Annex D- Service Level Requirements Checklist

The successful Proponent is required to meet the service level outlined below.

1. Incident Management – Time to First Response (TTFR)

- Vendor shall provide service desk and incident management services aligned with ITIL best practices and SLAs.
- Definitions:
  - Incident: Unplanned interruption or quality reduction in an IT service.
  - TTFR: Time between ticket creation and first meaningful human response (not automated).
  - Business Hours: Monday–Friday, 8:00 AM to 6:00 PM Atlantic Time.
- Priority Tiers and TTFR Targets
  - P1 – Critical
    - Description: System-wide outage, security breach, or failure of the system with no workaround.
    - TTFR Target: ≤ 15 minutes.
    - Initial Actions: Immediate acknowledgment; engage Incident Manager; notify stakeholders.
  - P2 – High
    - Description: Significant impact to department or large user group; significant degradation; workaround may exist.
    - TTFR Target: ≤ 60 minutes.
    - Initial Actions: Rapid triage; assign to resolver group; confirm user receipt.
  - P3 – Medium
    - Description: Moderate impact; single business unit or non-critical service; workaround available.
    - TTFR Target: ≤ 120 minutes.
    - Initial Actions: Acknowledge, document, plan next steps and estimated time to resolution (ETR).
  - P4 – Low
    - Description: Minor impact; cosmetic issues; single user incidents; no material business effect.
    - TTFR Target: ≤ 8 hours (business hours).

- Initial Actions: Acknowledge, queue for standard support process.

2. Service Availability

- Maintain minimum system uptime of 99%, calculated monthly (excluding scheduled maintenance).
- Use automated monitoring tools for uptime measurement.
- Provide monthly availability reports including:
  - Total downtime
  - Incident summaries
  - Maintenance windows
- Perform all system updates, patches, and maintenance outside standard business hours (Monday–Friday, 8:00 AM to 6:00 PM Atlantic Time), unless otherwise agreed.

3. Service Credits

- The vendor will define **Service Credit Framework** for SLA breaches:
  - Specify thresholds, calculation methods, and liability limits.

4. Data Migration

- Include a **Data Migration Plan** covering:
  - Scope of data
  - Timeline and milestones
  - Validation and reconciliation
  - Security and compliance
  - Contingency plans

5. Change Management

- Vendor shall implement a formal Change Management process to ensure controlled and documented changes to systems, applications, and infrastructure.
- Definitions:
  - Change: Any addition, modification, or removal of an IT service or component that may impact service delivery.
  - Standard Change: Pre-approved, low-risk, routine changes.
  - Emergency Change: High-priority changes required to resolve critical incidents or security vulnerabilities.
  - Business Hours: Monday–Friday, 8:00 AM to 6:00 PM Atlantic Time.

- **Requirements**
    - Approval Workflow: Changes must follow documented approval paths, including business and technical stakeholders.
    - Impact Assessment: Each change must include risk analysis, business impact evaluation, and rollback plan.
    - Scheduling: Non-emergency changes must be scheduled outside standard business hours unless otherwise agreed.
    - Communication: Notify affected stakeholders of planned changes at least 5 business days in advance.
    - Documentation: Maintain detailed records of all changes, including approvals, implementation steps, and outcomes.
    - Post-Implementation Review: Conduct review for all major and emergency changes to validate success and capture lessons learned.

Disaster Recovery & Business Continuity Requirements Checklist

1. Scope

- Vendor shall implement and maintain a **Disaster Recovery (DR) and Business Continuity (BC) plan** to ensure resilience and rapid recovery from major disruptions, aligned with industry best practices and Government of Bermuda's operational requirements.

2. Definitions

- **Disaster Recovery (DR)**: Processes and technologies to restore IT systems and data after a catastrophic event.
- **Business Continuity (BC)**: Strategies to maintain essential business operations during and after a disruption.
- **Business Hours**: Monday–Friday, **8:00 AM to 6:00 PM Atlantic Time**.
- **RTO (Recovery Time Objective)**: Maximum acceptable downtime before significant business impact.
- **RPO (Recovery Point Objective)**: Maximum acceptable data loss, defined as **24 hours**.

3. Requirements

- **Documented DR & BC Plan**: Vendor must provide a comprehensive plan covering:
    - Recovery procedures for critical systems.

    - Roles and responsibilities.
    - Communication protocols.

- **Backup Strategy**:
    - Daily backups for critical systems.
    - Offsite or cloud-based storage for redundancy.

- **Testing & Validation**:
    - Conduct **annual DR/BC tests** and provide results to Government of Bermuda.
    - Validate RTO and RPO compliance during tests.

- **Failover & Redundancy**:
    - Implement failover mechanisms for Tier 1 systems.
    - Ensure alternate site or cloud recovery capability.

- **Incident Escalation**:
    - Define escalation paths for disaster scenarios.
    - Notify Government of Bermuda within **15 minutes** of declaring a disaster event.

- **Compliance & Reporting**:
    - Provide quarterly DR/BC compliance reports.
    - Maintain audit-ready documentation.

6. Disaster Recovery & Business Continuity

- Vendor shall implement and maintain a **Disaster Recovery (DR) and Business Continuity (BC) plan** to ensure resilience and rapid recovery from major disruptions, aligned with industry best practices.

- **Definitions:**
    - **Disaster Recovery (DR)**: Processes and technologies to restore IT systems and data after a catastrophic event.
    - **Business Continuity (BC)**: Strategies to maintain essential business operations during and after a disruption.
    - **Business Hours**: Monday–Friday, **8:00 AM to 6:00 PM Atlantic Time**.
    - **Recovery Time Objective (RTO)**:
        - System must have an **RTO of 24 hours**, meaning the maximum acceptable amount of time in business hours that the system can be down after a failure or disaster before it significantly impacts business operations.

- **Recovery Point Objective (RPO)**:
    - System must have an **RPO of 24 hours**, meaning data loss cannot exceed 24 hours of transactions or changes.
- **Requirements**
- **Documented DR & BC Plan**: Vendor must provide a comprehensive plan covering:
    - Recovery procedures for critical systems.
    - Roles and responsibilities.
    - Communication protocols.
- **Backup Strategy**:
    - Daily backups.
    - Offsite or cloud-based storage for redundancy.
- **Testing & Validation**:
    - Conduct **annual DR/BC tests** and provide results
    - Validate compliance with **RTO (24 hours)** and **RPO (24 hours)** during tests.
- **Compliance & Reporting**:
    - Provide annual DR/BC compliance reports.
    - Maintain audit-ready documentation.

7. Termination & Exit Strategy

- Vendor shall provide a **clear and documented termination and exit process** to ensure smooth transition and protection of Government of Bermuda's data and operations upon contract termination or expiration.
- **Definitions:**
    - **Termination**: The formal ending of the service agreement by either party under to be agreed conditions
    - **Exit Strategy**: The planned process for transferring services, data, and responsibilities back to Government of Bermuda or to a new provider without disruption.

Requirements

- **Data Ownership**:
    - Government of Bermuda retains full ownership of all data throughout the engagement.
    - Vendor must return or securely destroy Government of Bermuda's data upon termination.
- **Data Transfer**:
    - Provide all Government of Bermuda data in agreed format (e.g., CSV, database export) within **30 days** of termination.
    - Ensure secure transfer using encryption and compliance with data protection standards.
- **Knowledge Transfer**:
    - Deliver documentation, configurations, and operational procedures to Government of Bermuda or designated successor.
    - Conduct handover sessions with Government of Bermuda's team.
- **Post-Termination Support**:
    - Offer **30 days** of limited support for transition activities after termination.
- **Compliance & Certification**:
    - Provide written certification of data deletion and compliance with contractual obligations.
- **Exit Plan Documentation**:
    - Vendor must maintain and share an **Exit Plan** detailing timelines, responsibilities, and risk mitigation steps.