Zero unresolved Critical security findings at go-live - no exceptions permitted,

b) Zero unresolved High security findings at go-live with no exceptions.

Unresolved Medium findings require documented risk acceptance signed by the DTA Director.

PMU Rights and Protections:

a) PMU reserves the absolute right to require additional security testing methodologies, tools, or assessments not explicitly listed herein, at no additional cost to RGoB provided such requests are within the general scope of security assurance therefore, the tests required must be costed at the *RFP stage*.

b) PMU may engage independent security reviewers to validate the Testing Agency findings; QA Agency shall address any discrepancies identified.

c) The Testing Agency shall stay current with emerging security threats and proactively recommend additional testing where vulnerabilities in similar systems have been identified.

d) The Testing Agency shall be liable for any security breaches resulting from inadequate testing or failure to identify known vulnerability patterns.

Binding Effect: This security assurance clause shall be strictly construed to maximize protection of IFMIS. The enumerated methodologies shall not limit PMU's right to require any security testing necessary to ensure system integrity, confidentiality, and availability.

15. Data Migration and Financial Integrity Assurance

Record Count and Financial Reconciliation

The QA Agency shall verify:

a) 100% verification of record counts across all migrated tables with source-to-target reconciliation,

b) Financial balance reconciliation for all control accounts including opening balances matching source system, trial balance reconciliation, and subsidiary ledger to general ledger reconciliation,

c) Reconciliation variance tolerance of zero for financial amounts.

Note: 'Critical financial data' includes all monetary amounts, account balances, transaction records, and fields essential for financial reporting accuracy.

Data Migration Validation Thresholds:

- Critical Financial Data: Zero tolerance for errors
- Data Quality Validation: Maximum 1% failure rate for non-critical data fields
- Record Count Reconciliation: 100% accuracy required
- Financial Amount Reconciliation: Zero variance tolerance (100% accuracy required)

Data Sampling and Validation: The QA Agency shall validate all data transformations and mappings against the approved mapping specifications, with full coverage required.

Audit Trail Verification: Verification that audit logs are migrated with source timestamps preserved; confirmation of user action traceability post-migration; validation of document attachments and linkages to transactions.

Cutover Procedure Validation: The QA Agency shall witness and validate the following but not limited to:

i. at least one cutover dry run,
ii. verification of rollback procedures before production cutover
iii. confirmation of data freeze periods and
iv. reconciliation checkpoints
v. sign-off on cutover readiness checklist before production migration.

Data migration shall not proceed to production without QA Agency certification of a successful cutover dry-run. A dry-run is deemed successful when all of the following objective criteria are met: (a) record count reconciliation shows zero discrepancy across all tables; (b) financial balance reconciliation for all control accounts shows zero variance; (c) at least ninety-five percent (95%) of data transformation mappings validate correctly against approved mapping specifications; and (d) all critical audit trail linkages are preserved and verifiable. The QA Agency shall issue a Cutover Readiness Certificate within three (3) working days of completing dry-run validation. A failed dry-run triggers a Dry-Run Failure Report; IIP shall remediate and request a further dry-run.

16. Objective Acceptance Criteria

To ensure clarity and avoid endless review cycles, issues shall be deemed 'satisfactorily resolved' when the following objective criteria are met:

a) Defects: The reported defect is no longer reproducible under the same test conditions.
b) Non-Compliance: The identified non-compliance has been corrected to fully meet the documented requirement in the FRS/SRS.
c) Performance: The system meets or exceeds the SLA threshold for the specific performance metric.
d) Documentation: Required documentation has been updated with the requested information and approved by PMU.
e) Security: Vulnerability has been remediated and re-testing confirms the issue is resolved (no longer exploitable).

Disputes regarding whether acceptance criteria have been met shall be escalated per the Dispute Escalation Procedure in Section 5.

17. Consequences for QA Delays

Testing reports shall be submitted within the agreed timelines as per the project schedule. This section elaborates the penalty provisions established in Section 4(f) of this TOR. The following consequences apply for delays attributable to the QA Agency:

Penalty Structure (Synchronized with Section 4(f)): For any delays in achieving the milestones to the satisfaction of RGoB, for reasons attributable to the QA Agency, the following penalties shall apply:

A) RGoB may levy a penalty up to 0.5% (point five) of the fee applicable for the milestone for every 2 days of delay.

B) Any foreseen delays which are discussed, documented and approved by RGoB in writing shall be exempted from penalties.

C) Three instances of delays exceeding 3 weeks (21 days) shall constitute grounds for termination for cause under Section 9.

D) Delays caused by late deliverables from IIP or circumstances beyond QA Agency's reasonable control (documented and approved by PMU in writing) shall not attract penalties. (e) PMU shall be the sole judge of whether delays are attributable to QA Agency. (f) Penalty deductions shall be made from the relevant milestone payment or subsequent payments if milestone payment has been released.

Binding Effect: This penalty clause shall be strictly enforced. The QA Agency acknowledges that timely delivery is critical to IFMIS implementation success and accepts these consequences as reasonable and proportionate.

18. Integration Testing Scope

Integration testing scope shall be determined by the external systems and interfaces documented in the approved Functional Requirements Specification (FRS) and System Requirements Specification (SRS).

The QA Agency shall test all interfaces identified therein. This approach ensures:

a) alignment with actual system design rather than assumptions,

b) coverage of any systems added or modified during implementation,

c) flexibility to accommodate RGoB's evolving integration needs.

IIP Obligations for Integration Testing:

a) IIP shall provide all test environments for external system integrations as specified in the FRS/SRS,

b) IIP shall provide or coordinate provision of test data for all integration scenarios,

c) IIP shall serve as Integration Test Lead and coordinate with external system owners,

d) IIP shall ensure interface documentation is complete and current,

e) IIP shall remediate all integration defects within the applicable timeframes (security defects per Section 14, functional defects per the approved framework in Section 6

QA Agency Responsibilities:

a) Review of integration specifications and interface documentation provided by IIP,

b) Development of integration test cases covering all interface scenarios documented in FRS/SRS,

c) Execution of integration tests in coordination with IIP,

d) Verification of data integrity, transaction completeness, and error handling across system boundaries,

e) Testing of fallback and recovery procedures for each integration,

f) Reporting of integration defects with clear identification of the responsible party (IIP or external system owner).

PMU Rights:

a) PMU may require testing of additional integrations not originally documented in FRS/SRS if identified during implementation,

b) PMU shall be informed of any integration scope changes and reserves the right to adjust QA effort and budget accordingly,

c) PMU may engage independent reviewers to validate integration test coverage.

Binding Effect: The integration testing scope shall encompass all external systems and interfaces documented in the approved FRS/SRS, and any amendments thereto. QA Agency cannot exclude any documented integration from testing without written PMU approval.

Annexure

Annex A: IFMIS Implementation Schedule and Deliverables (Reference)

The following table reproduces the IFMIS Implementation Schedule and Deliverables (Table 20) from the IFMIS Terms of Reference (Final Version, 31 March 2026). It is included here as a reference annex to enable the QA Agency to align its review activities, deliverables, and payment milestones with the corresponding IIP milestones and deliverables. The QA Agency shall treat this table as the authoritative source for IIP milestone sequencing. In the event of any discrepancy between this annex and the IFMIS TOR, the IFMIS TOR shall prevail.

T in the timeline column refers to the IFMIS Contract Commencement Date (T[IFMIS]) - the date of signing the IFMIS implementation contract with the Implementation Partner (IIP). T[IFMIS] = April 2026.

S. N	**Milestone**	**Deliverables from IIP**	**Timelines for completion**
1)	Signing the agreement and commencement of services	1) Signed agreement. 2) Submission of Performance bank guarantee	T
2)	Submission of detailed project plan **(PM1)**	3) Detailed project plan 4) Project management approach document	T + 1
3)	Completion of process design for IFMIS for Phase 1	5) As-Is study report for functions and services for Phase 1 6) To-be report detailing the recommendations for reengineering the current business processes, forms and formats, to-be process maps 7) Workshops for As-Is validation and to-be process validation	T + 3
4)	Sign-off on As-Is and To-Be Reports for IFMIS **(PM2)**	Updated Reports for deliverables listed in S. No 3 above based on feedback provided by GoB during review	T + 4
5)	Completion of System Design for IFMIS for phase 1 (PM2)	8) Finalize Prototypes for UI/UX for Phase 1 processes 9) Finalize System Requirements Specifications for IFMIS based on the approved to-be process report including	T + 3

S. N	Milestone	Deliverables from IIP	Timelines for completion
		system integration/interfacing requirements. 10) System Architecture & Design Document (SDD) for IFMIS 11) Training Plan for IFMIS 12) Data digitization and migration strategy 13) IT Infrastructure sizing report for Production and DR instance	
6)	Installation of development and test instances for IFMIS **(PM3)**	14) IT Infrastructure delivery & installation report for development, test and training instances	T + 4
7)	Sign-off on System Design for IFMIS **(PM 4)**	15) Updated Reports for deliverables listed above based on feedback provided by RGOB during review. 16) Test strategy, test plans, test cases 17) Templates for preparation of data by the government agencies	T + 6
8)	Completion of System Development and provide a system for third party acceptance testing and QA for Phase 1 modules. **(PM5)**	18) Design and development of solution proposed for IFMIS (*developed IFMIS solution submitted for UAT*) 19) Test results for testing carried out by IIP 20) Preliminary review report from RGOB to verify whether the delivered system covers all the processes as signed off for phase 1 (prior to acceptance of system for UAT)	T + 12
9)	Submission of third party and user acceptance testing reports for IFMIS	None (Deliverables for this milestone shall be responsibility of RGOB and is dependent on conformance of IIP's performance against the above-mentioned activities and milestones).	T + 14
10)	Addressing the gaps identified in Third party audit	21) Action Taken reports on issues identified during the acceptance testing and relevant corrective actions	T + 16

S. N	Milestone	Deliverables from IIP	Timelines for completion
11)	Data Quality Assessment and Data Migration	22) Status Reports (*multiple during data receipt and migration stages*) 23) Escalation Reports for delays in receipt of filled up data formats 24) Data Quality Assessment Reports (*multiple during data receipt and migration stages*) 25) Migration of updated and corrected data into IFMIS 26) Data migration status reports (*multiple during data receipt and migration stages*)	T + 16
12)	Operational acceptance of IFMIS for Phase 1 Modules **(PM6)**	27) Fully tested, error free version of the software for IFMIS (*including systems and sub-systems along with source Code, library files, DLL's, Setup programs, Documentation etc.*)	T + 18
13)	IFMIS Launch for Trail Phase	28) System Launch for trial phase	T + 18
14)	System Stabilization	29) Updated reports for the deliverables listed above based on issues identified and resolved during system stabilization period and submitted to RGOB. 30) Issue Log and Action Taken Report	T+ 21
15)	IFMIS Go-Live for Phase 1 **(PM 7)**	31) Updated reports for the deliverables listed above based on issues identified and resolved during system stabilization period and submitted to RGOB. 32) Go-Live Certificate from RGOB 33) Issue Log and Action Taken Report	T+ 21
16)	Warranty, Maintenance and Support Services for Phase 1	34) Warranty and AMC for the products deployed by the IIP for IFMIS 35) Post Implementation Support for IFMIS application software and supporting	Starting from Go-live of IFMIS Phase 1 and to last

S. N	Milestone	Deliverables from IIP	Timelines for completion
		system components including issue resolution, bug fixing etc. 36) Performance Monitoring Reports for the IFMIS Solution 37) Updated system design documents, specifications 38) Updated source code, application deployment files, configuration files for entire solution 39) Updated user manuals, administration manuals, training manuals etc 40) Software change logs etc	until end of the contract.
17)	Sign-off on As-Is and To-Be Reports for IFMIS Phase 2 **(PM 8)**	41) Same outputs as applicable for process and functional design for Phase 1 modules	T + 12 Months
18)	Completion of System Design for Phase 2 Modules **(PM 9)**	42) Same outputs as applicable for system design for phase for Phase 1 modules	T + 15 Months
19)	Completion of Development for Phase 2 modules **(PM 10)**	43) Same outputs as applicable for system development phase for Phase 1 modules	T + 24 Months
20)	Completion of Acceptance Testing and Certification of application software (Phase 2) **(PM 11)**	44) Same outputs as applicable for acceptance testing and certification for Phase 1 modules	T + 26 Months
21)	Go-Live for Phase 2 Modules (**PM 12**)	**45)** Same outputs as applicable for go-live for Phase 1 modules	T + 28 Months