Global Dot Bank

INTERNAL USE ONLY - CONFIDENTIAL

Operational Playbook

Unified Operating Model & Process Standards

CONFIDENTIALITY NOTICE

This document contains proprietary operational procedures and system architecture details. Unauthorized access or distribution is prohibited.

1. Purpose

The Operational Playbook provides a unified operating model across front, middle, and back-office functions. It defines processes that ensure efficiency, resilience, and regulatory integrity in all client interactions and transactions.

2. Core Operational Principles

- **Consistency in Service – Global standards, locally delivered**
- **Zero Operational Risk Tolerance – Preventive controls over detective ones**
- **Client Experience First – Every process is measured by client impact**
- **Operational Resilience – Built-in redundancies and disaster recovery**

3. Process Architecture

Client Onboarding & Verification

Handled via centralized KYC hub with automated identity verification, document scanning, and risk assessment. Average onboarding time: 24-48 hours for standard accounts, 5-7 days for corporate accounts.

Payments & Settlements

24/7 real-time transaction monitoring with dual authorization control. All payments above USD 10,000 require secondary approval. Settlement through SWIFT, SEPA, and proprietary instant payment rails.

Reconciliation & Reporting

Automated ledger matching and daily balance certification. Nostro reconciliation completed by 9 AM daily. Exception reports generated automatically with T+0 resolution target.

Treasury Operations

Liquidity management guided by Basel III ratios. Daily LCR monitoring, weekly stress testing, monthly NSFR reporting to ALCO (Asset Liability Committee).

4. Risk Management

- Operational risk identification via Key Risk Indicators (KRIs)
- Business Continuity Plans tested quarterly
- Incident Response Teams activated within 2 hours of any major disruption
- Root cause analysis mandatory for all incidents with customer impact

5. Technology & Security

- Core banking systems secured with 256-bit encryption and ISO 27001 certification
- Access control managed under Role-Based Access Management (RBAM)
- Cybersecurity Operations Center (CSOC) monitors 24/7 for intrusion detection
- Penetration testing conducted semi-annually by external security firms

6. Business Continuity & Disaster Recovery

- Tier-3 Data Centers across Bangkok, Singapore, and Frankfurt
- Failover protocol within 15 minutes of critical event
- Annual BCP simulation with independent auditor validation
- RTO (Recovery Time Objective): 4 hours for critical systems
- RPO (Recovery Point Objective): 1 hour maximum data loss

7. Performance & Continuous Improvement

Every division measured via KPIs aligned to Operational Excellence Metrics (OEM). Feedback loops ensure process evolution and error reduction. Quarterly Operational Review submitted to the Executive Committee.

Process Change Management

All operational changes require documentation in the Change Control Register, risk assessment, and approval from the Operational Risk Committee before implementation.