

# *GRC Audit Checklist*

## Governance Framework

### Board Governance

- ☐ Board composition meets Companies Act 2013 requirements
- ☐ Independent directors constitute required percentage
- ☐ Board meetings held as per statutory requirements
- ☐ Minutes of board meetings properly documented
- ☐ Board committees established (Audit, Nomination, Remuneration)
- ☐ Director training and familiarization programs conducted
- ☐ Board evaluation process implemented annually
- ☐ Related party transactions properly disclosed and approved

### Management Structure

- ☐ Organizational chart clearly defined with reporting lines
- ☐ Roles and responsibilities documented for key positions
- ☐ Delegation of authority matrix established
- ☐ Management committees functioning effectively
- ☐ Key managerial personnel appointments comply with regulations
- ☐ Succession planning for critical roles documented

## Corporate Policies

- ☐ Code of conduct for directors and employees adopted
- ☐ Whistleblower policy implemented with proper channels
- ☐ Anti-corruption and bribery policies established
- ☐ Conflict of interest policy documented
- ☐ Information security policy implemented
- ☐ HR policies comply with labor laws

## Risk Management

### Risk Assessment Framework

- ☐ Enterprise risk management policy approved by board
- ☐ Risk identification process covers all business areas
- ☐ Risk assessment methodology documented and consistent
- ☐ Risk appetite and tolerance levels defined
- ☐ Business continuity and disaster recovery plans tested
- ☐ Insurance coverage adequate for identified risks

### Operational Risk Management

- ☐ Key operational risks identified and assessed
- ☐ Internal controls designed to mitigate operational risks
- ☐ Regular monitoring of operational risk indicators
- ☐ Incident reporting and management system operational
- ☐ Vendor and third-party risk assessment conducted
- ☐ Cybersecurity risks assessed and managed



## Financial Risk Management

- ☐ Credit risk management policies implemented
- ☐ Liquidity risk monitoring mechanisms established
- ☐ Market risk exposure regularly assessed
- ☐ Foreign exchange risk management procedures active
- ☐ Interest rate risk management strategies defined
- ☐ Capital adequacy maintained as per regulations

## Compliance Framework

### Regulatory Compliance

- ☐ Companies Act 2013 compliance verified
- ☐ SEBI regulations adherence (for listed companies)
- ☐ RBI guidelines compliance (for financial institutions)
- ☐ GST compliance and return filings current
- ☐ Income Tax Act compliance verified
- ☐ Labor law compliance across all locations
- ☐ Environmental clearances and compliance verified
- ☐ Industry-specific regulatory compliance checked

### Statutory Filings and Returns

- ☐ Annual returns filed within prescribed timelines
- ☐ Financial statements filed as per requirements
- ☐ Board resolutions passed for statutory matters
- ☐ Regulatory approvals obtained where required
- ☐ Compliance certificates from statutory auditors obtained
- ☐ E-forms filed with MCA within due dates



## Internal Compliance Monitoring

- ☐ Compliance calendar maintained and updated
- ☐ Compliance monitoring system operational
- ☐ Regular compliance reports to board/management
- ☐ Non-compliance incidents tracked and resolved
- ☐ Compliance training programs conducted
- ☐ Legal and regulatory updates communicated

## Internal Controls and Audit

### Internal Control Systems

- ☐ Internal financial controls designed and implemented
- ☐ Control activities address identified risks
- ☐ Segregation of duties maintained adequately
- ☐ Authorization levels clearly defined and followed
- ☐ Documentation and record keeping standards met
- ☐ IT general controls and application controls effective

### Internal Audit Function

- ☐ Internal audit charter approved by audit committee
- ☐ Risk-based internal audit plan developed annually
- ☐ Internal audit findings tracked to closure
- ☐ Management responses to audit findings documented
- ☐ Follow-up audits conducted for high-risk areas
- ☐ Coordination with external auditors maintained



## External Audit Coordination

- ☐ Statutory auditor independence maintained
- ☐ Management letter points addressed timely
- ☐ Audit committee review of audit findings conducted
- ☐ External auditor recommendations implemented
- ☐ Coordination between internal and external auditors

## Data Protection and Privacy

### Information Security

- ☐ Information security policy comprehensive and current
- ☐ Data classification and handling procedures defined
- ☐ Access controls and user authentication systems robust
- ☐ Regular security assessments and penetration testing
- ☐ Incident response procedures documented and tested
- ☐ Employee training on information security conducted

### Privacy Compliance

- ☐ Personal data protection policies implemented
- ☐ Data processing agreements with vendors executed
- ☐ Customer consent mechanisms for data collection
- ☐ Data breach notification procedures established
- ☐ Regular privacy impact assessments conducted
- ☐ Cross-border data transfer compliance verified

# ESG (Environmental, Social, Governance)

## Environmental Compliance

- ☐ Environmental management system implemented
- ☐ Pollution control measures and monitoring active
- ☐ Waste management procedures compliant
- ☐ Energy consumption and efficiency monitored
- ☐ Carbon footprint assessment and reduction plans
- ☐ Environmental reporting requirements met

## Social Responsibility

- ☐ CSR policy and committee established (if applicable)
- ☐ CSR spending compliance with statutory requirements
- ☐ Stakeholder engagement processes documented
- ☐ Employee welfare and safety measures implemented
- ☐ Diversity and inclusion policies active
- ☐ Community development programs monitored

## Technology and Systems

### IT Governance

- ☐ IT governance framework aligned with business strategy
- ☐ IT risk management integrated with enterprise risk
- ☐ IT service management processes documented
- ☐ Business continuity plans for IT systems tested
- ☐ Software licensing compliance verified
- ☐ Cloud services governance and security assessed



## Data Management

- ☐ Data governance framework established
- ☐ Master data management processes implemented
- ☐ Data quality monitoring mechanisms active
- ☐ Data retention and archival policies followed
- ☐ System integration and data flow controls effective
- ☐ Regular data backup and recovery testing conducted

## Financial Reporting and Controls

### Financial Reporting

- ☐ Financial statements preparation process documented
- ☐ Accounting policies consistently applied
- ☐ Management discussion and analysis comprehensive
- ☐ Quarterly and annual reporting timelines met
- ☐ Related party disclosures complete and accurate
- ☐ Fair value measurements and impairments assessed

### Internal Financial Controls

- ☐ Control environment assessment completed
- ☐ Risk assessment for financial reporting conducted
- ☐ Control activities designed and operating effectively
- ☐ Information and communication systems adequate
- ☐ Monitoring activities for controls implemented
- ☐ Deficiencies in controls identified and remediated



# Sector-Specific Compliance

## Banking and Financial Services

- ☐ Basel III capital adequacy requirements met
- ☐ Know Your Customer (KYC) norms compliance
- ☐ Anti-Money Laundering (AML) procedures effective
- ☐ Loan classification and provisioning accurate
- ☐ Regulatory returns and reports submitted timely
- ☐ Consumer protection measures implemented

## Manufacturing

- ☐ Factory licenses and approvals current
- ☐ Product quality and safety standards compliance
- ☐ Supply chain risk management implemented
- ☐ Intellectual property protection measures active
- ☐ Export-import compliance verified
- ☐ Industrial safety and health regulations followed

## Information Technology

- ☐ Software development lifecycle controls implemented
- ☐ Client data security and confidentiality maintained
- ☐ Service level agreement compliance monitored
- ☐ Intellectual property and contract management effective
- ☐ Export control regulations compliance (if applicable)
- ☐ Quality management system certifications current





# Documentation and Reporting

## Policy Documentation

- ☐ All policies reviewed and updated annually
- ☐ Policy approval process followed consistently
- ☐ Policy communication and training documented
- ☐ Policy exceptions tracked and approved appropriately
- ☐ Version control for policy documents maintained

## Audit Documentation

- ☐ Audit working papers complete and organized
- ☐ Evidence supporting audit conclusions adequate
- ☐ Audit findings and recommendations clearly documented
- ☐ Management responses and action plans recorded
- ☐ Follow-up on previous audit findings tracked
- ☐ Audit reports distributed to appropriate stakeholders

## Compliance Reporting

- ☐ Regular compliance dashboards prepared
- ☐ Exception reports generated and reviewed
- ☐ Compliance metrics and KPIs tracked
- ☐ Board and committee reporting comprehensive
- ☐ Regulatory reporting accurate and timely
- ☐ Stakeholder communication on compliance matters effective

