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

Role Purpose

The **Security & Resilience Lead** works closely with engineering, operations, project, and architecture teams, leading reviews of changes, designs, configurations, and technology implementations to ensure compliance with security standards, reference architectures, and security frameworks. The role identifies risks, delivers technical reviews, supports secure change, and drives resilience improvements across infrastructure, applications, cloud platforms, and end-user services. The role requires a proactive, technically capable individual who can deliver at pace.

Associated British Foods plc | Group Services

Security & Risk Management

Key Accountabilities:

- 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