Job Description – Business Continuity Manager

Department	ODT
Work level	3
Reporting to	Head of Organisational Resilience
Direct reports (yes or no)	No

Job purpose

The Business Continuity Planning Manager is responsible for developing, embedding, testing, and continuously improving MIB's enterprise-wide business continuity capability. The role will work across all MIB business areas to ensure critical customer, claimant, member, operational, data, technology, supplier, and corporate services can continue during disruption and recover within agreed business tolerances. The postholder will coordinate activity across business functions, Technology, Risk, Compliance, Legal, Procurement, Finance, HR, Facilities, Communications, Information Security, Data Protection, Service Management, and third-party partners to build a practical, organisation-wide, audit-ready continuity framework.

Key accountabilities

- **Enterprise continuity framework:** Own and maintain MIB's Business Continuity Management framework, including policies, standards, templates, governance, assurance, and continuous improvement across the whole organisation.
- **ISO 22301 accreditation:** Lead MIB's activity to achieve and maintain accreditation to ISO 22301, coordinating evidence, controls, governance, assurance activity, stakeholder engagement, and continuous improvement across the organisation.
- **Business Impact Analysis:** Lead regular Business Impact Analysis activity across MIB business areas to identify critical services, priority activities, customer and stakeholder impacts, dependencies, recovery requirements, and acceptable disruption tolerances.
- **Business continuity planning:** Develop, review, and maintain continuity plans for critical MIB teams, business processes, premises, suppliers, technology dependencies, people requirements, data flows, and operational services.
- **Operational resilience alignment:** Alongside other colleagues in the Organisational Resilience team, work with Risk, Compliance, Technology, Service Management, Information Security,

Key accountabilities

Data Protection, and all business owners to ensure continuity arrangements support MIB's operational resilience, audit, regulatory, and customer service obligations.

- **Technology and disaster recovery alignment:** Partner with Technology and Service Management teams to ensure IT disaster recovery plans, recovery time objectives, recovery point objectives, backup arrangements, infrastructure resilience, and supplier recovery plans align with business needs.
- **Incident and crisis response:** Support MIB's response to major incidents and disruptive events by coordinating continuity activity, escalation routes, decision logs, communications, situation reporting, recovery priorities, and lessons learned.
- **Testing and exercising:** Design and deliver an annual enterprise-wide testing programme, including business area tests, tabletop exercises, scenario simulations, call-tree tests, crisis exercises, supplier exercises, and post-exercise improvement reviews.
- **Governance and reporting:** Produce regular reports for senior leadership, risk committees, audit forums, operational governance meetings, and relevant executive stakeholders, highlighting continuity maturity, risks, gaps, dependencies, actions, and progress.
- **Third-party continuity:** Assess continuity arrangements for critical suppliers and service partners, working with Procurement, Legal, contract owners, Technology, and business teams to ensure appropriate resilience, recovery, notification, and communication requirements are in place.
- **Risk, control, and audit evidence:** Maintain continuity risks, issues, control evidence, improvement plans, and action tracking, ensuring clear ownership, realistic timelines, and audit-ready documentation.
- **Training and awareness:** Build business-wide awareness of continuity responsibilities through briefings, playbooks, guidance, role-specific training, and practical support for plan owners and response teams.
- **Continuous improvement:** Capture lessons from incidents, exercises, audits, supplier reviews, and near misses, and drive corrective actions through to completion across MIB business areas.

Essential Experience

- Proven experience in business continuity, operational resilience, risk management, crisis management, disaster recovery, or a closely related discipline within a complex business environment.
- Experience leading Business Impact Analysis activity across multiple departments and translating findings into practical continuity plans, recovery strategies, and executive-level reporting.
- Experience designing and running business continuity tests, crisis exercises, simulations, supplier exercises, and post-exercise improvement plans.

- Strong understanding of operational dependencies across business processes, people, technology, suppliers, data, premises, customer service, regulatory obligations, and external stakeholders.
- Experience working with senior leaders, business owners, risk committees, audit teams, technology teams, operational teams, and third-party suppliers.
- Experience maintaining evidence, documentation, governance reporting, and improvement plans suitable for audit, regulatory, and executive review.
- Experience supporting or leading ISO 22301 accreditation, certification readiness, external assessment, or equivalent business continuity management system assurance activity.
- Experience embedding business continuity as a business-owned capability rather than a purely technology-led process.

Skills and Competencies

- Strong knowledge of business continuity lifecycle activities, including analysis, design, implementation, validation, embedding, and improvement.
- Understanding of ISO 22301 principles and good practice approaches to continuity and resilience management.
- Ability to define and challenge recovery time objectives, recovery point objectives, maximum tolerable periods of disruption, and minimum business continuity objectives.
- Excellent stakeholder management and influencing skills, with the ability to secure action from teams that do not directly report to the role.
- Strong written communication skills, including the ability to produce clear plans, reports, briefings, playbooks, and executive summaries.
- Analytical and structured approach to risk assessment, dependency mapping, gap analysis, and prioritisation.
- Calm and organised under pressure, with the ability to coordinate activity during live incidents or time-critical situations.
- Strong attention to detail and commitment to maintaining accurate, accessible, and audit-ready documentation.

Qualifications and Professional Memberships

- Business Continuity Institute qualification or membership, such as CBCI, MBCI, or equivalent, is desirable.
- Certification or training in ISO 22301, operational resilience, risk management, crisis management, IT service continuity, or disaster recovery is desirable.
- ITIL, risk management, project management, cyber resilience, or service management qualifications would be beneficial.
- Relevant degree or equivalent professional experience in risk, technology, operations, resilience, security, or business management.

Measures of Success

- Business Impact Analyses and continuity plans are current, complete, accessible, and reviewed on schedule across all priority MIB business areas.
- Critical MIB services have clearly defined recovery requirements, ownership, dependencies, escalation routes, and tested continuity arrangements.
- Business and technology continuity requirements are aligned, with clear linkage between business priorities, supplier arrangements, and disaster recovery capability.
- Continuity testing is completed in line with the agreed annual enterprise schedule, with lessons learned documented, owned, and tracked to closure.
- Senior leadership has clear visibility of continuity risks, gaps, dependencies, maturity, and remediation progress across MIB.
- Audit, risk, resilience, and assurance findings relating to continuity are addressed with clear evidence and sustainable control improvements.
- MIB's ISO 22301 accreditation plan is clearly owned, progressed against agreed milestones, supported by evidence, and embedded into ongoing governance and continuous improvement activity.
- Business areas understand their continuity responsibilities and are confident in invoking plans during disruption.

Personal Attributes

- Pragmatic, outcome-focused, and able to balance good practice with operational reality.
- Confident working across business and technology teams to resolve ambiguity and drive ownership.
- Resilient, calm, and credible during incidents, exercises, and challenging stakeholder conversations.
- Collaborative and service-minded, with a focus on enabling the business rather than creating process for its own sake.
- Curious and improvement-focused, using evidence, testing, and lessons learned to strengthen resilience over time.