Role definition

Job title:	Security Operations Team Leader		
Initial reporting line:	Head of Information Security and Compliance		
Direct reports:	Junior Information Security Analyst and Information Security Analyst		
Business unit:	Group IT	Base Location:	Rugby

Many of our staff work flexibly, and in many different ways – remote working, part-time, time to do the school run – please talk to us on application or during the interview process about the flexibility you need. We can't promise to give you exactly what you want, but we are happy to explore what is possible for the role.

Summary

Supporting the Head of Information Security & Compliance, you will lead the operations team members in ensuring that assets are appropriately secured, and the Group's Information Security posture position is maintained against agreed levels.

The main focus of the role is protecting data processed and systems managed by the Company (or approved partners) from threats to data confidentiality, integrity or availability and acting as the lead subject matter expert on security threats and counter-measures. We employ a wide variety of platforms, systems and controls to protect data and you will ensure that these controls remain effective and efficient. This includes assisting in the selection of new technologies working in partnership with the wider IT function.

You need an accurate and focussed approach with an eye for detail to support the businesses collaborative approach across the IT community.

Key objectives

- **Operational** – To lead a team focussed on ensuring the business is appropriately protected against threats to Information Security.
- **Innovation –** To assist in identifying opportunities to improve our current Information Security policies and controls including taking advantage of new tools and technologies as well as developing or improving processes.
- **Budgetary** – To ensure the Information Security Function delivers value from the 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.

Role definition

Principal responsibilities and accountabilities

- Monitor and work with our outsourced SOC to maintain the company security controls to agreed operational tempo. Take appropriate remedial steps if controls are identified to be ineffective or at risk of failure
- Attend service reviews to ensure all third party services continue to perform and deliver as expected against SLAs and KPIs. Drive performance improvements across all service contracts including selection of new or replacement service partners
- Monitor and continually enhance the group data protection through effective use of existing toolsets
- Ensure our business data is secure by identifying opportunities for technical and procedural improvement and creating business cases as required
- Input into bi-annual security risk assessments refresh activity across all divisions
- Input into the design and strategy process to ensure that the group continues to develop its maturity relating to data security and compliance
- Deliver Information Security management processes to all divisions and liaise with the technical control owners in different teams to ensure a coordinated approach to Information Security
- Travel to business locations (UK-wide) to monitor security posture and compliance, and promote awareness.
- Support high security Framework security controllers to maintain the companies' security framework contracts
- Be the technical point of contact for information security queries, changes and projects from the company's internal and external stakeholders, and ensure existing security controls remain effective and fit for purpose
- Manage information security incidents and investigations, as directed by the Head Information Security & Compliance. Identify areas of improvement within our incident detection and response processes
- Lead the investigation of phishing and scam alerts, threat intelligence, patch and antivirus monitoring/ reporting, monitor access internally and externally to IT systems and critical data stores.
- Support the Compliance Manager with internal auditing programme, internal investigation, E-Discovery, Subject Access Requests, and HR and legal teams support and assistance

Person specification

Qualifications and training

- Experience in a customer-facing IT technical or support role.
- Industry recognised security qualification of evidence of formal training leading to certification
- The ability to attain and maintain an HMG/MOD security clearance is mandatory

Technical skills and experience

- Background in an IT customer-facing role, ideally a technology or service arena
- Technical understanding of current security threats and controls including process and technical solutions
- Experience with Microsoft products and technologies.
- Experience in operational aspects of information security (threat hunting, vulnerability monitoring, remediation)
- Working knowledge of ISO27001 or other security frameworks (Cyber Essentials, NIST)
- Excellent communicator with an aptitude to communicate at both a technical and business level
- Willingness to undertake training for security accreditations and associated certifications
- Knowledge and understating of Information Security, Risk Management and Data Protection Legislation is desired.
- A high level or personal integrity and discretion is mandatory.