

JOB DESCRIPTION

Job Title:	Date & Version Control
	Date:
Technology Risk Oversight Manager	July 2024
Reports to:	Version:
Chief Risk Officer	1.1
Direct Reports:	Produced by:
None	Chief Risk Officer

Job Purpose & Scope

To support the business in delivering its IT & cyber security strategy by providing independent oversight and assurance in respect of the management of the associated risk & control environment, particularly in the context of BAU activity, change initiatives, business continuity, supplier management and operational resilience.

Duties and Key Responsibilities

Main areas of work

1. Develop, maintain and execute a second line oversight plan to assess the design and operating effectiveness of Society controls for managing risks around information security, information technology, change management, third-party supplier management & operational resilience.
2. Conduct risk assessments of IT systems, processes, and infrastructure to identify vulnerabilities and potential threats, and to ensure compliance with the Society's Information Technology related suite of policies.
3. Support the first line in assessing the effectiveness of IT related outsourcing and supplier arrangements.
4. Conduct third party audits alongside first line colleagues
5. Influence first line to ensure that technology risks are identified, managed, and reported through governance as appropriate.
6. Provide oversight and question with regard to all change initiatives that touch on IS, IT & Operational Resilience risk.
7. Provide a self-sustaining, second line view on IT & IS related incidents to the Operational Resilience Forum and oversee resolution.
8. Review and question first line Risk & Control Self-Assessment submissions and key control testing.
9. Maintain a detailed understanding of all IS, IT, third-party supplier management and operational resilience risk related regulation and industry best practice to provide guidance, support and question to senior management with regard to the impacts on the Society.
10. Working collaboratively with Internal Audit to strengthen technology risk management practices for the benefit of the Society.
11. Provide holiday cover for Risk and Compliance colleagues as required.
12. Undertake any other duties as may reasonably be required.

Conduct Rules

All employees are expected to act in accordance with the PRA and FCA Conduct Rules:

- You must act with integrity
- You must act with due skill, care and diligence
- You must be open and co-operative with the FCA, the PRA and other regulators
- You must pay due regard to the interests of customers and treat them fairly
- You must observe proper standards of market conduct
- You must act to deliver good outcomes for retail customers

Financial Crime

All employees are expected to:

- Be aware of their personal legal obligations and the legal obligations of the Society in relation to Financial Crime
- Be aware of the Society's Anti-Money Laundering systems and controls and follow the Society's procedures
- Be alert for anything suspicious in respect of money laundering or fraud and report any suspicions in line with internal procedures
- Do not discuss any suspicions with anyone outside of the Society and do not 'tip off' a customer or prejudice an investigation

Person Specification

Qualifications & Knowledge	<p>Essential:</p> <ul style="list-style-type: none"> • Excellent understanding of IT Operations including ITIL and IT security best practice. • Understanding of Cyber security frameworks such as NIST • Thorough working knowledge of the basics of operational risk management, including RCSA and key control testing. • CISSP qualification or similar experience. • Knowledge and experience of ISO 27001/2 • Understanding of operational resilience and the techniques to manage this risk. <p>Regulatory Knowledge:</p> <ul style="list-style-type: none"> • Data Protection Act • GDPR
Experience	<ul style="list-style-type: none"> • Experience of planning and undertaking deep dive thematic reviews. • Experience of managing or providing assurance over the management of technology related risks. • Experience of interpreting regulations
Skills & Abilities	<ul style="list-style-type: none"> • Excellent written and oral communication skills. • Excellent time management, planning and organisational skills are essential. • The ability to build lasting working relationships, manage stakeholders work collaboratively and influence others, while maintaining second line independence. • Excellent PC skills with knowledge of Word, PowerPoint, Outlook and Excel is essential. • Logical thinking is regularly required to resolve queries raised by colleagues.
Other Requirements	<ul style="list-style-type: none"> • Self-motivated, flexible with the ability to meet tight deadlines and manage multiple deliverables. • Ongoing necessity to keep abreast of risk management developments and industry trends.