# RBEYOND

**Internal Control Documentation**  
**Document Version:** 1.0  
**Effective Date:** July 3, 2025  
**Prepared By:** Internal Audit & Risk Management Department  
**Reviewed By:** Compliance & Regulatory Affairs Division

## 1. Introduction & Purpose

### 1.1 Overview

This document serves as the **Internal Control Framework** for RBEYOND, a financial entity operating across key verticals including retail banking, digital lending, and financial technology services. It has been prepared to systematically define, document, and track critical controls implemented across core operational, financial, IT, and compliance processes.

The purpose of this document is to provide a **centralized reference point** for internal and external stakeholders—such as auditors, regulatory bodies, management, and risk owners—ensuring that all significant risks are adequately mitigated through effective and well-designed internal controls.

This control documentation supports RBEYOND’s commitment to **transparency, accountability, and regulatory compliance**, ensuring that its control environment is robust, traceable, and continuously improved.

### 1.2 Objectives

The core objectives of this control document are to:

* Establish a formal inventory of controls mapped to business processes and risks.
* Ensure compliance with applicable **regulatory and statutory frameworks** (national and international).
* Prevent, detect, and respond to instances of **fraud, policy violations, and data breaches**.
* Facilitate **risk mitigation** through clearly defined control mechanisms.
* Enhance the organization's ability to **withstand audits**, due diligence, and supervisory reviews.
* Promote **control ownership** and accountability across functions and verticals.
* Support the **design and testing** of controls for operational effectiveness and internal audits.

### 1.3 Scope

This control document applies to all relevant business units, processes, and IT systems across RBEYOND’s organizational structure, including but not limited to:

* **Departments Covered:**
  + Retail Banking Operations
  + Compliance & Legal
  + Risk Management
  + Information Technology & Cybersecurity
  + Finance & Treasury
  + Product & Digital Innovation
* **Processes Covered:**
  + Customer onboarding and KYC
  + Loan origination and approval
  + Transaction monitoring and fraud detection
  + Regulatory reporting
  + Access control and privilege management
  + Data governance and backup
* **Systems Covered:**
  + Core banking system (CBS)
  + Document management systems
  + AML/CFT screening tools
  + CRM and ERP platforms
  + Regulatory reporting engines
  + Internal audit and risk platforms

### 1.4 Regulatory Framework Alignment

This document is aligned with the control and compliance expectations laid out under the following key regulatory and legal frameworks:

* **SOX (Sarbanes-Oxley Act)** – Internal financial controls and auditability.
* **Basel III** – Operational risk management, capital adequacy, and stress testing.
* **GDPR** – Protection of personal data of EU-based customers.
* **IFRS (International Financial Reporting Standards)** – Financial reporting integrity.
* **RBI Guidelines (India)** – IT Framework for NBFCs, Master Directions on KYC, and Cybersecurity Controls.
* **Federal Reserve & OCC Guidelines (USA)** – Enterprise risk, IT risk, and model risk management.
* **DPDP Act (India)** – Data protection and lawful processing of digital personal data.

These frameworks provide the foundation against which all defined controls are benchmarked for design adequacy and operating effectiveness.

## 2. Entity Overview

### 2.1 Organizational Structure

RBEYOND is a diversified financial services organization operating across retail banking, lending, digital financial platforms, and investment services. The company operates in a matrix structure combining centralized governance with decentralized business unit autonomy to enhance risk management, regulatory compliance, and operational efficiency.

The organizational hierarchy consists of the following core business and support units:

**Business Units:**

* Retail & SME Lending Division
* Digital Payments & Wallet Services
* Investment & Wealth Management
* Treasury & ALM (Asset-Liability Management)
* Corporate Finance & Strategic Partnerships

**Support & Oversight Functions:**

* Risk Management
* Compliance & Regulatory Affairs
* Internal Audit
* Legal & Corporate Governance
* Information Technology & Security
* Finance & Accounting
* Human Resources

A structured governance model ensures that decision-making, reporting, and escalations flow efficiently through all levels—from business units up to board committees.

### 2.2 Key Roles & Responsibilities

To ensure effective control implementation, RBEYOND clearly defines ownership and accountability across strategic, tactical, and operational levels:

| **Role** | **Responsibility** |
| --- | --- |
| **Board of Directors** | Oversight of internal control system, approving risk appetite, and strategic governance. |
| **Audit Committee** | Reviews internal control adequacy, audit findings, and management responses. |
| **Risk Management Committee (RMC)** | Oversees risk identification, measurement, mitigation strategies, and control performance across the enterprise. |
| **Chief Risk Officer (CRO)** | Leads the enterprise risk management (ERM) function, ensures proper risk-control alignment, and monitors high-impact control failures. |
| **Chief Compliance Officer (CCO)** | Ensures compliance with laws and regulations; leads the control mapping to external regulatory requirements. |
| **Chief Financial Officer (CFO)** | Oversees financial controls, reporting integrity, and compliance with accounting standards (e.g., IFRS). |
| **Chief Information Security Officer (CISO)** | Owns the IT control framework, data protection, and cybersecurity architecture. |
| **Head of Internal Audit** | Independently evaluates the design and operating effectiveness of internal controls and reports to the Audit Committee. |
| **Control Owners (Process Heads/Managers)** | Execute controls in their respective domains and maintain evidence for monitoring and testing. |
| **First Line of Defense (Business Units)** | Responsible for executing day-to-day operations within the risk-control boundaries defined by corporate policy. |

Each role is assigned with a control ownership model based on the **Three Lines of Defense Framework**, ensuring robust segregation of duties and effective internal control governance.

### 2.3 Business Processes

RBEYOND’s operations are structured around a wide range of financial and support processes. Controls are mapped to these processes to ensure transparency, compliance, fraud prevention, and risk mitigation:

| **Business Domain** | **Core Processes** |
| --- | --- |
| **Lending Operations** | Customer onboarding, KYC/AML validation, credit appraisal, underwriting, loan disbursal, collection & recovery. |
| **Investment & Wealth Management** | Portfolio management, investor profiling, risk-based advisory, compliance with suitability norms. |
| **Payments & Digital Transactions** | Payment gateway integration, digital wallet KYC, transaction screening, chargeback handling, settlement and reconciliation. |
| **Treasury & ALM** | Cash flow monitoring, liquidity risk controls, FX exposure management, investment decisions, capital adequacy. |
| **Customer Operations** | Dispute resolution, service quality monitoring, contact center governance, customer consent & data rights. |
| **IT & Cybersecurity** | Access controls, system monitoring, data classification, vulnerability management, backup and disaster recovery. |
| **Regulatory Reporting** | Regulatory returns (RBI, SEBI, etc.), supervisory disclosures, XBRL filings, control attestation and audit trail submission. |
| **Financial Management** | General ledger, budgeting and forecasting, financial consolidation, intercompany transactions, IFRS alignment. |

These processes are subject to **risk-based control testing** and ongoing improvements through audit observations, regulatory feedback, and operational learnings.

## 3. Risk Assessment & Control Environment

### 3.1 Identified Risk Categories

RBEYOND operates within a dynamic financial environment that exposes it to a wide array of risks. As part of its **Enterprise Risk Management (ERM)** program, the following key risk categories have been identified and assessed for materiality, likelihood, and impact:

| **Risk Category** | **Description** | **Typical Impact Areas** |
| --- | --- | --- |
| **Credit Risk** | Possibility of financial loss due to a borrower’s failure to repay a loan or meet contractual obligations. | Loan portfolio quality, provisioning, capital adequacy. |
| **Market Risk** | Exposure to changes in market variables such as interest rates, exchange rates, or equity prices. | Treasury operations, asset valuation, trading book. |
| **Operational Risk** | Risk of loss resulting from failed internal processes, systems, human error, or external events. | Process failures, reconciliation errors, business continuity. |
| **Liquidity Risk** | Inability to meet short-term financial obligations due to inadequate cash flow or funding. | Payment processing, redemptions, settlement cycles. |
| **Fraud Risk** | Internal or external attempts to circumvent systems for financial gain, including collusion, identity theft, and transaction manipulation. | Transaction integrity, brand risk, financial loss. |
| **Cyber Risk** | Threats to data confidentiality, system availability, and information integrity due to cyberattacks or IT vulnerabilities. | Data breaches, ransomware, regulatory sanctions. |
| **Compliance & Regulatory Risk** | Risk of legal or regulatory sanctions due to non-compliance with laws, regulations, or internal policies. | License impact, monetary penalties, supervisory scrutiny. |

Each risk is linked to specific controls which are classified by type (preventive, detective, corrective) and mapped to processes within the control inventory.

### 3.2 Risk Appetite & Tolerance Levels

RBEYOND’s **Board of Directors**, in consultation with the **Risk Management Committee (RMC)**, defines the institution’s **Risk Appetite Statement (RAS)** annually. This statement outlines the maximum level of risk the company is willing to accept across key categories, supported by thresholds and triggers for action.

| **Risk Category** | **Appetite Level** | **Tolerance Threshold** |
| --- | --- | --- |
| Credit Risk | Moderate | Gross NPA ratio < 3.5% |
| Market Risk | Low | VaR < 1.5% of capital for trading book |
| Operational Risk | Low | Zero tolerance for system-wide outages or regulatory breaches |
| Liquidity Risk | Low | LCR > 110%, NSFR > 105% |
| Fraud Risk | Very Low | Fraud-to-Transaction ratio < 0.05% |
| Cyber Risk | Very Low | Zero tolerance for data loss, >99.9% system uptime |
| Compliance Risk | Zero Tolerance | All critical controls must be fully effective (100% compliance rating) |

These thresholds guide management responses, control intensification, and incident escalation. Breaches of risk tolerance require documented root cause analysis and board-level reporting.

### 3.3 Control Frameworks Adopted

To ensure its internal control system is aligned with global best practices, RBEYOND adheres to the following **industry-standard control frameworks** across its operations:

| **Framework** | **Domain** | **Purpose of Adoption** |
| --- | --- | --- |
| **COSO – Internal Control – Integrated Framework** | Enterprise-wide risk & control design | Provides a principles-based approach to define, assess, and monitor internal controls aligned with objectives across operations, reporting, and compliance. |
| **COBIT (Control Objectives for Information and Related Technologies)** | IT governance, information systems, and process controls | Helps manage IT-related risks, ensures alignment between IT and business goals, and establishes effective control over digital platforms. |
| **ISO/IEC 27001:2022** | Information security & data governance | Ensures implementation of an Information Security Management System (ISMS), including data access control, incident response, and ongoing audit. |
| **RBI IT Framework for NBFCs & Banks** | Regulatory compliance (India) | Guides technology risk governance, data localization, cybersecurity resilience, and internal audit in regulated financial institutions. |
| **Basel III Operational Risk Framework (ORF)** | Capital and risk management | Applies standardized and advanced measurement approaches to operational risk and provides guidance for loss event data classification. |

All control activities within this document are either **fully or partially mapped to one or more of the above frameworks**, ensuring audit traceability, design robustness, and regulatory alignment.

The internal control environment is periodically reviewed by the **Internal Audit Function**, and enhancements are recommended based on test results, incident analysis, and evolving regulatory mandates.

## 4. Detailed Control Activities

This section outlines RBEYOND’s **key internal control activities**, categorized into **financial, operational, and compliance** domains. Controls are classified as **preventive, detective, or corrective**, and mapped to associated risks, roles, and regulatory requirements. Each control is documented to ensure clear accountability and traceability.

### 4.1 Financial Controls

#### 4.1.1 Reconciliation Procedures

* **4.1.1.1 Bank Reconciliation**  
  All operational and settlement accounts are reconciled daily by the Finance team. Exceptions are flagged automatically and investigated within 24 hours. Reconciliation logs are digitally archived.  
  Control Type: Detective | Frequency: Daily | Owner: Finance Controller
* **4.1.1.2 General Ledger (GL) Reconciliation**  
  All subsidiary ledgers (accounts receivable, payable, loans, etc.) are reconciled with the GL monthly. Unmatched entries are escalated.  
  Control Type: Detective | Frequency: Monthly | Owner: Financial Reporting Head
* **4.1.1.3 Intercompany Reconciliation**  
  Intercompany balances are reconciled quarterly. Any discrepancies require joint sign-off from both entities’ controllers and escalation to the CFO.  
  Control Type: Preventive/Detective | Frequency: Quarterly | Owner: Group Finance

#### 4.1.2 Authorization Limits

* **4.1.2.1 Transaction Approval Matrix**  
  A centrally maintained matrix defines financial and operational approval thresholds by role and department. All exceptions require CFO approval and audit log.  
  Control Type: Preventive | Frequency: Continuous | Owner: Financial Controller
* **4.1.2.2 Payment Authorization**  
  Dual-authorization is mandatory for payments above ₹10 lakhs or USD equivalent. Automated approval workflows are embedded in the ERP system.  
  Control Type: Preventive | Frequency: Per transaction | Owner: Treasury Team

#### 4.1.3 Segregation of Duties (SoD)

* **4.1.3.1 SoD Enforcement Matrix**  
  No individual is allowed to initiate, approve, and reconcile a transaction end-to-end. The SoD matrix is embedded within core systems, and reviewed bi-annually by Internal Audit.  
  Control Type: Preventive | Frequency: Bi-annually | Owner: Risk & Controls Team

#### 4.1.4 Journal Entry & Month-End Close Controls

* **4.1.4.1 Journal Entry Controls**  
  Manual journal entries require preparer and approver segregation. Entries over ₹5 lakhs require supporting documentation and CFO-level approval.  
  Control Type: Preventive | Frequency: Monthly | Owner: GL Accounting Lead
* **4.1.4.2 Month-End Close Checklist**  
  Standardized closing checklist across departments, with task owners, due dates, and sign-offs. Reviewed by Financial Controller before reporting.  
  Control Type: Detective | Frequency: Monthly | Owner: Financial Reporting Head

### 4.2 Operational Controls

#### 4.2.1 Transaction Monitoring

* **4.2.1.1 AML Transaction Screening**  
  All transactions are screened real-time using rule-based and machine-learning models. Suspicious activity is logged and reviewed by AML Compliance Team.  
  Control Type: Detective | Frequency: Real-time | Owner: AML Officer
* **4.2.1.2 KYC Validation**  
  KYC documents undergo automated OCR checks and are cross-verified against government and sanction lists. Any discrepancies are auto-flagged.  
  Control Type: Preventive | Frequency: At onboarding and periodic refresh | Owner: Onboarding Operations Lead
* **4.2.1.3 Internal Fraud Detection Engine**  
  A behavioral analytics engine monitors employee/system anomalies to detect potential internal fraud (e.g., override frequency, privilege misuse).  
  Control Type: Detective | Frequency: Continuous | Owner: Information Security & Fraud Risk Unit

#### 4.2.2 IT Controls

* **4.2.2.1 User Access Management**  
  Role-based access controls (RBAC) are implemented across systems. Access provisioning and de-provisioning are tracked via ticketing tools and reviewed monthly.  
  Control Type: Preventive | Frequency: Monthly | Owner: IT Security Lead
* **4.2.2.2 Change Management Controls**  
  All system changes (code, infrastructure) must pass through a controlled CI/CD pipeline with peer reviews, staging validation, and rollback plans.  
  Control Type: Preventive | Frequency: Per release | Owner: DevOps Manager
* **4.2.2.3 Endpoint Protection & Monitoring**  
  Anti-malware, EDR (Endpoint Detection & Response), and encryption tools are deployed on all corporate assets. Security events are logged centrally.  
  Control Type: Detective | Frequency: Real-time | Owner: CISO Office

#### 4.2.3 Business Continuity & Disaster Recovery

* **4.2.3.1 Business Continuity Plan (BCP)**  
  Department-wise BCPs exist for critical operations. DR drills are conducted semi-annually with metrics on RTO/RPO.  
  Control Type: Preventive | Frequency: Semi-annually | Owner: BCP Coordinator, Operations Team
* **4.2.3.2 Data Backup & Recovery**  
  Full and incremental backups of critical systems are scheduled daily and weekly. Backup success/failure logs are auto-reviewed.  
  Control Type: Detective | Frequency: Daily/Weekly | Owner: IT Infrastructure Lead

### 4.3 Compliance Controls

#### 4.3.1 Regulatory Reporting

* **4.3.1.1 Basel III Capital Reporting Controls**  
  Capital adequacy ratio, LCR, and NSFR calculations are automated via the risk engine and reviewed by the Risk & Treasury teams monthly.  
  Control Type: Preventive | Frequency: Monthly | Owner: Treasury Risk Manager
* **4.3.1.2 FATCA & CRS Compliance**  
  Customer tax status and residency are verified at onboarding. Reports are generated quarterly and validated by Legal & Compliance.  
  Control Type: Preventive/Detective | Frequency: Quarterly | Owner: Compliance Officer
* **4.3.1.3 Dodd-Frank Stress Test Submissions**  
  If applicable to global operations, macroeconomic stress testing scenarios are modeled and submitted to regulatory bodies in line with calendar schedules.  
  Control Type: Preventive | Frequency: Annually | Owner: Risk Modeling Team

#### 4.3.2 Tax Compliance

* **4.3.2.1 Withholding Tax Monitoring**  
  System-generated checks on applicable TDS/GST withholding at payment initiation. Tax compliance reports are submitted monthly.  
  Control Type: Preventive | Frequency: Monthly | Owner: Taxation Manager
* **4.3.2.2 Transfer Pricing Review**  
  Intercompany service arrangements are reviewed annually to align with Arm’s Length Pricing principles.  
  Control Type: Preventive | Frequency: Annually | Owner: CFO Office / External Consultant

#### 4.3.3 Audit Trails & Record Keeping

* **4.3.3.1 Audit Trail Preservation**  
  All critical systems maintain immutable audit logs. Changes, approvals, and data access are timestamped and encrypted.  
  Control Type: Detective | Frequency: Continuous | Owner: Information Security Team
* **4.3.3.2 Document Retention Policy**  
  Data and document retention is aligned to regulatory mandates (e.g., 8 years for KYC, 10 years for audit records). Enforcement is automated via DMS.  
  Control Type: Preventive | Frequency: Continuous | Owner: Legal & Records Management

## 5. Monitoring & Reporting

The effectiveness of RBEYOND’s internal control environment is sustained through continuous **monitoring mechanisms, structured reporting frameworks, and timely escalation protocols**. This ensures that control breaches, emerging risks, and process inefficiencies are identified, remediated, and communicated to relevant stakeholders proactively.

### 5.1 Key Performance Indicators (KPIs) & Key Risk Indicators (KRIs)

RBEYOND utilizes **quantitative control metrics** to assess operational health and risk exposure across business functions. These indicators are tracked regularly and reviewed by the Risk Committee, Control Owners, and Business Heads to identify control failures, emerging trends, and exceptions.

#### 5.1.1 Key Performance Indicators (KPIs)

| **KPI Name** | **Description** | **Target** | **Frequency** | **Owner** |
| --- | --- | --- | --- | --- |
| Control Test Coverage | % of controls tested in the control inventory | ≥ 95% | Quarterly | Internal Audit |
| Timely Closure of Issues | % of control issues remediated within deadline | ≥ 90% | Monthly | Risk Owners |
| Reconciliation Timeliness | % of accounts reconciled within defined TAT | 100% | Monthly | Finance Team |
| Month-End Close Adherence | % of departments closing books within 5 days | ≥ 95% | Monthly | Financial Controller |
| SLA Adherence (Transaction Approvals) | % of transactions approved within SLA | ≥ 98% | Monthly | Process Owners |

#### 5.1.2 Key Risk Indicators (KRIs)

| **KRI Name** | **Description** | **Tolerance Threshold** | **Frequency** | **Monitoring Unit** |
| --- | --- | --- | --- | --- |
| System Downtime | Minutes of unplanned core system downtime | < 60 mins/month | Monthly | IT Ops |
| Failed Logins (Security Risk) | Count of failed privileged access attempts | < 50/month | Weekly | CISO |
| Suspicious Transactions Flagged | % of transactions flagged by AML engine | < 0.1% of total | Daily | AML Unit |
| Audit Issues Rated “High” | Number of open high-risk audit issues | 0 | Monthly | Internal Audit |
| Non-Compliant Regulatory Reports | Missed or inaccurate regulatory filings | 0 | Monthly | Compliance Officer |

These indicators are embedded within the **ERM Dashboard**, accessible by management and the Board.

### 5.2 Internal Audit Findings & Remediation Plans

RBEYOND maintains an **independent Internal Audit Function**, reporting to the Audit Committee, which conducts regular risk-based audits of business processes, IT controls, and compliance domains.

* **Audit Planning:**  
  Based on annual risk assessments and past audit history, critical processes and high-risk areas are prioritized.
* **Findings Classification:**  
  Audit findings are rated as High, Medium, or Low based on potential impact and likelihood.
* **Remediation Tracking:**  
  All findings are entered into the **Issue Management Tracker (IMT)** with assigned owners and closure timelines. Progress is reviewed weekly.
* **Audit Committee Oversight:**  
  Outstanding high-priority issues are escalated to the Audit Committee in quarterly meetings. Any issue open for >90 days beyond deadline is flagged for executive attention.
* **Root Cause Analysis:**  
  For repeat issues or systemic failures, root cause analysis (RCA) is mandatory, along with a sustainable action plan signed off by senior management.

### 5.3 Management Reporting

RBEYOND ensures timely and insightful reporting to decision-makers at all levels to maintain effective control oversight.

#### 5.3.1 Executive Dashboard

A centralized **Risk & Control Dashboard** (built in Power BI) provides visual summaries of:

* Control status (active, ineffective, overdue for review)
* Open audit findings by severity
* Control test results and evidence health
* Emerging risks and threshold breaches (KRIs)
* Control owner performance and accountability

The dashboard is accessible to the CRO, CFO, CISO, and the CEO’s Office, with filters for business unit, geography, and control category.

#### 5.3.2 Monthly MIS Pack

Each month, a **Management Information System (MIS) Pack** is circulated to relevant departments and senior leaders, containing:

* Summary of control breaches and exceptions
* Key KPIs and KRIs
* Closed and overdue audit items
* Compliance tracker (reporting calendar, upcoming filings)
* Control improvement initiatives in-flight

#### 5.3.3 Escalation Protocols

Escalation tiers are defined by severity and time-to-resolve:

| **Severity** | **Escalation Level** | **Timeline** |
| --- | --- | --- |
| High (e.g., fraud, data breach, regulatory violation) | Board, CRO, CEO | Immediate (within 2 hours) |
| Medium (e.g., process breakdown, internal system failure) | Function Head, Compliance, Risk | Within 24 hours |
| Low (e.g., missed documentation, expired access logs) | Process Owner | Weekly Review |

Each incident report must include a classification, impact assessment, action owner, and resolution timeline. Incident logs are archived in the **GRC (Governance, Risk & Compliance)** platform for audit and review purposes.

## 6. Roles & Responsibilities

A clear definition of roles and responsibilities is critical for the successful execution, monitoring, and improvement of the internal control environment at RBEYOND. This section defines the accountability framework under the **Three Lines of Defense (3LoD) Model** and establishes escalation pathways for unresolved control failures.

### 6.1 Control Owners

Control Owners are individuals or teams responsible for **implementing, executing, and maintaining internal controls** within their respective business functions. They are accountable for:

* Ensuring controls are consistently performed as designed
* Retaining supporting documentation or system evidence
* Conducting self-assessments and risk awareness within their units
* Responding to audit or compliance observations related to their controls
* Initiating remediation plans for failed or outdated controls

**Typical Control Owners** at RBEYOND include:

| **Role** | **Example Control Area** |
| --- | --- |
| Finance Controller | GL Reconciliation, Journal Entries |
| AML Compliance Lead | Transaction Screening, AML Risk Rating |
| Treasury Head | Liquidity Reporting, Investment Limits |
| IT Security Manager | Access Controls, Patch Management |
| Legal & Compliance Officer | Regulatory Reporting, FATCA Compliance |
| Product Ops Lead | SoD Enforcement, Customer Onboarding Controls |

Each control in the Control Register is mapped to an identified Control Owner in accordance with process risk mapping.

### 6.2 Control Reviewers

Reviewers are **independent parties responsible for validating** that controls are:

* Properly designed and implemented
* Operating effectively on a consistent basis
* Backed by sufficient evidence and audit trail

Control Reviewers do not execute controls themselves. Their primary responsibilities include:

* Reviewing control logs and documentation
* Verifying control test results and exceptions
* Signing off on periodic control assessments
* Challenging control adequacy during risk reviews
* Validating remediation closures

**Typical Control Reviewers** at RBEYOND include:

| **Role** | **Review Focus Area** |
| --- | --- |
| Internal Audit | Full-spectrum control testing and effectiveness review |
| Risk & Controls Team | Design adequacy and SoD assessments |
| Chief Compliance Officer | Regulatory alignment and control sufficiency |
| Chief Risk Officer | Enterprise risk mitigation and KRI thresholds |
| Business Unit Heads | Department-level oversight and accountability |

Reviewers report significant deficiencies or recurring failures to the **second or third line of defense** depending on impact.

### 6.3 Escalation Path for Control Failures

In case of a control breakdown, failure to operate, or test failure, an immediate escalation protocol must be followed to ensure timely mitigation and response.

#### 6.3.1 Escalation Tiers

| **Impact Level** | **Definition** | **Escalation Path** | **Timeline** |
| --- | --- | --- | --- |
| **Critical** | Regulatory violation, financial misstatement, fraud exposure, data breach | CRO, CCO, CEO, Board / Audit Committee | Within 2 hours |
| **High** | Repeated control failure, audit red-flag, high-value transaction risk | Function Head, Risk Management, Internal Audit | Within 24 hours |
| **Medium** | Process deviation, overdue reconciliation, minor policy gap | Control Owner’s Supervisor, Compliance Analyst | Within 48 hours |
| **Low** | One-time exception, documentation lapse, minor breach | Self-logged by Control Owner, reviewed in weekly ops meeting | Within 5 days |

#### 6.3.2 Failure Response Protocol

Once a control failure is identified:

1. **Control Owner** logs the issue in the Internal Control Tracker (ICT).
2. **Reviewer** validates the failure, classifies impact level, and checks if compensating controls exist.
3. **Root Cause Analysis (RCA)** is initiated for high or critical issues.
4. **Remediation Plan** with owners and timelines is created.
5. **Progress is monitored** weekly until closure, and status is escalated if overdue.
6. **Closure Validation** is performed by the original Reviewer or Internal Audit.

All escalations are recorded in the GRC Platform with timestamps, audit trails, and documentation to ensure accountability and transparency.

## 7. Documentation & Evidence

A strong internal control system relies not only on well-defined control activities, but also on **verifiable documentation** and **traceable evidence** to demonstrate design integrity, operating effectiveness, and regulatory compliance. This section outlines RBEYOND’s standards and expectations for maintaining such documentation.

### 7.1 Sample Templates and Standardized Control Documentation

To promote consistency, all business and functional units are required to use standardized templates for executing and evidencing controls. These templates are version-controlled, periodically updated, and stored in the centralized **Control Documentation Repository (CDR)** hosted on the internal GRC platform.

#### 7.1.1 Common Templates

| **Template Name** | **Description** | **Maintained By** |
| --- | --- | --- |
| **Control Execution Checklist** | Step-by-step procedural checklist for recurring controls (e.g., month-end close, KYC refresh) | Control Owners |
| **Transaction Approval Form** | Multi-level digital form capturing amount, approver comments, thresholds, and digital signature | Finance / Business Ops |
| **Exception Log Register** | Used to record control exceptions, reasons for deviation, and any compensating measures | Risk & Controls Team |
| **Access Request / Removal Form** | Standard IT form for requesting system access, de-provisioning, or privilege modification | IT Security |
| **Incident & RCA Template** | Standard reporting format for control failures, with root cause and corrective actions | Control Owner & Reviewer |
| **Audit Readiness File (ARF)** | Folder of supporting documents for each audited control, tagged with evidence type and control ID | Internal Audit Liaisons |

Templates are accessible via the company’s **Internal Wiki and Compliance Hub**, and each business unit has a Control Champion responsible for ensuring their usage.

### 7.2 Reference to Governing Policies

Control documentation must align with RBEYOND’s formally approved governance policies and regulatory frameworks. The following policies serve as **anchor references** for control execution and audit testing:

| **Policy Name** | **Version** | **Owner** | **Relevance to Control Framework** |
| --- | --- | --- | --- |
| **Internal Controls over Financial Reporting (ICFR) Policy** | v3.1 | CFO | Basis for all financial controls (journal entries, reconciliations, SoD) |
| **IT Security & Access Management Policy** | v2.7 | CISO | Governs user access, privilege escalation, endpoint security |
| **Anti-Fraud & Whistleblower Policy** | v1.9 | CRO | Covers fraud detection controls, reporting mechanisms, escalation |
| **Records Retention & Data Classification Policy** | v2.3 | Legal & Compliance | Defines evidence retention timelines, access, and audit logs |
| **Regulatory Compliance Policy** | v3.0 | Chief Compliance Officer | Outlines regulatory reporting responsibilities and evidence handling |
| **Business Continuity & DR Policy** | v1.5 | COO | Covers documentation of DR testing, business impact assessments |
| **Vendor Risk Management Policy** | v2.2 | Procurement | Defines third-party control assurance, SLAs, SOC-2 requirements |

All documentation must reflect adherence to these policies. Controls failing to cite policy basis may be considered **incomplete or non-compliant** during audits.

### 7.3 Audit Evidence Requirements

For each control, **evidence of execution and effectiveness** must be retained in either **automated logs**, **signed records**, or **system screenshots**, based on the nature of the control. The audit team uses this evidence during walkthroughs, control testing, and substantiation of reports.

#### 7.3.1 Types of Acceptable Audit Evidence

| **Evidence Type** | **Examples** | **Acceptable Format** |
| --- | --- | --- |
| **System Logs** | Access logs, audit trails, transaction timestamps | System exports (CSV/XML), screenshots with timestamps |
| **Digital Approvals** | Workflow approvals, sign-offs via ERP/CRM | PDF extracts, screenshots of audit trail |
| **Email Records** | Approvals, clarifications, escalations | Archived email threads (EML or PDF format) |
| **Manual Checklists** | Signed paper/e-forms of procedural checklists | Scanned PDF with date, signature, control ID |
| **Exception Reports** | Logs of flagged events, incidents, or alerts | System-generated reports, manual registers |
| **Supporting Documents** | KYC documents, regulatory filing copies, tax proofs | Scans or originals as per policy retention requirements |

#### 7.3.2 Evidence Retention Standards

| **Evidence Type** | **Retention Period** | **Storage Location** |
| --- | --- | --- |
| Financial Controls | 8 years | Finance Shared Drive / DMS |
| Regulatory Reports | 10 years | Compliance Vault |
| KYC & Onboarding Records | 8 years post-relationship | Customer DMS |
| Access Logs & Security Events | 3–5 years (as per IT Policy) | SIEM or Cloud Log Archive |
| Audit Working Papers | 7 years | Internal Audit SharePoint |

Evidence older than the mandated retention period must be destroyed in accordance with the **Data Disposal Protocol**, and destruction logs must be maintained.

## 8. Review & Update Mechanism

To maintain the **relevance, effectiveness, and compliance** of RBEYOND’s internal controls, all controls undergo **scheduled reviews**, are subject to **formal change management**, and are tracked through a **version-controlled documentation system**.

### 8.1 Frequency of Control Reviews

All controls are reviewed based on their **risk rating, regulatory significance, and criticality to operations**. The schedule is designed to ensure preventive identification of control obsolescence, design failure, or misalignment with real-world business conditions.

#### 8.1.1 Review Frequency Matrix

| **Control Category** | **Review Frequency** | **Responsible Team** |
| --- | --- | --- |
| High-Risk Controls (e.g., AML, financial reporting, access control) | Quarterly | Control Owners + Risk Team |
| Moderate-Risk Controls (e.g., process-level reconciliations, manual approvals) | Semi-Annually | Process Owners |
| Low-Risk or Supporting Controls (e.g., documentation checklists, file naming standards) | Annually | Business Control Champions |
| Compliance-Controlled Areas (e.g., regulatory filings, data privacy) | Quarterly or as per regulatory update | Compliance & Legal |
| IT and Cybersecurity Controls | Bi-annually | CISO Office |

The **Internal Audit** and **GRC Platform** issue automated alerts for overdue reviews and ensure reminders are sent to control owners before the review window.

### 8.2 Process for Updating Controls (Change Management)

Control changes—whether due to internal transformation, external regulations, or audit recommendations—must follow RBEYOND’s **Control Change Management Procedure (CCMP)**. This ensures that any control modification is documented, risk-assessed, tested, and approved before going live.

#### 8.2.1 Control Update Workflow

1. **Change Trigger:**
   * Regulatory update
   * Process redesign
   * New IT system implementation
   * Internal audit finding
   * Risk assessment or incident
2. **Change Request Submission:**  
   Control Owner raises a **Control Change Request (CCR)** in the GRC platform, specifying:
   * Justification for the change
   * Risk rating impact
   * Affected processes and departments
   * Expected go-live date
3. **Risk & Impact Assessment:**  
   Risk Management and Internal Audit assess the:
   * Control design strength
   * Impact on KRIs, regulatory obligations
   * Dependency on automation or manual workflows
4. **Pilot Testing (if applicable):**  
   New control version is piloted in a test or non-critical environment for functionality and integration.
5. **Formal Approval:**  
   Control changes require approvals from:
   * Risk & Controls Team (design validation)
   * Process Owner / Function Head (execution capability)
   * Compliance (if regulatory)
   * Internal Audit (for closure of related observations)
6. **Training & Communication:**  
   Updated controls are communicated to affected teams through internal bulletins, training sessions, or intranet updates.
7. **Implementation & Documentation:**  
   Final control version is published with new **control ID version**, mapped documents/templates, and attached evidence requirements.

### 8.3 Version Control & Approval History

All controls in the **Control Inventory Register (CIR)** are subject to **strict version control** managed via the GRC system. Every control update is assigned a unique version number and carries an immutable audit trail.

#### 8.3.1 Versioning Format

| **Element** | **Format Example** |
| --- | --- |
| Control ID | FIN-001-JE (Financial → Journal Entry) |
| Version Number | v1.0 (Initial), v1.1 (Minor Change), v2.0 (Major Redesign) |
| Effective Date | July 3, 2025 |
| Status | Draft, Active, Under Review, Archived |

#### 8.3.2 Approval History Log

Each control contains a structured **approval history** embedded in its metadata:

| **Field** | **Example** |
| --- | --- |
| Change Initiated By | Finance Controller |
| Risk Impact Assessment Completed By | Risk Manager |
| Approved By | CRO, CCO |
| Final Review Date | June 30, 2025 |
| Next Scheduled Review | September 30, 2025 |
| Linked Audit Observation (if any) | IA-FY24-FIN-12 (Unsegregated journal entries) |

All historical versions of control documents are archived and accessible for internal or regulatory audits. Archived controls are clearly marked as **“Obsolete – Not in Use”** and are excluded from current test cycles.

## 9. Annexures

This section includes supplemental documents and reference materials critical for the effective implementation and understanding of the internal control framework. All annexures are maintained in digital form and accessible via RBEYOND’s **GRC Portal** under the “Control Documentation” module.

### 9.1 Annexure A – Glossary of Key Terms

| **Term** | **Definition** |
| --- | --- |
| **Control Owner** | The individual or function responsible for implementing and executing a specific control. |
| **Control Reviewer** | A party independent of the Control Owner responsible for verifying control effectiveness. |
| **GRC Platform** | Governance, Risk & Compliance system used for managing controls, risks, issues, and documentation. |
| **Control ID** | A unique identifier assigned to each control for tracking and audit purposes. |
| **KPI** | Key Performance Indicator – a metric that measures control performance. |
| **KRI** | Key Risk Indicator – a metric that signals potential risk exposures. |
| **SoD** | Segregation of Duties – a principle to prevent conflict of interest by separating responsibilities. |
| **Control Failure** | A situation where a control does not operate as designed or fails to mitigate associated risk. |
| **RCA** | Root Cause Analysis – a structured approach to determine the underlying reason for a control failure. |
| **CCR** | Control Change Request – a formal request raised to modify, replace, or retire a control. |

### 9.2 Annexure B – Sample Control Register (Excerpt)

| **Control ID** | **Description** | **Type** | **Frequency** | **Owner** | **Reviewer** | **Evidence Required** |
| --- | --- | --- | --- | --- | --- | --- |
| FIN-001-JE | Journal Entry Approval | Preventive | Monthly | GL Controller | Finance Head | Approved JE forms, supporting docs |
| IT-004-AC | User Access Provisioning | Preventive | Per Request | IT Security Admin | CISO Office | Access request form, approval email |
| AML-003-TX | Suspicious Transaction Screening | Detective | Real-time | AML Compliance Officer | Risk Manager | AML tool logs, flagged transaction review |
| REG-002-LCR | Liquidity Coverage Ratio Calculation | Preventive | Monthly | Treasury Team | Internal Audit | LCR model export, approval note |
| OPS-007-KYC | KYC Document Verification | Preventive | Onboarding | Ops Manager | Compliance Lead | OCR report, ID scans |

The full register includes over 200 controls, each with fields for risk rating, control category, regulatory mapping, and audit cycle.

### 9.3 Annexure C – Sample Forms & Templates

These standardized forms are available via the internal GRC portal and must be used for all related activities:

#### C.1 Control Execution Checklist (Excerpt)

markdown

CopyEdit

Control ID: FIN-001-JE

Control Name: Journal Entry Approval

Prepared By: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Approved By: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_

☐ Journal Entry complies with SoD

☐ Supporting documents are attached (invoice, memo, calculation sheet)

☐ JE amount exceeds ₹5L – CFO approval attached

☐ Entry posted in SAP FICO module

☐ Entry reconciled during month-end close

Remarks: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

#### C.2 Control Change Request Form (CCR)

| **Field** | **Input** |
| --- | --- |
| Control ID | OPS-012-RPT |
| Change Type | Update frequency from monthly to weekly |
| Reason | Increased reporting volume post regulatory circular |
| Risk Impact | Medium |
| Initiated By | Compliance Officer |
| Approval Required From | CRO, Audit, Compliance |
| Go-Live Date | August 1, 2025 |

#### C.3 Incident & RCA Report (Excerpt)

yaml

CopyEdit

Incident: Missed FATCA reporting deadline for Q1

Impact: Regulatory non-compliance; potential fine of ₹5L

Root Cause: Delay in customer residency classification in system

Corrective Action: Automate FATCA flag mapping; add 2nd-level review step

Owner: Compliance Tech Team

Expected Closure: August 15, 2025

### 9.4 Annexure D – Policy & Regulatory Reference Mapping

| **Control ID** | **Linked Policy** | **Regulation Reference** |
| --- | --- | --- |
| AML-001 | Anti-Fraud & AML Policy | PMLA Act, RBI AML Guidelines |
| IT-004 | IT Security Policy | ISO 27001, RBI Cyber Security Framework |
| TAX-005 | Tax Policy | Income Tax Act, OECD Transfer Pricing |
| REG-009 | Regulatory Compliance Policy | Basel III, RBI Master Circulars |
| HR-007 | HR & Ethics Policy | Whistleblower Protection Act |

Each control in the inventory is linked to a master policy and, where applicable, external compliance obligations. This ensures alignment during audits and regulatory inspections.

### 9.5 Annexure E – Review & Test Calendar

| **Quarter** | **Key Activities** |
| --- | --- |
| Q1 | Annual Control Review Kickoff, Audit Scoping |
| Q2 | Internal Audit Field Testing, Issue Validation |
| Q3 | Remediation Follow-up, RCA Workshops |
| Q4 | Risk Reassessment, Control Refresh, Policy Updates |