Role Profile

Role Title	Level	Team	Function
Access Management Analyst		IFGL Technology	IT Security

Purpose of the Role
Reporting to the Head of IT Security, the Access Management Analyst will work closely with other members of the IT Security Team in enforcement of the IFGLs Information Security policies and standards. This role focuses on using the policies and standards for actionable for day-to-day operations, actively monitoring security systems to pre-empt potential threats, ensuring alignment with industry best practices and swift, proactive responses to any incidents. This Access Management Analyst role will support the Senior Security Engineers in maintaining a secure IT landscape while fostering a culture of vigilance and proactive risk mitigation.

Key Contribution Areas

Measures

Key Contribution Areas	Measures
Support the Implementation of Information Security Policies	Collaborate with the IT Security Team in areas to include: • Contribution to periodic reviews by providing research or findings related to evolving risks and technologies. • Gather feedback on policy requirements understanding and their practical implications within specific operational areas. • Contribution towards proposed solutions or actions addressing identified non-compliance issues at the operational level. • Assist in updating and maintaining policy documentation accessible to staff, ensuring ease of access and understanding.
Access Management	Collaborate with the IT Security Team in areas to include: • Assist in maintaining the Access Control Framework by contributing to policy and guideline documentation within designated areas. • Aid in defining roles, permissions, and access levels aligned with business needs under guidance. • Support the JML process by aiding in ensuring timely provisioning, modification, or revocation of access rights. • Assist in documentation and coordination related to staff changes affecting access privileges. • Assist in enforcing the Principle of Least Privilege by contributing to access reviews and adjustments under guidance. • Aid in aligning access permissions with PoLP principles within designated responsibilities. • Support in conducting regular access reviews and audits, contributing to identifying and addressing access discrepancies. • Assist in utilising automated tools or mechanisms to facilitate periodic access reviews within specific operational domains.

Assist in the provision of Information Security training and awareness for colleagues across the Group	Collaborate with the IT Security Team in areas to include: • Aid in tailoring Information Security training programs for different departments and roles, contributing insights or research. • Assist in delivering Information Security training through diverse mediums or sessions, aiding in workshops, webinars, or course support. • Support in collecting participant feedback to evaluate the effectiveness of Information Security training programs. • Assist in implementing ongoing awareness campaigns or communication channels related to Information Security threats and best practices. • Support awareness sessions on Information Security matters across various levels within the organisation.
Support adherence with relevant Information Security Frameworks and Certifications	Collaborate with the IT Security Team in areas to include: • Contribution towards the establishment of processes to ensure ongoing alignment and compliance within designated areas. • Participation in documentation and audits to support the certification process and renewals under supervision. • Assist in conducting internal assessments or audits to evaluate adherence to Information Security Frameworks within specific operational domains. • Assist in staying updated with industry trends, best practices, and regulatory standards regarding Information Security Frameworks.
Collaborate on Network and Cloud Security Measures Assist in Implementing Security Measures within Networks and Cloud Environments	Collaborate with the IT Security Team in areas to include: • Assist in contributing to strategic plans by providing research or analysis related to security objectives in network and Cloud environments. • Support in documenting security architectures or building blocks for network and Cloud environments, under guidance. • Participation in monitoring compliance measures and supporting enforcement activities as directed. • Participation in drills or simulations to test the effectiveness of response plans within designated areas.

Assist in Risk Assessment Processes	Collaborate with the IT Security Team in areas to include: • Assist in contributing to the development of a standardised risk assessment framework by providing research or insights. • Contribution towards analysis or data gathering for risk assessment reports within specific operational domains. • Aid in organising and supporting regular vulnerability assessments and penetration testing activities under guidance. • Aid in prioritising and addressing high-risk vulnerabilities within assigned responsibilities. • Assist in contributing to the development and maintenance of incident response plans aligned with identified risks.

Functional or Technical Knowledge and Skills Required

- A Higher National Diploma in Computer Science, Information Security, or a related field, or equivalent hands-on experience. Preference given to those pursuing or holding advanced certifications like CISSP, CISM, or their equivalents.
- Minimum of 3+ years in roles focusing on network and/or Cloud security, showcasing a track record of increasing responsibility.
- Demonstrated expertise in devising and executing security solutions within network and Cloud environments.
- Familiarity with security frameworks like NIST and ISO27000 series, along with staying abreast of emerging security threats, trends, and technologies.
- A basic understanding of compliance and risk management
- Proficiency in network security protocols, Cloud security solutions (Azure/AWS/GCP), firewalls, intrusion detection systems, VPNs, etc.
- Competence in utilising vulnerability assessment tools, incident response frameworks, and methodologies for risk management.

Personal Capabilities Required, e.g. skills, attitude, strengths

- Strong analytical skills enabling the assessment of security risks and formulation of appropriate mitigation strategies.
- adept problem-solving capabilities
- Proficient in logical thinking and reasoning, capable of adapting swiftly to dynamic environments while effectively managing multiple priorities.
- Confident relationship management skills, at ease when engaging with stakeholders across various levels, including Executive and Board members.
- Good verbal and written communication abilities, adept at translating intricate technical subjects into language suited to the audience's comprehension level.

People, Budget and Project Scope

- Reports directly to the Head of IT Security within the Technology Department, working closely with the IT Security Team and other relevant departments.
- Operates within the corporate risk framework, ensuring alignment with the company's risk appetite and integrating security strategies that complement this framework.