Job Title:	Cybersecurity Assurance Specialist	**Reports to:**	Snr. Manager, Cybersecurity Assurance
Department/ Sub-department:	Information Technology	**Division:**	Technology & Operations
Grade:	Band 5	**Date:**	
Job holder:		**Supervisor:**	
Signature:		**Signature:**	

Job Purpose Statement
The Cybersecurity Assurance Specialist role will be responsible for conducting General IT Controls (GITC) assessments within production systems. This proactive role aims to audit production environments before compliance teams flag potential issues, ensuring vulnerabilities, gaps, and misconfigurations are identified and remediated. The primary focus will be on auditing critical IT controls and configurations to maintain and enhance the organization's security posture. For issues that cannot be immediately addressed, the role will ensure they are properly documented in the Risk Control Self-Assessment (RCSA) for further remediation and mitigation.

Key Accountabilities (Duties and Responsibilities)		
Perspective	**% Weighting** *(to add up to 100%)*	**Output**
Proactive GITC Auditing and Vulnerability Identification	30%	• Conduct regular audits of production systems to assess GITC and identify gaps in configurations, security controls, and vulnerabilities. • Perform a thorough review of access controls, system configurations, data integrity, and compliance with internal policies and industry standards. • Identify security risks and proactively recommend appropriate remediation actions to mitigate threats.
Risk Control Self-Assessment (RCSA) Documentation	30%	• Work closely with Governance and Compliance teams to document key findings in the RCSA. • For any gaps or issues that cannot be immediately resolved, ensure they are properly recorded and tracked in the RCSA, with clear action plans for resolution. • Continuously review and update the RCSA to reflect the current security and compliance posture of production systems.
Collaboration and Reporting	20%	• Provide regular reports and recommendations to management and stakeholders on the status of audits, security risks, and remediation efforts. • Collaborate with internal teams such as the IT, security, and operations teams to ensure that

		gaps are effectively closed and issues are remediated in a timely manner. • Support ongoing compliance initiatives by providing insights into security vulnerabilities and assisting with external audits.
Support and Continuous Improvement	20%	• Assist in the preparation and execution of internal penetration tests and security assessments. • Continuously assess and improve the current auditing and testing processes for efficiency and effectiveness. • Provide recommendations on tools, processes, and methodologies to enhance the security posture of production systems.

Job Dimensions

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

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

Decision Making Authority /Mandates/Constraints: the decisions the position holder is empowered to make *(Indicate if it is Operational, Managerial or Strategic). Please also highlight any budgetary control responsibility if applicable for the role.*
Operational Managerial

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 Job Specifications
• Minimum of 4 years of experience in IT auditing, specifically in GITC, vulnerability assessments, and security controls within production systems. • Strong knowledge of security frameworks, regulatory standards (ISO 27001, NIST, SOC 2, GDPR), and security testing tools.

Ideal Job Specifications
• Bachelor's degree in Cybersecurity, Information Technology, Computer Science, or related field; certifications such as CISA, CISSP, or CISM are preferred. • Experience as an IT Auditor in GITC, with expertise in auditing production systems, access controls, and the general audit lifecycle. • Strong attention to detail, communication skills, and ability to identify and resolve risks proactively. • Excellent analytical and problem-solving skills, with the ability to manage multiple audit tasks and collaborate with cross-functional teams.