IT Risk Analyst

Job Description

Reporting To:	Information Security Manager
Responsibility for others:	None
Department:	Information Security
Location:	Horsham (Some travel to London and other UK sites may be required)
Hours of Work:	Monday to Friday 9.00am to 5.30pm with 1 hour for lunch

Overall Purpose of the Job:

To ensure that the Group's technology risks and controls are monitored and reported on a regular basis, maintain awareness of emerging risk and to ensure compliance with the Group's Risk Management within Group IT.

Key Activities & Responsibilities:

- Reviewing technology controls across the Benchmark group to identify potential vulnerabilities and weaknesses
- Conducting risk assessments for all new technology projects, applications and services, identifying risks and agreeing mitigation actions
- Documenting, defining and reporting on technology risk
- Working with Group Risk, to ensure technology risk and controls are aligned with regulatory and compliance requirements across the Benchmark group
- Ongoing review and monitoring of risk issues and actions
- Execution of control testing and validation of the risk/control indicators
- Maintaining awareness of emerging security risks and trends and raise awareness of risks where appropriate

Required Skills/Experience:

- Proven track record in technology risk identification and management
- Knowledge and experience of the wider and emerging technology space, such as infrastructure, database, networks, mobile device management and cloud technologies
- Experience of information risk governance and an understanding of risk analysis, management techniques and methodologies

- Strong analytical skills with the capability to assess the information provided, and provide clear and appropriate direction
- Excellent communication and reporting skills, including the ability to simplify complex technical information into clear executable Business intelligence
- Ability to build positive rapport and trust quickly
- Ability to communicate with stakeholders at all levels

Desirable Skills/Experience:

- Financial Services industry experience
- CISSP/CRISC Certification
- Working knowledge of the regulatory environment, information security best practices (ISO 27001:2013, NIST Cyber Security framework etc.)
- Excellent planning and organisational skills
- Ability to understand broader business issues
- Communication and presentation skills

Personal Characteristics:

The ideal candidate is:

- Energetic and motivated
- Calm under pressure
- Ability to work independently and as part of a team
- Able to gain buy-in and effective influencer

Due to the dynamic nature of the IT industry, it is also important for this person to be willing to expand their IT knowledge, and to upgrade their skill set as and when required.

Note: This description is not intended to cover all the duties of the role. Reasonable additional duties may be assigned or duties may be reassigned at any time and at the discretion of management