**Compliance Strategy Document**

**1. Regulatory Compliance**

**A. Banking Regulations**

To ensure adherence to financial industry standards, the following regulations will be enforced:

* **Basel III Compliance**
  + Maintain **capital adequacy ratios** (CET1, Tier 1, Total Capital).
  + Implement **liquidity coverage ratio (LCR)** and **net stable funding ratio (NSFR)** requirements.
* **Anti-Money Laundering (AML) Guidelines**
  + **Transaction monitoring** for unusual patterns.
  + **Customer due diligence (CDD)** and **enhanced due diligence (EDD)** for high-risk clients.
  + Compliance with **FATF (Financial Action Task Force)** recommendations.
* **Know Your Customer (KYC) Regulations**
  + **Identity verification** using government-issued IDs and biometric checks.
  + **Ongoing monitoring** of customer transactions for risk assessment.

**B. Data Protection & Privacy Regulations**

To safeguard customer data, the following frameworks will be followed:

* **General Data Protection Regulation (GDPR) – EU**
  + **Right to erasure** and **data portability** for EU citizens.
  + **Data Protection Impact Assessments (DPIAs)** for high-risk processing.
* **California Consumer Privacy Act (CCPA)**
  + **Opt-out mechanisms** for data sharing.
  + **Annual compliance audits** for businesses handling Californian data.
* **Local Banking Regulatory Compliance**
  + Adherence to **national banking laws** (e.g., **Dodd-Frank Act (US), PSD2 (EU), RBI Guidelines (India)**).

**2. Compliance Mechanisms**

**A. Automated Transaction Monitoring**

* **AI-driven anomaly detection** to flag suspicious transactions.
* **Real-time alerts** for potential **fraud, money laundering, or sanctions violations**.

**B. Suspicious Activity Reporting (SAR)**

* **Mandatory filing** of SARs to financial intelligence units (e.g., **FinCEN, FIU-IND**).
* **Whistleblower protection** for employees reporting violations.

**C. Regular Audits**

* **Internal Audits** (Quarterly)
  + Conducted by the **Compliance & Risk Management Team**.
  + Covers **data security, transaction logs, and access controls**.
* **External Audits** (Annual)
  + Performed by **third-party auditors** (e.g., Big 4 firms).
  + Ensures **unbiased regulatory compliance validation**.

**D. Comprehensive Documentation**

* **Policies & Procedures Manual**
  + Clearly defined **AML, KYC, and data protection policies**.
* **Audit Trails & Record Keeping**
  + **5+ years retention** for financial records (as per regulatory requirements).

**3. Compliance Training & Awareness**

* **Quarterly employee training** on **AML, GDPR, and fraud prevention**.
* **Phishing simulations** to reinforce security best practices.

**4. Penalties & Remediation**

* **Non-compliance fines** tracked and reported to regulators.
* **Corrective Action Plans (CAPs)** for any compliance failures.