Role Title	**Security & Resilience Manager**
Reports to	Director of Security & Risk Management
Directly Supervises	N/A
Total team size	4

Role Purpose

The **Security & Resilience Manager** leads the Security & Resilience team in Group Services, ensuring technology services are deployed, and operated in a secure and resilient manner. Working closely with infrastructure, applications, data, architecture, security operations, and risk teams, the manager provides technical leadership, assurance, and governance across projects, operational changes, and strategic initiatives. The role oversees security reviews, resilience assessments, standards compliance, and continuous improvement activities while acting as a senior technical SME. The role requires a hands-on leader to manage priorities and contributes directly to the successful delivery of security and resilience outcomes.

Associated British Foods plc | Group Services

Security & Risk Management

Key Accountabilities:

- Manage the workload and demand for security input for the team in an agile (kanban) driven format. Manage daily stand-ups ensuring all workload (including forward planning) is allocated, delivered to a high standard, on time and within budget via the security and resilience team, leveraging assistance from the SOC L3 team where required.
- Provide weekly updates on progress, issues, blockers and risks and to the Director of Security and Risk, and monthly updates to the Group Services SLT.
- Manage the performance of the Security and Resilience team, including year performance appraisals, and providing mentoring and support for team members.

In addition to the management responsibilities, the Security and Resilience Manager is also a key member of the team, delivering the same security and resilience outcomes as the rest of the team, including but not limited to;

- Collaborate with wider security teams (SOC, Engineering, Architecture) and business units to and stakeholders to provide expert security advice and drive secure outcomes.
- Assess, design, and recommend security controls across hybrid Azure / AD environments
- Lead or contribute to complex security consultancy engagements across multiple projects and domains
- Identify security risks and define actionable remediation plans to improve overall security posture
- Support cloud security initiatives (Identity, Access Management, Conditional Access, Zero Trust, etc.)
- Drive continuous improvement of security services, tooling, and consultancy approaches

Essential Skills, Knowledge & Experience:

- Strong experience in hybrid Azure / Active Directory environments, including identity security and access control
- Proven ability to advise on security controls within large, complex organisations
- Solid understanding of security frameworks and best practices (e.g. ISO 27001, NIST, CIS)
- Experience improving organisational security posture through risk-based approaches
- Strong knowledge of modern security concepts (Zero Trust, identity-first security, cloud security)
- Ability to clearly communicate complex technical concepts to varied audiences
- Demonstrated ability to influence stakeholders across all levels without formal authority
- Self-motivated, proactive, and comfortable working independently with minimal
- Strong collaboration and stakeholder management skills
- Ability to manage multiple priorities and deliver at pace
- The ability to produce clear, concise, and actionable reports, recommendations, and advice, translating complex technical and security risks into meaningful business insights for stakeholders at all levels.

The successful candidate will be able to apply this knowledge pragmatically to improve organisational security, resilience, and risk management outcomes.

Desirable Skills, Knowledge & Experience:

- Industry certifications (e.g. CISSP, CISM, AZ-500, SC-100, CRISC)
- Experience with Azure security services (Defender, Sentinel, Entra ID)
- Threat modelling and risk assessment
- Security architecture or design
- Penetration testing or threat hunting
- Understanding of Cyber Threat Intelligence principles
- Experience working in consulting or customer-facing roles

Other requirements of the role:

- Must be a self-starter, able to take ownership and drive initiatives independently
- Comfortable working in a fast-paced, evolving environment
- Strong problem-solving and decision-making
- Excellent interpersonal, written, and verbal communication skills
- Willingness to travel occasionally as required
- Flexible/hybrid working model