KPMG

Enterprise Wide Risk Management Framework

Regulatory Compliance

1 Risk Governance

Committee Structure and Authority
- Board and Board Risk Committee
- Mandate + delegated authorities

Holistic approach
- Risk Management philosophy and key principles
- Link to strategic planning capital + funding frameworks

Risk Culture, Values and Behaviours
- "Tone at the top"
- Reward and Remuneration
- Transparency and disclosure

Risk Appetite Statement
- Key Risks
- Risk Bearing capacity
- Risk Tolerance and Limits

Risk Framework + Key Risk Policies
- Approve ERM Framework
- Risk Policy Framework & Hierarchy

2 Risk Oversight and Control Function

- CRO mandate and organisation
- Stress testing and resilience
- Review, challenge, reporting & escalation
- Framework & policy oversight and maintenance
- Model Validation and Approval
- Enterprise wide view and aggregation

3 Risk Operating Model
- 3 lines of defence
- Demarcation of roles and responsibilities
- Independence and objectivity

4 Risk Management
- Identification
- Assessment
- Measurement
- Response & Mitigation
- Control & Monitor

5 Portfolio Review Optimisation and Pricing
- Risk approval & underwriting
- Risk return & optimisation

6 Contingency Planning and Resilience
- Contingency Planning
- Resilience testing
- Franchise protection

7 Risk Data Aggregation, Infrastructure and Reporting

- Board and management reporting
- Enterprise wide view & aggregation
- Common risk language/risk taxonomy
- BaU and stressed

1 Risk Governance	• Clear organisational structure and arrangements in place to ensure an effective and transparent delegation of authority from the Board to Senior Executives. • Risk management philosophy and risk principles (approved by the Board) are consistent with the vision, objectives and values of the Bank which places its shareholders, customers and regulators expectations at its heart. • Well defined triangulation process between the risk appetite, strategic, capital and funding planning process that aligns business objectives and range of implications for the risk profile and financial resources of the firm. • Established conduct related behaviors and values that are reinforced by performance appraisal methods and remuneration. Behaviours, incentives and values should emphasise the importance of the sustainability of the Bank and its business and respect for its stakeholders. • Clearly articulated Risk Appetite Statement that is integral to the bank's strategic objectives. • Identification of key risks through setting materiality thresholds (in context of earnings, funding, capital or other relevant factors). • ERM Framework and key risk policies are Board approved and are comprehensive and commensurate with the complexity and risk profile of the firm. Clear risk policy hierarchy and approval structure.
2 Risk Oversight and Control Function	• Mandate of the Risk Oversight and Control function and the role of the Chief Risk Officer are congruent. • Risk Oversight and Control function is independent, objective and sufficiently well resourced to oversee the ERM Framework; and possesses sufficient authority to offer robust challenge to the business.
3 Risk Operating Model	• The risk operating model (e.g. 3 Lines of Defence) is well defined and explicit in terms of both functional and individual roles, responsibilities and accountabilities that should be observed.
4 Risk Management	• Processes by which key risks are identified, measured, monitored, reported and mitigated, documented in formal risk policies, guidance and process notes.
5 Portfolio Review Optimisation and Pricing	• Clear policies on how risk taking decisions are made and approved through the application of a risk based pricing approach. • Portfolio quality and performance are reviewed periodically with emphasis on risk return trade off profile through the use of forward looking analysis.
6 Contingency Planning and Resilience	• Resilience testing performed to ensure appropriate contingency and recovery plans are in place for franchise protection and a resolution plan demonstrates the bank's resolvability without recourse to public funds.
7 Risk Data Aggregation, Infrastructure & Reporting	• Standard set of defined risk terminology applied throughout the Bank to enable consistent risk identification, understanding of risk, the development of risk policy and facilitates risk aggregation. • Clear data governance policy, including ownership of risk data and effective data quality management.