Role definition

Job title:	Information Security Analyst		
Initial reporting line:	Head Information Security & Compliance		
Direct reports:	N/A		
Business unit:	Group IS	Base Location:	Stratford upon on Avon, Salford Quays, Tamworth or Rugby

Summary

The Information Security Analyst supports the Head of Information Security & Compliance in maintaining and enhancing the Group's Information Security position against agreed levels, through the effective use of existing security tools and features, assessing and implementing new technology, and the policing and auditing of compliance with ongoing training, awareness and education for the user base.

The key deliverables of the role are:

- Provide frontline support for information security queries from the company's internal and external stakeholders
- Monitor access, internally and externally, to IT systems and critical data stores
- Monitor and review external threat feeds and undertake appropriate remediation activities
- Monitor and maintain the information security systems within the Group
- Investigate the causes of information security incidents and provide recommendations to the Head Information Security & Compliance for remediation and prevention of recurrence
- Respond to information security incidents, as directed by the Head Information Security & Compliance
- Support the Asset and Compliance officer with an internal auditing programme, liaising with external consultants as directed by the Head Information Security & Compliance to determine the effectiveness and compliance with the Group's policies.
- Review and propose improvements to the Group's policies, procedures, training materials and guidance relating to the Group's information security arrangements

Additionally the role will assist in

- Providing recommendations to the Head of Information Security on how the information security arrangements of the Business can be improved
- Performing security risk assessments of information systems and data flows, document findings and prioritise remediation plans in line with organisational agreed risk appetite
- Conducting vulnerability and risk assessments of IT components, produce recommendations for improvement and communicate these to internal stakeholders
- Assessing and advising internal stakeholders on information security risk for new systems and applications and changes to systems and applications
- Conducting audits of information security controls and practices and measure and report on performance and risk, including third party suppliers
- Providing support for internal investigation, E-Discovery, HR and legal teams support and assistance
- Implementing the Group's policies, procedures, training materials and Information Security awareness programmes

The role requires a highly accurate and focussed approach to support the business's collaborative approach across the IT community. A high level of personal integrity and discretion is mandatory.

Key objectives *(4 maximum)*

- **Operational** – To ensure the business is making best use of its existing Information security tools and services
- **Innovation –** To take advantage of new Information Security software tools and to develop processes to maintain and enhance the Group's security posture including the management of our IT assets and license estate
- **Budgetary** – To ensure the Information security function delivers value from security investment
- **Securing the Group** – to assist in maintaining the security of the business and promoting secure practices through continual training and improved information security awareness

Principal responsibilities and accountabilities

- Create value metrics in the Group's security position
- Monitor and continually enhance the Group's security position through effective use of existing toolsets
- Ensuring our business data is secure by ensuring hardware assets such as laptops and tablets are tracked
- Ensure systems updates and patch management are effectively controlled either via internal teams or third party contracts
- Input into bi-annual security risk assessments and refresh activity across all divisions
- Delivery of IT (Shared) Information Security management processes to all divisions.
- Travel to business locations (UK-wide) to monitor security position and security compliance
- Work with local business teams and HR teams to ensure assets are returned for reallocation
- Travel to business locations (UK-wide) to promote information Security awareness
- Work with Head of Information Security & Compliance to maintain and enhance the Group's Security position
- Work with current high security framework security controllers to maintain the Group's high security framework contracts and frameworks
- Obtain and maintain personal MOD security clearance

Person specification

Qualifications and training

- A minimum of 5 years' experience in a customer facing IT technical or support role
- Some relevant experience in Information Security
- Industry recognised security qualification or evidence of formal training leading to certification

Technical skills and experience

- Background in an IT customer facing role, ideally a technology or service arena
- Excellent stakeholder management and ability to communicate at all levels
- A good understanding of security principles and experience of delivering this through a combination of internal and external suppliers
- Excellent communicator with an aptitude to communicate at both a technical and business level
- A good overall knowledge of Information security principles
- Willingness to undertake training for security accreditations and associated certifications