BFSI Compliance & Regulatory Policy Manual

Banking, Financial Services & Insurance (BFSI)

Version: 3.2

Effective Date: January 2026

Confidential – Internal Use Only

1. Regulatory Framework Overview (Revision Block 1)

This document outlines the regulatory and compliance framework applicable to banking and financial institutions operating under RBI, SEBI, IRDAI, and other governing bodies. The organization shall comply with: • Reserve Bank of India (RBI) Master Directions • Prevention of Money Laundering Act (PMLA) • Basel III Capital Regulations • Information Technology Act, 2000 • Data Protection and Privacy Regulations The Compliance Department is responsible for ensuring regulatory alignment across business functions.

Governance & Oversight: • Chief Compliance Officer (CCO) oversight • Monthly compliance review meetings • Escalation of regulatory breaches within 24 hours • Root cause analysis and corrective action planning Failure to comply with regulatory mandates may result in disciplinary action, regulatory penalties, and reputational damage.

2. Know Your Customer (KYC) Policy (Revision Block 1)

KYC procedures must be completed prior to account activation. Minimum KYC Requirements: • Government-issued ID proof • Address verification • PAN verification • Biometric verification (if applicable) Periodic KYC updates shall be conducted every 2 years for high-risk customers and every 8 years for low-risk customers.

Governance & Oversight: • Chief Compliance Officer (CCO) oversight • Monthly compliance review meetings • Escalation of regulatory breaches within 24 hours • Root cause analysis and corrective action planning Failure to comply with regulatory mandates may result in disciplinary action, regulatory penalties, and reputational damage.

3. Anti-Money Laundering (AML) Framework (Revision Block 1)

The AML framework ensures monitoring and reporting of suspicious activities. Key Controls: • Monitoring transactions above INR 10,00,000 • Automated transaction monitoring systems • Suspicious Transaction Reports (STR) filing within 7 days • Enhanced Due Diligence (EDD) for high-risk customers The Money Laundering Reporting Officer (MLRO) oversees AML operations.

Governance & Oversight: • Chief Compliance Officer (CCO) oversight • Monthly compliance review meetings • Escalation of regulatory breaches within 24 hours • Root cause analysis and corrective action planning Failure to comply with regulatory mandates may result in disciplinary action, regulatory penalties, and reputational damage.

4. Risk Management Framework (Revision Block 1)

Risk categories include: • Credit Risk • Market Risk • Operational Risk • Liquidity Risk • Compliance Risk A Risk Appetite Statement (RAS) shall be approved by the Board annually.

Governance & Oversight: • Chief Compliance Officer (CCO) oversight • Monthly compliance review meetings • Escalation of regulatory breaches within 24 hours • Root cause analysis and corrective action planning Failure to comply with regulatory mandates may result in disciplinary action, regulatory penalties, and reputational damage.

5. Information Security & Cyber Governance (Revision Block 1)

The institution shall implement ISO 27001 aligned controls. Controls include: • Multi-factor authentication • Encryption of customer data • Role-based access controls (RBAC) • Security incident monitoring Quarterly vulnerability assessments and annual penetration testing are mandatory.

Governance & Oversight: • Chief Compliance Officer (CCO) oversight • Monthly compliance review meetings • Escalation of regulatory breaches within 24 hours • Root cause analysis and corrective action planning Failure to comply with regulatory mandates may result in disciplinary action, regulatory penalties, and reputational damage.

6. Transaction Monitoring & STR Reporting (Revision Block 1)

Automated systems must flag: • Structuring transactions • Rapid fund transfers • Cross-border high-value transfers STRs must be filed with FIU-IND within regulatory timelines.

Governance & Oversight: • Chief Compliance Officer (CCO) oversight • Monthly compliance review meetings • Escalation of regulatory breaches within 24 hours • Root cause analysis and corrective action planning Failure to comply with regulatory mandates may result in disciplinary action, regulatory penalties, and reputational damage.

7. Record Retention Policy (Revision Block 1)

Transaction records must be retained for a minimum of 10 years. KYC records must be preserved for 5 years post account closure. Audit logs must be maintained securely and tamper-proof.

Governance & Oversight: • Chief Compliance Officer (CCO) oversight • Monthly compliance review meetings • Escalation of regulatory breaches within 24 hours • Root cause analysis and corrective action planning Failure to comply with regulatory mandates may result in disciplinary action, regulatory penalties, and reputational damage.

8. Compliance Monitoring & Internal Audit (Revision Block 1)

The Compliance function shall perform quarterly reviews. Internal Audit shall conduct independent assessments annually. Board-level reporting must include compliance breaches and corrective actions.

Governance & Oversight: • Chief Compliance Officer (CCO) oversight • Monthly compliance review meetings • Escalation of regulatory breaches within 24 hours • Root cause analysis and corrective action planning Failure to comply with regulatory mandates may result in disciplinary action, regulatory penalties, and reputational damage.

9. AI & Model Risk Governance (Revision Block 1)

AI-based decision systems must: • Undergo validation before deployment • Maintain explainability documentation • Avoid bias in credit scoring models • Be reviewed periodically for drift Model governance committee oversight is mandatory.

Governance & Oversight: • Chief Compliance Officer (CCO) oversight • Monthly compliance review meetings • Escalation of regulatory breaches within 24 hours • Root cause analysis and corrective action planning Failure to comply with regulatory mandates may result in disciplinary action, regulatory penalties, and reputational damage.

10. Business Continuity & Disaster Recovery (Revision Block 1)

BCP and DR plans must ensure: • RTO < 4 hours • RPO < 30 minutes • Alternate data center readiness • Annual DR drills Incident escalation matrix must be documented.

Governance & Oversight: • Chief Compliance Officer (CCO) oversight • Monthly compliance review meetings • Escalation of regulatory breaches within 24 hours • Root cause analysis and corrective action planning Failure to comply with regulatory mandates may result in disciplinary action, regulatory penalties, and reputational damage.

1. Regulatory Framework Overview (Revision Block 2)

This document outlines the regulatory and compliance framework applicable to banking and financial institutions operating under RBI, SEBI, IRDAI, and other governing bodies. The organization shall comply with: • Reserve Bank of India (RBI) Master Directions • Prevention of Money Laundering Act (PMLA) • Basel III Capital Regulations • Information Technology Act, 2000 • Data Protection and Privacy Regulations The Compliance Department is responsible for ensuring regulatory alignment across business functions.

Governance & Oversight: • Chief Compliance Officer (CCO) oversight • Monthly compliance review meetings • Escalation of regulatory breaches within 24 hours • Root cause analysis and corrective action planning Failure to comply with regulatory mandates may result in disciplinary action, regulatory penalties, and reputational damage.

2. Know Your Customer (KYC) Policy (Revision Block 2)

KYC procedures must be completed prior to account activation. Minimum KYC Requirements: • Government-issued ID proof • Address verification • PAN verification • Biometric verification (if applicable) Periodic KYC updates shall be conducted every 2 years for high-risk customers and every 8 years for low-risk customers.

Governance & Oversight: • Chief Compliance Officer (CCO) oversight • Monthly compliance review meetings • Escalation of regulatory breaches within 24 hours • Root cause analysis and corrective action planning Failure to comply with regulatory mandates may result in disciplinary action, regulatory penalties, and reputational damage.

3. Anti-Money Laundering (AML) Framework (Revision Block 2)

The AML framework ensures monitoring and reporting of suspicious activities. Key Controls: • Monitoring transactions above INR 10,00,000 • Automated transaction monitoring systems •

Suspicious Transaction Reports (STR) filing within 7 days • Enhanced Due Diligence (EDD) for high-risk customers The Money Laundering Reporting Officer (MLRO) oversees AML operations.

Governance & Oversight: • Chief Compliance Officer (CCO) oversight • Monthly compliance review meetings • Escalation of regulatory breaches within 24 hours • Root cause analysis and corrective action planning Failure to comply with regulatory mandates may result in disciplinary action, regulatory penalties, and reputational damage.

4. Risk Management Framework (Revision Block 2)

Risk categories include: • Credit Risk • Market Risk • Operational Risk • Liquidity Risk • Compliance Risk A Risk Appetite Statement (RAS) shall be approved by the Board annually.

Governance & Oversight: • Chief Compliance Officer (CCO) oversight • Monthly compliance review meetings • Escalation of regulatory breaches within 24 hours • Root cause analysis and corrective action planning Failure to comply with regulatory mandates may result in disciplinary action, regulatory penalties, and reputational damage.

5. Information Security & Cyber Governance (Revision Block 2)

The institution shall implement ISO 27001 aligned controls. Controls include: • Multi-factor authentication • Encryption of customer data • Role-based access controls (RBAC) • Security incident monitoring Quarterly vulnerability assessments and annual penetration testing are mandatory.

Governance & Oversight: • Chief Compliance Officer (CCO) oversight • Monthly compliance review meetings • Escalation of regulatory breaches within 24 hours • Root cause analysis and corrective action planning Failure to comply with regulatory mandates may result in disciplinary action, regulatory penalties, and reputational damage.

6. Transaction Monitoring & STR Reporting (Revision Block 2)

Automated systems must flag: • Structuring transactions • Rapid fund transfers • Cross-border high-value transfers STRs must be filed with FIU-IND within regulatory timelines.

Governance & Oversight: • Chief Compliance Officer (CCO) oversight • Monthly compliance review meetings • Escalation of regulatory breaches within 24 hours • Root cause analysis and corrective action planning Failure to comply with regulatory mandates may result in disciplinary action, regulatory penalties, and reputational damage.

7. Record Retention Policy (Revision Block 2)

Transaction records must be retained for a minimum of 10 years. KYC records must be preserved for 5 years post account closure. Audit logs must be maintained securely and tamper-proof.

Governance & Oversight: • Chief Compliance Officer (CCO) oversight • Monthly compliance review meetings • Escalation of regulatory breaches within 24 hours • Root cause analysis and corrective action planning Failure to comply with regulatory mandates may result in disciplinary action, regulatory penalties, and reputational damage.

8. Compliance Monitoring & Internal Audit (Revision Block 2)

The Compliance function shall perform quarterly reviews. Internal Audit shall conduct independent assessments annually. Board-level reporting must include compliance breaches and corrective actions.

Governance & Oversight: • Chief Compliance Officer (CCO) oversight • Monthly compliance review meetings • Escalation of regulatory breaches within 24 hours • Root cause analysis and corrective action planning Failure to comply with regulatory mandates may result in disciplinary action, regulatory penalties, and reputational damage.

9. AI & Model Risk Governance (Revision Block 2)

AI-based decision systems must: • Undergo validation before deployment • Maintain explainability documentation • Avoid bias in credit scoring models • Be reviewed periodically for drift Model governance committee oversight is mandatory.

Governance & Oversight: • Chief Compliance Officer (CCO) oversight • Monthly compliance review meetings • Escalation of regulatory breaches within 24 hours • Root cause analysis and corrective action planning Failure to comply with regulatory mandates may result in disciplinary action, regulatory penalties, and reputational damage.

10. Business Continuity & Disaster Recovery (Revision Block 2)

BCP and DR plans must ensure: • RTO < 4 hours • RPO < 30 minutes • Alternate data center readiness • Annual DR drills Incident escalation matrix must be documented.

Governance & Oversight: • Chief Compliance Officer (CCO) oversight • Monthly compliance review meetings • Escalation of regulatory breaches within 24 hours • Root cause analysis and corrective action planning Failure to comply with regulatory mandates may result in disciplinary action, regulatory penalties, and reputational damage.

1. Regulatory Framework Overview (Revision Block 3)

This document outlines the regulatory and compliance framework applicable to banking and financial institutions operating under RBI, SEBI, IRDAI, and other governing bodies. The organization shall comply with: • Reserve Bank of India (RBI) Master Directions • Prevention of Money Laundering Act (PMLA) • Basel III Capital Regulations • Information Technology Act, 2000 • Data Protection and Privacy Regulations The Compliance Department is responsible for ensuring regulatory alignment across business functions.

Governance & Oversight: • Chief Compliance Officer (CCO) oversight • Monthly compliance review meetings • Escalation of regulatory breaches within 24 hours • Root cause analysis and corrective action planning Failure to comply with regulatory mandates may result in disciplinary action, regulatory penalties, and reputational damage.

2. Know Your Customer (KYC) Policy (Revision Block 3)

KYC procedures must be completed prior to account activation. Minimum KYC Requirements: • Government-issued ID proof • Address verification • PAN verification • Biometric verification (if applicable) Periodic KYC updates shall be conducted every 2 years for high-risk customers and every 8 years for low-risk customers.

Governance & Oversight: • Chief Compliance Officer (CCO) oversight • Monthly compliance review meetings • Escalation of regulatory breaches within 24 hours • Root cause analysis and corrective action planning Failure to comply with regulatory mandates may result in disciplinary action, regulatory penalties, and reputational damage.

3. Anti-Money Laundering (AML) Framework (Revision Block 3)

The AML framework ensures monitoring and reporting of suspicious activities. Key Controls: • Monitoring transactions above INR 10,00,000 • Automated transaction monitoring systems • Suspicious Transaction Reports (STR) filing within 7 days • Enhanced Due Diligence (EDD) for high-risk customers The Money Laundering Reporting Officer (MLRO) oversees AML operations.

Governance & Oversight: • Chief Compliance Officer (CCO) oversight • Monthly compliance review meetings • Escalation of regulatory breaches within 24 hours • Root cause analysis and corrective action planning Failure to comply with regulatory mandates may result in disciplinary action, regulatory penalties, and reputational damage.

4. Risk Management Framework (Revision Block 3)

Risk categories include: • Credit Risk • Market Risk • Operational Risk • Liquidity Risk • Compliance Risk A Risk Appetite Statement (RAS) shall be approved by the Board annually.

Governance & Oversight: • Chief Compliance Officer (CCO) oversight • Monthly compliance review meetings • Escalation of regulatory breaches within 24 hours • Root cause analysis and corrective action planning Failure to comply with regulatory mandates may result in disciplinary action, regulatory penalties, and reputational damage.

5. Information Security & Cyber Governance (Revision Block 3)

The institution shall implement ISO 27001 aligned controls. Controls include: • Multi-factor authentication • Encryption of customer data • Role-based access controls (RBAC) • Security incident monitoring Quarterly vulnerability assessments and annual penetration testing are mandatory.

Governance & Oversight: • Chief Compliance Officer (CCO) oversight • Monthly compliance review meetings • Escalation of regulatory breaches within 24 hours • Root cause analysis and corrective action planning Failure to comply with regulatory mandates may result in disciplinary action, regulatory penalties, and reputational damage.

6. Transaction Monitoring & STR Reporting (Revision Block 3)

Automated systems must flag: • Structuring transactions • Rapid fund transfers • Cross-border high-value transfers STRs must be filed with FIU-IND within regulatory timelines.

Governance & Oversight: • Chief Compliance Officer (CCO) oversight • Monthly compliance review meetings • Escalation of regulatory breaches within 24 hours • Root cause analysis and corrective action planning Failure to comply with regulatory mandates may result in disciplinary action, regulatory penalties, and reputational damage.

7. Record Retention Policy (Revision Block 3)

Transaction records must be retained for a minimum of 10 years. KYC records must be preserved for 5 years post account closure. Audit logs must be maintained securely and tamper-proof.

Governance & Oversight: • Chief Compliance Officer (CCO) oversight • Monthly compliance review meetings • Escalation of regulatory breaches within 24 hours • Root cause analysis and corrective action planning Failure to comply with regulatory mandates may result in disciplinary action, regulatory penalties, and reputational damage.

8. Compliance Monitoring & Internal Audit (Revision Block 3)

The Compliance function shall perform quarterly reviews. Internal Audit shall conduct independent assessments annually. Board-level reporting must include compliance breaches and corrective actions.

Governance & Oversight: • Chief Compliance Officer (CCO) oversight • Monthly compliance review meetings • Escalation of regulatory breaches within 24 hours • Root cause analysis and corrective action planning Failure to comply with regulatory mandates may result in disciplinary action, regulatory penalties, and reputational damage.

9. AI & Model Risk Governance (Revision Block 3)

AI-based decision systems must: • Undergo validation before deployment • Maintain explainability documentation • Avoid bias in credit scoring models • Be reviewed periodically for drift Model governance committee oversight is mandatory.

Governance & Oversight: • Chief Compliance Officer (CCO) oversight • Monthly compliance review meetings • Escalation of regulatory breaches within 24 hours • Root cause analysis and corrective action planning Failure to comply with regulatory mandates may result in disciplinary action, regulatory penalties, and reputational damage.

10. Business Continuity & Disaster Recovery (Revision Block 3)

BCP and DR plans must ensure: • RTO < 4 hours • RPO < 30 minutes • Alternate data center readiness • Annual DR drills Incident escalation matrix must be documented.

Governance & Oversight: • Chief Compliance Officer (CCO) oversight • Monthly compliance review meetings • Escalation of regulatory breaches within 24 hours • Root cause analysis and corrective

action planning Failure to comply with regulatory mandates may result in disciplinary action, regulatory penalties, and reputational damage.

1. Regulatory Framework Overview (Revision Block 4)

This document outlines the regulatory and compliance framework applicable to banking and financial institutions operating under RBI, SEBI, IRDAI, and other governing bodies. The organization shall comply with: • Reserve Bank of India (RBI) Master Directions • Prevention of Money Laundering Act (PMLA) • Basel III Capital Regulations • Information Technology Act, 2000 • Data Protection and Privacy Regulations The Compliance Department is responsible for ensuring regulatory alignment across business functions.

Governance & Oversight: • Chief Compliance Officer (CCO) oversight • Monthly compliance review meetings • Escalation of regulatory breaches within 24 hours • Root cause analysis and corrective action planning Failure to comply with regulatory mandates may result in disciplinary action, regulatory penalties, and reputational damage.

2. Know Your Customer (KYC) Policy (Revision Block 4)

KYC procedures must be completed prior to account activation. Minimum KYC Requirements: • Government-issued ID proof • Address verification • PAN verification • Biometric verification (if applicable) Periodic KYC updates shall be conducted every 2 years for high-risk customers and every 8 years for low-risk customers.

Governance & Oversight: • Chief Compliance Officer (CCO) oversight • Monthly compliance review meetings • Escalation of regulatory breaches within 24 hours • Root cause analysis and corrective action planning Failure to comply with regulatory mandates may result in disciplinary action, regulatory penalties, and reputational damage.

3. Anti-Money Laundering (AML) Framework (Revision Block 4)

The AML framework ensures monitoring and reporting of suspicious activities. Key Controls: • Monitoring transactions above INR 10,00,000 • Automated transaction monitoring systems • Suspicious Transaction Reports (STR) filing within 7 days • Enhanced Due Diligence (EDD) for high-risk customers The Money Laundering Reporting Officer (MLRO) oversees AML operations.

Governance & Oversight: • Chief Compliance Officer (CCO) oversight • Monthly compliance review meetings • Escalation of regulatory breaches within 24 hours • Root cause analysis and corrective action planning Failure to comply with regulatory mandates may result in disciplinary action, regulatory penalties, and reputational damage.

4. Risk Management Framework (Revision Block 4)

Risk categories include: • Credit Risk • Market Risk • Operational Risk • Liquidity Risk • Compliance Risk A Risk Appetite Statement (RAS) shall be approved by the Board annually.

Governance & Oversight: • Chief Compliance Officer (CCO) oversight • Monthly compliance review meetings • Escalation of regulatory breaches within 24 hours • Root cause analysis and corrective action planning Failure to comply with regulatory mandates may result in disciplinary action, regulatory penalties, and reputational damage.

5. Information Security & Cyber Governance (Revision Block 4)

The institution shall implement ISO 27001 aligned controls. Controls include: • Multi-factor authentication • Encryption of customer data • Role-based access controls (RBAC) • Security incident monitoring Quarterly vulnerability assessments and annual penetration testing are mandatory.

Governance & Oversight: • Chief Compliance Officer (CCO) oversight • Monthly compliance review meetings • Escalation of regulatory breaches within 24 hours • Root cause analysis and corrective action planning Failure to comply with regulatory mandates may result in disciplinary action, regulatory penalties, and reputational damage.

6. Transaction Monitoring & STR Reporting (Revision Block 4)

Automated systems must flag: • Structuring transactions • Rapid fund transfers • Cross-border high-value transfers STRs must be filed with FIU-IND within regulatory timelines.

Governance & Oversight: • Chief Compliance Officer (CCO) oversight • Monthly compliance review meetings • Escalation of regulatory breaches within 24 hours • Root cause analysis and corrective action planning Failure to comply with regulatory mandates may result in disciplinary action, regulatory penalties, and reputational damage.

7. Record Retention Policy (Revision Block 4)

Transaction records must be retained for a minimum of 10 years. KYC records must be preserved for 5 years post account closure. Audit logs must be maintained securely and tamper-proof.

Governance & Oversight: • Chief Compliance Officer (CCO) oversight • Monthly compliance review meetings • Escalation of regulatory breaches within 24 hours • Root cause analysis and corrective action planning Failure to comply with regulatory mandates may result in disciplinary action, regulatory penalties, and reputational damage.

8. Compliance Monitoring & Internal Audit (Revision Block 4)

The Compliance function shall perform quarterly reviews. Internal Audit shall conduct independent assessments annually. Board-level reporting must include compliance breaches and corrective actions.

Governance & Oversight: • Chief Compliance Officer (CCO) oversight • Monthly compliance review meetings • Escalation of regulatory breaches within 24 hours • Root cause analysis and corrective action planning Failure to comply with regulatory mandates may result in disciplinary action, regulatory penalties, and reputational damage.

9. AI & Model Risk Governance (Revision Block 4)

AI-based decision systems must: • Undergo validation before deployment • Maintain explainability documentation • Avoid bias in credit scoring models • Be reviewed periodically for drift Model governance committee oversight is mandatory.

Governance & Oversight: • Chief Compliance Officer (CCO) oversight • Monthly compliance review meetings • Escalation of regulatory breaches within 24 hours • Root cause analysis and corrective action planning Failure to comply with regulatory mandates may result in disciplinary action, regulatory penalties, and reputational damage.

10. Business Continuity & Disaster Recovery (Revision Block 4)

BCP and DR plans must ensure: • RTO < 4 hours • RPO < 30 minutes • Alternate data center readiness • Annual DR drills Incident escalation matrix must be documented.

Governance & Oversight: • Chief Compliance Officer (CCO) oversight • Monthly compliance review meetings • Escalation of regulatory breaches within 24 hours • Root cause analysis and corrective action planning Failure to comply with regulatory mandates may result in disciplinary action, regulatory penalties, and reputational damage.

1. Regulatory Framework Overview (Revision Block 5)

This document outlines the regulatory and compliance framework applicable to banking and financial institutions operating under RBI, SEBI, IRDAI, and other governing bodies. The organization shall comply with: • Reserve Bank of India (RBI) Master Directions • Prevention of Money Laundering Act (PMLA) • Basel III Capital Regulations • Information Technology Act, 2000 • Data Protection and Privacy Regulations The Compliance Department is responsible for ensuring regulatory alignment across business functions.

Governance & Oversight: • Chief Compliance Officer (CCO) oversight • Monthly compliance review meetings • Escalation of regulatory breaches within 24 hours • Root cause analysis and corrective action planning Failure to comply with regulatory mandates may result in disciplinary action, regulatory penalties, and reputational damage.

2. Know Your Customer (KYC) Policy (Revision Block 5)

KYC procedures must be completed prior to account activation. Minimum KYC Requirements: • Government-issued ID proof • Address verification • PAN verification • Biometric verification (if applicable) Periodic KYC updates shall be conducted every 2 years for high-risk customers and every 8 years for low-risk customers.

Governance & Oversight: • Chief Compliance Officer (CCO) oversight • Monthly compliance review meetings • Escalation of regulatory breaches within 24 hours • Root cause analysis and corrective action planning Failure to comply with regulatory mandates may result in disciplinary action, regulatory penalties, and reputational damage.

3. Anti-Money Laundering (AML) Framework (Revision Block 5)

The AML framework ensures monitoring and reporting of suspicious activities. Key Controls: • Monitoring transactions above INR 10,00,000 • Automated transaction monitoring systems • Suspicious Transaction Reports (STR) filing within 7 days • Enhanced Due Diligence (EDD) for high-risk customers The Money Laundering Reporting Officer (MLRO) oversees AML operations.

Governance & Oversight: • Chief Compliance Officer (CCO) oversight • Monthly compliance review meetings • Escalation of regulatory breaches within 24 hours • Root cause analysis and corrective action planning Failure to comply with regulatory mandates may result in disciplinary action, regulatory penalties, and reputational damage.

4. Risk Management Framework (Revision Block 5)

Risk categories include: • Credit Risk • Market Risk • Operational Risk • Liquidity Risk • Compliance Risk A Risk Appetite Statement (RAS) shall be approved by the Board annually.

Governance & Oversight: • Chief Compliance Officer (CCO) oversight • Monthly compliance review meetings • Escalation of regulatory breaches within 24 hours • Root cause analysis and corrective action planning Failure to comply with regulatory mandates may result in disciplinary action, regulatory penalties, and reputational damage.

5. Information Security & Cyber Governance (Revision Block 5)

The institution shall implement ISO 27001 aligned controls. Controls include: • Multi-factor authentication • Encryption of customer data • Role-based access controls (RBAC) • Security incident monitoring Quarterly vulnerability assessments and annual penetration testing are mandatory.

Governance & Oversight: • Chief Compliance Officer (CCO) oversight • Monthly compliance review meetings • Escalation of regulatory breaches within 24 hours • Root cause analysis and corrective action planning Failure to comply with regulatory mandates may result in disciplinary action, regulatory penalties, and reputational damage.

6. Transaction Monitoring & STR Reporting (Revision Block 5)

Automated systems must flag: • Structuring transactions • Rapid fund transfers • Cross-border high-value transfers STRs must be filed with FIU-IND within regulatory timelines.

Governance & Oversight: • Chief Compliance Officer (CCO) oversight • Monthly compliance review meetings • Escalation of regulatory breaches within 24 hours • Root cause analysis and corrective action planning Failure to comply with regulatory mandates may result in disciplinary action, regulatory penalties, and reputational damage.

7. Record Retention Policy (Revision Block 5)

Transaction records must be retained for a minimum of 10 years. KYC records must be preserved for 5 years post account closure. Audit logs must be maintained securely and tamper-proof.

Governance & Oversight: • Chief Compliance Officer (CCO) oversight • Monthly compliance review meetings • Escalation of regulatory breaches within 24 hours • Root cause analysis and corrective action planning Failure to comply with regulatory mandates may result in disciplinary action, regulatory penalties, and reputational damage.

8. Compliance Monitoring & Internal Audit (Revision Block 5)

The Compliance function shall perform quarterly reviews. Internal Audit shall conduct independent assessments annually. Board-level reporting must include compliance breaches and corrective actions.

Governance & Oversight: • Chief Compliance Officer (CCO) oversight • Monthly compliance review meetings • Escalation of regulatory breaches within 24 hours • Root cause analysis and corrective action planning Failure to comply with regulatory mandates may result in disciplinary action, regulatory penalties, and reputational damage.

9. AI & Model Risk Governance (Revision Block 5)

AI-based decision systems must: • Undergo validation before deployment • Maintain explainability documentation • Avoid bias in credit scoring models • Be reviewed periodically for drift Model governance committee oversight is mandatory.

Governance & Oversight: • Chief Compliance Officer (CCO) oversight • Monthly compliance review meetings • Escalation of regulatory breaches within 24 hours • Root cause analysis and corrective action planning Failure to comply with regulatory mandates may result in disciplinary action, regulatory penalties, and reputational damage.

10. Business Continuity & Disaster Recovery (Revision Block 5)

BCP and DR plans must ensure: • RTO < 4 hours • RPO < 30 minutes • Alternate data center readiness • Annual DR drills Incident escalation matrix must be documented.

Governance & Oversight: • Chief Compliance Officer (CCO) oversight • Monthly compliance review meetings • Escalation of regulatory breaches within 24 hours • Root cause analysis and corrective action planning Failure to comply with regulatory mandates may result in disciplinary action, regulatory penalties, and reputational damage.