Role definition

Job title:	Cyber Security Implementation Manager		
Initial reporting line:	Head of Information Security and Compliance		
Direct reports:	none		
Business unit:	Group IS	Base Location:	Rugby with travel as required

Summary

The Cyber Security Implementation Manager role exists to support the Head of Information Security & Compliance and team members in ensuring that new systems processing or protecting information assets are appropriately identified, configured, and documented. By doing so they assist in maintaining the Group's Information Security posture position to agreed levels.

The main focus of the role is ensuring a smooth, consistent process for the implementation of new technology aligning to our secure by design and private by design standards. The postholder acts as the point of contact between the various IT functions across all Morgan Sindall Group companies and the security function ensuring that we have appropriate technical designs and risk assessments in place for all projects. This includes ensuring alignment with our accreditations (Cyber Essentials, ISO27001, Secure By Design etc) and that appropriate security monitoring & documentation is in place where required.

The Group has an outsourced documentation partner delivering our digital twin model for security and wider infrastructure and the postholder manages the delivery of this service for the security based components. The post holder also acts as an assurer for the consistency of the wider documentation pack.

The Cyber Security Implementation Manager is the de facto problem manager for security escalations and is expected to manage small projcts where the Cyber Security function is bringing new processes, products or services into production.

The key deliverables of the role are:

- Provide and deliver a single point of contact with processes for the safe onboarding of new technology into the Group. This includes attending monthly PMO meetings, running the technology onboarding process (acceptance into service), coordinating queries, and assuring / reviewing the security designs of IT / digital projects from across the Group
- Ensure the accurate configuration and updates to the security documentation packs included in the Groups digital twin
- Review and assure other components of the digital twin and liaise with service owners if quality issues are identified
- Identify opportunities for improvement for both technical and procedural control sets
- Liaise with technical control (service) owners in different teams to ensure a coordinated approach to project onboarding and service transition
- Take ownership of any problem tickets raised on security projects or controls and coordinate their resolution within the security team
- Collate and duplicate findings from audits, scans and penetration tests into a single source of truth to be shared with service owners so risk based approach to mitigation can be implemented
- Support information security incidents and investigations, as directed by the Head Information Security & Compliance.
- Input into the wider design and strategy process to ensure that the Group continues to develop their maturity relating to data security and compliance
- Act as a security business partner and ambassador across the Morgan Sindall Group of companies to assist our colleagues in delivering secure solutions to business problems

The role requires a focus on detail and appropriate levels of procedure and documentation alongside the relationship management of a wide range of stakeholders. The ability to engage openly with internal and external stakeholders in order to drive mutually successful outcomes is critical. A high level or personal integrity and discretion is mandatory as is the ability to attain and maintain an HMG security clearance. A knowledge and understating of Information Security, Risk Management and Data Protection Legislation is essential

Key objectives *(4 maximum)*

- **Operational** – To ensure new projects are brought into service with an appropriate level of due diligence aligned with secure by design and privacy by design.

- **Innovation –** To identify 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 accuracy of documentation packs, good service transition and management of problems.

Principal responsibilities and accountabilities

- Ensure new projects are risk assessed and brought into service with appropriate review and controls
- Manage our digital twin security documentation and ensure it is updated and accurate
- Ensuring our security controls and outcomes are maintained by identifying and resolving problems
- Input into security risk assessments across all divisions
- Coordination with key stakeholders to ensure visibility of technology change and risk management
- Work across our decentralised businesses with local IT and digital teams to ensure new projects are implemented with appropriate security designs aligned to our security frameworks
- Work as part of the Group Cyber Security and Data Protection team to maintain and enhance the groups Security position
- Work with current Framework and Project Security Controllers to maintain the companies' security framework contracts
- Obtain and maintain personal HMG security clearance.

Person specification

Qualifications and training

- A minimum of 5 years' experience in a customer facing IS technical or support role.
- Industry recognised security qualification of evidence of formal training leading to certification

Technical skills and experience

- Background in an Information Security role, we are not looking for a pure technical 'hands on' engineer but a generalist who has an ability to communicate effectively at both a technical and business level
- Strong 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)
- Good working knowledge of ISO27001 or other Security frameworks (Cyber Essentials, NIST CSF)
- Willingness to undertake training for security accreditations and associated certifications