Job Description – Operational Resilience Officer

Department	Operational Delivery Team
Grade	14
Reporting to	Head of Information Security & ODT Governance
Direct reports (yes or no)	No
WTW Code	AFY635-P4-14

Job Purpose

- The Chief Risk Officer (CRO) is responsible for and owns the ongoing development of the Operational Resilience Framework. The Chief Operating Officer (COO) is responsible for the implementation and embedding of the Operational Resilience Framework within MIB.
- This role is to support the COO with implementation and embedding of the framework within MIB.

Key Accountabilities

- Operational Resilience Frameworks: Support initial implementation of the framework throughout its programme phase.
- Under BAU, support business adherence to the Operational Resilience Framework, through testing, oversight and continuous improvement, ensuring alignment with industry standards and any applicable regulations. Continuously assess and recommend refinements to the framework to address evolving risks and the regulatory environment where applicable to MIB.
- Compliance and Reporting: Ensure strict adherence to all operational resilience-related regulations and standards. Prepare detailed reports for senior management and regulatory bodies if applicable, documenting compliance and recommending improvements.
- Collaboration: Partner with internal departments to embed resilience considerations into every function and cultivate strong relationships with external partners to enable coordinated resilience strategies.
- Risk Management: Participate in the identification, evaluation, and mitigation of operational and business risks. Develop and monitor mitigation strategies, adjusting as needed to address new and emerging threats.
- If applicable, Lead, Coordinate and Deliver the annual PS21/3 Self-Assessment, including drafting submissions, engaging collaborators and supporting all related Executive and Board Reporting.

Key Accountabilities

- If applicable, as part of the annual PS21/3 Self-Assessment exercise, partner with the business, technical and operational teams, providing guidance and challenge to ensure Regulatory Compliance across both Technical and non-technical resilience domains.

Role requirements

- Strategic vision and foresight to anticipate challenges and develop long-term resilience plans.
- Strong personal leadership, communication and stakeholder management skills that underpin scenario testing ownership, Important Business Services oversight, Dependency mapping governance, Third party resilience oversight, ExCo and Board metrics, reporting and governance and leading post incident learning reviews.
- Ability to maintain composure and effectiveness while managing crises or working under pressure.
- Proficiency in multitasking and prioritising responsibilities to align with strategic goals.
- Comprehensive knowledge of operational resilience frameworks and best practices.
- Expertise in crisis management and stakeholder communication during incident response.
- Advanced skill in developing and delivering impactful training programs that prioritise organisational readiness.
- Thorough understanding of regulatory requirements and reporting best practices.
- Superior collaboration and relationship-building skills with both internal and external stakeholders.
- High competency in risk identification, assessment, and mitigation.
- Significant experience in same or similar role.