Function:	Information Security Analyst	Role Holder:	TBC
Reporting Lines:	Information Security Manager	Base Location:	Lancashire Insurance Services Limited: London, UK

1.   Purpose

Information security is an essential function at Lancashire and so is committed to its continuous improvement; the addition of this role is an important element in achieving its security objectives during Lancashire's time of digital transformation and growth.

Reporting to the Information Security Manager, the post holder will be responsible for evaluating cyber security controls, conducting risk assessments and collaborating with cross-functional teams. The post holder will support the Information Security Manager in maintaining all aspects of information security risk management including responding to security inquiries and incidents, maintaining cyber security governance, and ensuring compliance with relevant regulatory requirements.

2.   Responsibilities

- Support the Information Security Manager in delivering the Information Security Management System and to drive continuous improvement for information security.
- Evaluate and assess cyber security controls across the business and its third party vendors to ensure compliance with the NIST Cyber Security Framework (CSF).
- Conduct comprehensive risk assessments using the NIST CSF.
- Use risk management techniques to identify cyber threats, risks and issues in a timely manner.
- Support, develop and conduct third-party vendor security assurance activities.
- Collaborate with cross-functional teams to develop and implement risk management activities.
- Respond to security support tickets and other enquiries; providing information security support and escalation.
- Support the creation and collection of metrics, validation of security control performance and the identification of emerging cyber risks.
- Collaborate with the Enterprise Risk Management (ERM) team to maintain, develop and deliver cyber risk reporting and appetite statements.
- Maintain Information Security policy and procedure ensuring content is relevant to the current cyber threat landscape.
- Maintain, develop and test the Cyber Incident Response Plan, ensuring content is relevant to the current cyber threat landscape.
- Monitor, maintain and manage Lancashire compliance with its relevant cyber security regulation obligations.
- Manage actions and output generated by stakeholder engagements; for example customers, regulators, internal and external auditors.
- Maintain currency with emerging security trends, threat intelligence, industry standards and good practice, and security enhancing technologies.

3. Essential Skills, Knowledge & Experience

- Sound knowledge of and experience in an Information Security role.
- Experience working in a professional or financial services environment
- Hands-on experience conducting cyber risk assessments and developing cyber risk mitigation strategies.
- Hands-on experience conducting cyber security control assessments, and developing and maintain cyber risk reporting and risk appetite statements.
- Hands-on knowledge and experience working with recognised security frameworks such as, NIST CSF, ISO27001 etc.
- Hands-on experience managing and maintaining cybersecurity compliance with regulatory frameworks such as FCA, PRA, NYDFS etc.
- Experience developing a governance framework by maintaining policy and procedure.
- Ability to achieve against agreed deadlines.
- Ability to work both independently and collaboratively.
- Strong interpersonal and communication skills (written and verbal), with the ability to interact with technical and non-technical stakeholders at all levels.
- Strong analytical, problem-solving, organisation and planning skills.
- A pro-active and enthusiastic approach.
- Knowledge of Microsoft systems (on-premise and Azure cloud), technologies, infrastructure, awareness of systems management and operational support tools.
- Acknowledges and responds positively to exceptional events in information security to meet the objectives of the business.