JOB DESCRIPTION

Position Title: Head of Governance, Risk and Compliance (GRC), Info Sec – 12 Month FTC

Reports to: Global CISO

Location: London

Summary of Position:

This position will report directly to the global CISO and also be responsible for managing a small in-house team who plan, schedule, monitor and report on activities relating to information/cyber security. The role will work in collaboration with Information Technology, Group Risk and Compliance, HR, Facilities and a number of third parties.

Key Responsibilities & Accountabilities:

- Support the Global CISO in maintaining and realising the cyber security strategy
- Take overall responsibility of information security risk and compliance
- Assume responsibility for the BMS Information Security Control Framework
- Produce and maintain a the Information Security governance and oversight target operating model
- Produce policies and supporting governance material
- Take ownership for the Information Security Risk management processes
- Identify information security threats and work with technical teams to understand BMS exposure
- Provide specialist Information Security input to IT and business operations
- Ensure information security initiatives are up to date and security risks are identified and managed
- Investigate, analyse, and review Information Security breaches, including near misses, making recommendations for appropriate control improvements
- Build close relationships with key internal users, senior managers and external suppliers
- Coordinate security plans with third party vendors and ensure output from security services delivered by third parties is acted upon accordingly
- Responsible for management of cyber events, including notification, escalation, response and post incident review
- Adhere to company and regulatory policies, procedures together with mandatory training requirements.

Functional & Behavioural Competencies required:

- Proven leadership skills in a similar Information Security function
- Experience of naturing and retaining a talent
- Proven experience in information security
- Excellent writing and communication skills
- Proven experience in third party supplier and vendor selection and management
- Significant experience and success in managing multiple issues, problems and work streams with a clear ability to prioritise
- Good understanding of culture change techniques when implementing information security improvements
- Ability to consider the implications of process change and potential impact upon the strategies of the global business
- Ability to maintain the integrity of process and approach, as well as controls, for the whole incident management process including the ability to co-ordinate and manage major/highly sensitive investigations with potential for business wide impact/reputational damage

Information Security:

- Experience of managing information security services specifically in relation to service design and on-going management
- Experience developing and maintaining written security controls, compliance monitoring, and defining treatment strategies
- Experience of Information Security risk management concepts
- Experience of Information Security transformation programmes
- Experience of in building and support incident management frameworks.
- Experience of security frameworks such as NIST CSF/ISO-27001

- Personally demonstrate the five BMS values and ensure that team members are aligned with these:
    - Accountable
    - Entrepreneurial
    - Collaborative
    - Empowering
    - Disciplined