// FRAMEWORK OVERVIEW

GRC Workflow
Insurance Sector

Governance, Risk & Compliance — end-to-end operational framework for insurance carriers, reinsurers, and intermediaries.

GOVERNANCE
RISK MANAGEMENT
COMPLIANCE
REGULATORY
CONTINUOUS IMPROVEMENT

▸ REGULATORY FRAMEWORKS

Solvency II | IRDAI Guidelines | NAIC Model Laws | ICP / IAIS | IFRS 17 | GDPR / DPDP Act | AML / KYC | ISO 31000 | Basel III (for bancassurance)

PILLAR 01

Governance

PILLAR 02

Risk Management

PILLAR 03

Compliance

G.1 Board & Leadership Oversight

- → Board Risk & Audit Committee
- → Chief Risk Officer (CRO)
- → Chief Compliance Officer (CCO)
- → 3 Lines of Defence model

G.2 Policy & Framework Setting

- → Enterprise Risk Appetite Statement
- → Underwriting & Claims Policies
- → Delegated Authorities Matrix
- → Code of Conduct & Ethics

G.3 Strategic Alignment

- → ORSA (Own Risk & Solvency Assessment)
- → KPIs & KRIs Dashboard
- → Capital Allocation Review
- → Reinsurance Strategy

G.4 Internal Audit Function

- → Annual Audit Plan
- → Independent Assurance Reviews
- → Issue Tracking & Remediation
- → Audit Committee Reporting

G.5 Stakeholder Reporting

- → Regulatory Filings & Returns
- → Board Reporting Pack
- → Investor & Rating Agency Reports
- → Public Disclosure (SFCR/RSR)

◉ CORE GRC PROCESS FLOW

01 Risk Identification & Taxonomy

Systematically identify all risk categories across the insurance value chain — underwriting risk, market risk, credit risk, operational risk, liquidity risk, and emerging risks (cyber, climate, pandemic).

Risk Register | Risk Taxonomy | Horizon Scanning | Business Environment Analysis

↓

02 Risk Assessment & Quantification

Evaluate identified risks using qualitative and quantitative methods. Apply actuarial models, scenario analysis, and stress testing to size exposure and likelihood. Set risk appetite thresholds.

Heat Maps | Actuarial Modelling | VaR / TVaR | Stress Testing | SCR Calculation

↓

03 Compliance Obligation Mapping

Map all applicable regulatory obligations to internal controls. Maintain a live compliance obligations register aligned to IRDAI, Solvency II, AML, data protection, and product regulation requirements.

Obligations Register | Control Library | Reg-Change Monitoring | Gap Analysis

↓

04 Control Design & Implementation

Design preventive, detective, and corrective controls across underwriting, claims, distribution, investments, and operations. Implement technology-enabled controls and automated workflows for efficiency.

Control Framework | RCSA | Segregation of Duties | Automated Monitoring

↓

05 Monitoring, Testing & Assurance

Continuously monitor risk levels and control effectiveness. Conduct regular control testing, key risk indicator (KRI) surveillance, regulatory reporting, and independent second-line assurance reviews.

KRI Monitoring | Control Testing | Compliance Surveillance | Real-time Dashboards

↓

06 Incident & Breach Management

Detect, report, investigate, and remediate risk events, compliance breaches, and operational losses. Escalate material incidents to senior management and regulators within required timeframes.

Incident Log | Root Cause Analysis | Regulatory Notification | Loss Database

↓

07 Reporting, Review & Continuous Improvement

Produce comprehensive risk and compliance reports for the Board, regulators, and management. Conduct periodic reviews of the GRC framework and integrate lessons learned into updated policies and controls.

Board Reporting | ORSA Report | Regulatory Returns | Framework Review

Continuous Feedback Loop

Reporting insights, emerging risks, and control failures feed back into Risk Identification (Step 01), ensuring the GRC cycle is dynamic and adaptive to the evolving insurance landscape.

◈ RISK & COMPLIANCE LAYER

R.1 ⚖️ **Insurance-Specific Risk Types**

- → Underwriting / Pricing Risk
- → Reserving & Actuarial Risk
- → Catastrophe (CAT) Risk
- → Reinsurance Credit Risk
- → Asset-Liability Mismatch
- → Lapse / Persistency Risk

C.1 🔍 **Compliance Domains**

- → Product Approval & Pricing
- → Sales Conduct & Distribution
- → Claims Handling Standards
- → AML / CFT Screening
- → Data Privacy (GDPR / DPDP)
- → Market Conduct Monitoring

T.1 🛠️ **GRC Technology Stack**

- → GRC Platform (Archer / ServiceNow)
- → Actuarial Modelling (Prophet / Igloo)
- → Fraud Detection (AI/ML)
- → RegTech for Reg Monitoring
- → SIEM for Cyber Risk
- → BI Dashboards (Power BI)

E.1 🌐 **Emerging Risk Areas**

- → Climate / ESG Risk
- → Cyber Liability & Resilience
- → AI / Model Risk
- → Pandemic & Systemic Risk
- → Third-Party / Vendor Risk
- → Geopolitical & Macro Risk

K.1 📈 **Key Metrics (KRIs / KPIs)**

- → Combined Ratio & Loss Ratio
- → Solvency Coverage Ratio
- → Complaint Ratio (per 10,000)
- → Policy Lapse Rate
- → Regulatory Breach Count

3 LINES OF DEFENCE	**7** CORE PROCESS STEPS
9+ REGULATORY FRAMEWORKS	**6** EMERGING RISK CATEGORIES
360° CONTINUOUS LOOP	

GRC INSURANCE FRAMEWORK · GOVERNANCE · RISK MANAGEMENT · COMPLIANCE · CONTINUOUS IMPROVEMENT