Job Title:	IT Governance and Compliance Analyst	**Reports to:**	Manager, Governor and Compliance
Department/ Sub-department:	Information Security, Information Technology	**Division:**	Technology & Operations
Grade:	Band 3	**Date:**	
Job holder:		**Supervisor:**	
Signature:		**Signature:**	

Job Purpose Statement
The IT Governance and Compliance Analyst is responsible for ensuring the effective and efficient management of IT risks and controls within the bank by developing, implementing, and maintaining a robust IT governance framework. This includes aligning IT with business objectives, ensuring compliance with relevant regulations and industry standards, and mitigating cybersecurity risks to protect organizational assets and maintain operational integrity.

Key Results Areas		
Perspective	**% Weighting** *(to add up to 100%)*	**Output**
Governance Framework	10%	1. Develop and implement a comprehensive IT governance framework that aligns with business strategy, risk appetite, and regulatory requirements. 2. Define and articulate the bank's IT governance principles, policies, and procedures. 3. Oversee the implementation of IT governance best practices, including COBIT, NIST, PCI DSS, ISO 27001, and ISO 31000.
Compliance Management	10%	1. Monitor and ensure compliance with applicable cybersecurity frameworks, regulatory requirements, and internal security policies. 2. Lead the preparation for and execution of cybersecurity audits and assessments. 3. Maintain up-to-date knowledge of current and emerging cybersecurity regulations and standards.
Risk Management	40%	1. Lead and conduct comprehensive risk assessments including threat modelling, vulnerability scans, penetration testing, and business impact analyses. 2. Develop and maintain a comprehensive Risk Register, documenting all identified risks, their likelihood and impact, and the chosen risk treatment strategies. 3. Develop and implement risk mitigation plans in collaboration with the relevant stakeholders 4. Monitor and track key risk indicators (KRIs) and key performance indicators (KPIs) related to IT risk.

		5. Conduct regular risk reviews and updates to ensure the accuracy and completeness of risk assessments. 6. Develop and implement a risk-based approach to decision-making across all IT-related activities.
Training & Awareness	30%	1. Conduct IT governance, risk management and cybersecurity training and awareness programs for employees to ensure compliance with policies and procedures. 2. Provide guidance to IT on regulatory and compliance matters, supporting a culture of compliance.
Continuous Improvement	10%	1. Develop tactical governance and compliance reports for highlighting key metrics and risk insights. 2. Champion a culture of continuous improvement by driving secure systems, a resilient workforce, and informed decision-making.

Job Dimensions

Reporting Relationships: jobs that report to this position directly and indirectly	
Direct Reports	None
Indirect Reports	None

Stakeholder Management: key stakeholders that the position holder will need to liaise/work with to be successful in this role.	
Internal IT Department Enterprise & Compliance Risk Department Internal Audit	**External** External Auditors Regulators

Decision Making Authority /Mandates/Constraints: the decisions the position holder is empowered to make *(Indicate if it is Operational, Managerial or Strategic)*.
Operational –procedures and policy maintenance and implementation, audit management and planning

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)*
6-12 months

Ideal Person Specifications
1. Bachelor's degree in Cybersecurity, Information Technology, Business, or related field. 2. Relevant professional certifications such as CISA, CISM, CRISC, CGEIT, or ISO 27001 are highly preferred. 3. Proven experience in cybersecurity governance, risk management, and compliance (minimum 3-5 years). 4. In-depth knowledge of cybersecurity standards and frameworks (e.g., NIST, ISO 27001, PCI-DSS, GDPR).

Ideal Person Specifications
5. Familiarity with regulatory requirements and the ability to interpret and implement compliance standards. 6. Proven experience in conducting threat modelling exercises, vulnerability assessments, and business impact analyses. 7. Strong understanding of risk management methodologies and frameworks. 8. Strong analytical, problem-solving, and communication skills. 9. Ability to work collaboratively across teams and present complex information to non-technical stakeholders. 10. Knowledge of cloud security and privacy compliance. 11. Familiarity with data protection and privacy laws.

Behavioural Competencies
1. Strong attention to detail and organizational skills. 2. Ability to work independently and manage multiple tasks simultaneously. 3. Strong interpersonal skills and the ability to collaborate effectively with teams at all levels.

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