Enterprise Risk Management (ERM) Framework

Integrated Risk Governance Structure

CONFIDENTIALITY NOTICE

This document contains sensitive risk management procedures and control mechanisms. Distribution is restricted to Board members, executive leadership, and authorized risk personnel only.

1. Purpose

To establish an integrated risk governance structure ensuring financial stability, operational integrity, and customer trust across all GDB operations.

2. Guiding Principles

- **Accountability: Risk ownership lies with management at all levels**
- **Transparency: Risks are identified, measured, and reported systematically**
- **Resilience: Risk strategy supports long-term sustainability**
- **Compliance: Aligned with Basel III, ISO 31000, and COSO ERM standards**

3. Risk Governance Structure

Committee	Responsibility	Reporting Line
Board Risk & Audit Committee (BRAC)	Oversees all enterprise-level risks, approves policy, reviews reports quarterly	Board of Directors
Chief Risk Officer (CRO)	Leads risk strategy, reporting, and oversight	CEO & BRAC
Enterprise Risk Office (ERO)	Implements the ERM program, maintains risk registers	CRO
Operational Risk Units (ORUs)	Manage line-of-business risk	Division Heads

4. Risk Categories

- **Credit Risk – Counterparty and borrower default exposure**
- **Market Risk – Interest rate, FX, and liquidity volatility**

- **Operational Risk – Process, system, or human errors**
- **Compliance & Legal Risk – Regulatory breaches or litigation**
- **Cyber & Data Risk – Threats to data integrity, privacy, or systems**
- **Reputational Risk – Brand or public confidence erosion**
- **Strategic Risk – Business model and macroeconomic exposure**

5. Risk Identification & Assessment

- Quarterly risk reviews through Key Risk Indicators (KRIs)
- Stress testing and scenario analysis on liquidity and credit portfolios
- Risk self-assessment (RSA) mandated for all department heads
- External risk assessments conducted annually by independent consultants

6. Risk Appetite Framework (RAF)

Defined annually by the Board. Includes quantitative limits (capital adequacy, exposure ratios) and qualitative thresholds (reputation, compliance). Continuous monitoring via centralized dashboard.

7. Risk Mitigation & Control

Three Lines of Defense Model:

- **1st Line: Business units manage risk within defined appetite**
- **2nd Line: Risk and Compliance monitor adherence**
- **3rd Line: Internal Audit independently validates effectiveness**

8. Reporting & Escalation

- Monthly Risk Dashboard reviewed by CRO
- Immediate escalation of red-flag incidents to the BRAC
- Semi-annual independent audit of risk controls
- Annual ERM effectiveness review presented to the Board

Critical Threshold Breach Protocol

Any breach of Board-approved risk appetite limits must be reported to the CRO within 1 hour, BRAC within 4 hours, and full Board within 24 hours. Remediation plan required within 48 hours.