Branch Compliance Review Checklist

1. General Compliance Oversight

- Staff have access to updated compliance policies and procedures.
- Staff have signed annual compliance acknowledgments.
- Branch complies with all circulars from head office/BoG directives.
- Evidence of regular compliance training (AML/CFT, KYC, Data Protection, etc.).

2. Anti-Money Laundering (AML)/CFT Compliance

- Know Your Customer (KYC) documentation is complete and current.
- Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) procedures are followed.
- Transaction monitoring and suspicious transaction reporting mechanisms in place.
- Internal STR logs available and escalated cases documented.
- Staff can explain red flags and AML escalation procedures.

3. Customer Onboarding & KYC

- All accounts have completed KYC as per BoG/FIC guidelines.
- Customer identification documents are valid and correctly captured.
- ID verifications done and verification codes captured
- Proof of address and source of funds (where applicable) is verified.
- Customer Risk Rating is applied and documented.
- Dormant/inactive accounts reviewed and reported as required.

4. Internal Controls & Risk Management

- Segregation of duties (e.g., teller, supervisor) is maintained.
- Dual control procedures observed (e.g. vault, branch keys).
- Branch follows internal audit/compliance recommendations.
- Fees and charges complies with approved rates and tarrifs.
- Incidents or breaches are logged and reported.

5. Records & Documentation

- All required records (transactions, KYC, STRs, approvals) are stored securely.
- Files are organized and retrievable (hard copy and/or digital).
- Retention policies are understood and implemented (e.g., 5 years for customers transactions, 5 years at the end of business relationship, …).
- Clean desk policy is observed - Sensitive customer data is not left exposed (e.g., on desks or unlocked drawers).

6. Data Protection & Confidentiality

- Staff understand basic Data Protection obligations.
- Personal data is collected with consent and used appropriately.
- Systems with customer data are password-protected and locked when not in use.
- No unauthorized access to customer data or staff files.
- Disposal of confidential documents follows record management policy (e.g., shredding).

7. Regulatory Reporting

- Branch submits accurate and timely reports to head office for BoG/FIC reporting.
- Adverse media or external issues concerning customers escalated to compliance.
- Regulatory and statutory license and certificate on display where required

8. Complaint Handling & Customer Protection

- Complaints log available and maintained.
- All complaints are acknowledged and resolved in accordance with policy timelines.
- Regulatory disclosures and posters (e.g., Complaints redress channel, AML posters) are visible.
- Products/services are clearly explained to customers.

9. Training & Awareness

- Staff have undergone recent training in compliance topics (record available).
- New hires received onboarding training, including AML and data protection.
- Refresher trainings are tracked and scheduled.

10. Physical & Operational Security

- CCTV cameras functional and recordings retained per policy.
- Cash handling limits and vault controls adhered to.
- Access to sensitive areas (e.g., server room, vault) is restricted.
- Fire extinguishers, first aid kits, and emergency protocols in place.
- Security guards are at post and attendance records captured.