Job Title:	Cloud &IOT Security Engineer	**Reports to:**	Senior Manager, Security Engineering
Department/ Sub-department:	Information Security, Information Technology	**Division:**	Technology & Operations
Grade:	Band 5	**Date:**	
Job holder:		**Supervisor:**	
Signature:		**Signature:**	

Job Purpose Statement
This role focuses on developing, implementing, and maintaining secure solutions for cloud infrastructures and Internet of Things (IoT) ecosystems. As a mid-level technical position, it plays a pivotal role in safeguarding the bank's cloud environments and IoT systems from evolving threats, ensuring robust security configurations, and facilitating seamless integration with organizational objectives.

Key Results Areas		
Perspective	**% Weighting** *(to add up to 100%)*	**Output**
Cloud & IOT Security	40%	• Assist in designing and deploying secure cloud architectures on platforms such as AWS & Azure • Implement and monitor foundational security measures, including Identity and Access Management (IAM), encryption, and network segmentation. • Support the integration of security tools, such as Cloud Security Posture Management (CSPM) and vulnerability scanners, into cloud environments. • Collaborate on the development of secure IoT systems by enforcing device authentication, secure communication protocols, and data protection strategies. • Identify and mitigate security risks in IoT ecosystems, such as device vulnerabilities or insecure configurations. • Participate in the evaluation and implementation of IoT-specific security frameworks and standards.

Technical Advisory & Collaboration	20%	• Work with stakeholders to understand business requirements and translate them into technical security solutions. • Provide technical leadership in security incident response related to cloud or IoT systems. • Advise on regulatory and compliance requirements (e.g., GDPR, ISO 27001, NIST 800-53, and IoT-specific standards like ETSI EN 303 645)
Incidence Response and Threat Management	20%	• Support incident detection and response for cloud and IoT environments by analysing alerts and assisting with investigations. • Conduct vulnerability assessments and help remediate security findings. • Contribute to threat modelling exercises to identify and address potential attack vectors.
Ongoing Compliance and Audit Support	20%	• Work closely with the Governance, Risk, and Compliance (GRC) team to ensure adherence to regulatory requirements such as GDPR, ISO 27001, PCI DSS, NIST, and IoT-specific standards like ETSI EN 303 645. • Assist in preparing documentation and evidence for internal and external audits, including risk assessments, security configurations, and incident reports. • Ensure that all cloud and IoT security practices align with ongoing compliance audits and organizational policies. • Track remediation of findings from audits and ensure timely resolution of non-compliance issues.

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

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

Technical Competencies

- **Cloud Security**: Foundational knowledge of AWS, Azure, or GCP security services (e.g., AWS IAM, Azure Defender, GCP Security Command Center).
- **IoT Security**: Understanding of IoT communication protocols (MQTT, CoAP, HTTPS) and device security concepts.
- **Compliance**: Familiarity with frameworks such as GDPR, ISO 27001, PCI DSS, and NIST 800-53.
- **Tools**: Experience with security tools such as vulnerability scanners, SIEM, endpoint security solutions, and compliance platforms.

Certifications (Preferred):

- Cloud Security: AWS Certified Security Specialty, Azure Security Engineer Associate, or Google Professional Cloud Security Engineer.
- Cybersecurity: CompTIA Security+, Certified Ethical Hacker (CEH), or Cisco CyberOps Associate.
- Compliance: ISO 27001 Lead Implementer/Auditor, or other governance-related certifications.

Behavioural Competencies

- Strong analytical and problem-solving skills with a technical mind-set.
- A proactive approach to ensuring security and compliance in cloud and IoT environments.
- Effective communication and collaboration abilities, with a focus on teamwork.
- Commitment to continuous learning and professional growth.