Job Title:	Senior Manager, Non-Financial Risk	**Reports to:**	Head of ERMC
Unit:	Enterprise Risk Management	**Division**	Enterprise Risk Management
Grade:	Band 6 – Senior Manager	**Date:**	
Job holder:		**Supervisor:**	Head of Enterprise Risk Management
Signature:		**Signature:**	

Job Purpose Statement
To lead independent second-line oversight of the Bank's non-financial risks, with operational risk as the primary focus, including transaction execution, third-party and fraud risk oversight. The role establishes and embeds risk and control assessment, incident and loss management, GRC data governance, key risk indicators, business continuity and operational resilience, while challenging first-line control owners and reporting material exposures, trends and actions to Management and the Board. It coordinates specialist oversight of ICT, cyber, third-party, conduct, reputational, sustainability, legal and regulatory risks without displacing the mandates of Technology, Information Security, Compliance or Legal.

Key Result Areas		
Perspective	**% Weighting** *(to add up to 100%)*	**Output**
Financial	15%	**Fraud and Transaction Execution Risk** • Act as the primary Non-Financial Risk partner for fraud oversight across products, business units and channels; challenge fraud trends, typologies, preventive and detective controls, incident handling, recovery and recurrence prevention. • Review controls over transaction initiation, authorisation, processing, settlement and reconciliation; challenge maker-checker failures, payment exceptions, reversals, breaks and customer impact. • Use incident and loss data, control testing and fraud intelligence to drive proactive control improvements with first-line business, Operations and Fraud Risk owners.
Customer	15%	**Business Advisory and Stakeholder Reporting** • Provide independent risk opinions on new products, digital channels, projects and material changes before approval and during post-implementation review.

		• Participate in product, technology, outsourcing and change governance, advising on material non-financial risks before decisions are taken. • Produce monthly management and quarterly Board reports covering trend analysis, material incidents and losses, RCSA outcomes, resilience testing, control effectiveness, appetite breaches, risk outlook and decisions required. **Reputational and Conduct Risk** • Assess reputational and conduct exposures arising from incidents, customer outcomes, partner conduct, complaints and public communications, and coordinate mitigation with the relevant owners.
Internal business processes	60%	**Operational Risk Framework, Challenge and Appetite** • Implement the Operational Risk Management Framework, taxonomy, standards and oversight plan. • Independently challenge first-line risk ownership and control effectiveness across people, processes, systems and external events. • Assess operational, third-party, fraud and transaction execution exposures against policy and approved appetite; challenge risk acceptance, exceptions and overdue remediation, and escalate material gaps through delegated governance. • Maintain policies, KRIs, control standards, appetite thresholds, incident logs, risk acceptances and action trackers, and recommend enhancements to the ERMF and relevant policies. **RCSA and Control Effectiveness** • Lead annual and event-driven RCSA reviews across branches, business and support functions; challenge process maps, inherent and residual risk ratings, control design, operating evidence and accountable owners. • Conduct thematic reviews and proportionate second-line control testing; compare RCSA results with incidents, losses, complaints, audit findings and KRIs, and verify the quality of remediation evidence. • Require reassessment after material incidents, process changes, new products or regulatory developments. **Risk Monitoring, Incidents and GRC** • Oversee timely capture of incidents and near misses, loss measurement, classification, escalation, root-cause analysis, lessons learned and corrective action; coordinate regulatory notifications with Compliance where required. • Monitor and calibrate KRIs and control indicators for errors, fraud, outages, third-party failures, complaints

		and overdue issues; analyse emerging threats and industry developments to recommend timely interventions. • Own functional governance of the GRC platform (risk and control records, workflows, user access, data quality, reconciliations, audit trails and dashboards), while IT retains technical administration. • Escalate severe incidents, persistent control failures and overdue high-risk actions promptly; support regulatory examinations, audit requests and verified remediation evidence. **Third-Party Risk Management** • Oversee adherence to the Third-Party Risk Management Framework across selection, due diligence, approval, contracting, onboarding, monitoring, renewal and exit. • Independently review material vendors and intra-group services for service, cyber, data, concentration, subcontracting and resilience risk; challenge control evidence, performance, contingency and exit plans. • Identify themes across third-party engagements and escalate material weaknesses or dependency concentrations to the relevant risk and outsourcing governance forums. **BCM and Operational Resilience** • Oversee business impact analyses, critical services, dependencies, recovery objectives, crisis plans and alignment of business continuity with disaster recovery and third-party arrangements. • Challenge tabletop, alternate-site, DRS and end-to-end test results; track gaps to closure and escalate critical services at risk of exceeding approved disruption tolerances. • Advise during disruptions and oversee post-incident reviews while business and technology owners execute response and recovery. **ICT, Cyber, Data and Change Risk** • Challenge specialist assessments of technology availability, access, change, vulnerabilities, cyber response, data integrity, privacy and digital-channel resilience, without assuming technical control ownership. • Provide independent risk challenge on AI use cases, automation and significant technology or process changes; track material control gaps and risk acceptances.

		Sustainability, Legal and Regulatory Risk Interfaces • Integrate material environmental, social and climate-related non-financial exposures into RCSA, third-party reviews, scenarios and risk reporting with the Sustainability owner. • With Legal and Compliance, assess the operational implications of litigation, regulatory change, breaches and obligations, and track implementation by accountable owners while those functions retain their specialist mandates.
Learning and growth	10%	**Risk Culture and Capability** • Build risk culture and technical capability across the first and second lines. • Coach first-line risk champions and deliver targeted RCSA, incident reporting, GRC and continuity training to risk champions and management; test awareness and improve guidance from feedback. • Maintain professional competence in operational risk, resilience, technology, sustainability and relevant regulatory developments, and coach team members where assigned.
Total	**100%**	

Job Dimensions

Reporting Relationships: jobs that report to this position directly and indirectly	
Direct Reports	• As per approved structure
Indirect Reports	Risk champions and designated first-line coordinators (functional coordination only)

Stakeholder Management: key stakeholders that the position holder will need to liaise/work with to be successful in this role.	
Internal • All business units and branches • Operations, Technology and Information Security • Legal, Compliance and Sustainability • Procurement and Human Resources • Internal Audit and Group Risk • Crisis and governance committees	External • BNR and other regulators (as delegated) • Critical service providers and the GRC vendor • External auditors • Relevant industry bodies

Decision Making Authority /Mandates/Constraints: the decisions the position holder is empowered to make *(Indicate if it is Operational, Managerial or Strategic)*
Set the risk oversight work plan and RCSA/GRC standards within approved policy (Managerial). Request evidence and challenge first-line assessments, controls, risk acceptances and remediation; recommend conditions, escalation or restriction of activities outside appetite. Escalate material incidents and breaches immediately through approved channels. Formal business decisions, risk acceptance and policy approval remain with delegated authorities.

Work cycle and impact: time horizon and nature of impact (Planning) *(e.g. Less than 1 week, 2 weeks, 2 weeks – 1 month, 1month – 3 months, 3-6 months, 6-12 months, above 1 year)*
Daily to weekly: incident triage, appetite breaches, critical KRI and GRC exception monitoring. **Monthly to quarterly:** RCSA reviews, thematic testing, resilience exercises, governance reports and action follow-up. **Annual and forward-looking:** framework refresh, risk appetite calibration, operational risk scenarios, BCM programme and emerging-risk assessment. Impact spans customer outcomes, resilience, regulatory standing, financial loss and reputation.

Ideal Job Specifications
Academic: • Bachelor's degree in risk management, business, finance, law, information systems, engineering or a related discipline; a postgraduate qualification is an advantage. **Professional:** • Relevant credentials such as CRM, CERM, CRISC, CISA, CBCI, ISO 22301 or ISO 27001 are an advantage. • Proficiency with Excel, PowerPoint, data analysis and GRC dashboards; able to turn complex risk data into clear management decisions. **Desired work experience:** • At least 6–8 years of relevant banking or financial-services experience, including 3–5 years in operational/non-financial risk, controls, BCM, technology risk, compliance or audit; experience leading cross-functional work preferred. • Demonstrated experience in RCSA review, incident and loss management, GRC tools, KRIs, issue remediation, BCM testing and Management/Board reporting. • Working knowledge of the three lines of defence and applicable BNR requirements.

Technical Competencies	
Operational Risk and Controls	Expertise in RCSA, risk and control taxonomy, control testing, incidents, losses, KRIs, root causes, risk appetite, GRC data quality and effective second-line challenge.
Resilience and Technology	Working knowledge of BCM, BIA, critical services, DRS, cyber/ICT, data, outsourcing, digital change and incident coordination; collaborates effectively with technical control owners.
Leadership and Commercial Acumen	Balances practical risk advice with independent judgement, influences senior stakeholders, reports to committees, coaches risk champions and understands commercial banking operations.

Behavioural Competencies	
Emotional Intelligence	Maintains independence and composure under pressure; recognises bias and challenges respectfully with evidence.
Social and Cross-cultural Awareness	Works across functions and cultures, listens to customers and colleagues, and communicates risk clearly and ethically.
Agile	Responds quickly to emerging risk, learns from incidents, adapts assessments to change and follows actions to closure.

This JD is signed-off with reference having been made to the organisation's core values and aligned competencies against these values.