

Role Profile

Role Title	Level	Team	Function
Business Continuity Analyst		IFGL Technology	IT Operations

Purpose of the Role
The Business Continuity Analyst will be responsible for developing, implementing, co-ordinating and maintaining comprehensive business continuity and disaster recovery plans to ensure the resilience and continuity of the IFGL organisation operations in the event of an unforeseen disruption. Working closely with the IT Resilience Analyst, and IFGL business units, the role will involve assessing risk, designing recovery strategies, to mitigate potential impacts, customer detriment and minimize downtime.

Key Contribution Areas	Measures
Risk Assessments Business Impact Risk Assessment – (BIRA)	<ul style="list-style-type: none"> Working with all business units, identify and assess any potential risks and vulnerabilities that could disrupt business operations, including natural disaster, cyber threats, pandemics, reduction in staff, failure of key third party providers, and other emergencies.
Business Impact Analysis	<ul style="list-style-type: none"> Using the information collected during the completion of the BIRA, determine the potential effects of various disruptive scenarios on the organisations operations, financial stability and reputation
Plan Development	<ul style="list-style-type: none"> Working with all business units, develop and document detailed business continuity plans, outlining procedures and protocols for responding to, and recovering from disruption. Working with the IT Resilience Analyst develop and document detailed IT disaster recovery plans outlining procedures and protocols for responding to, and recovering from disruptions.
Implementation and Testing	<ul style="list-style-type: none"> Working with relevant stakeholders to implement and regularly test, demonstrate and record, the effectiveness of business continuity planning, ensuring that they align with industry best practices and regulatory requirements for the jurisdictions IFGL operates in.
Training and Awareness	<ul style="list-style-type: none"> Collaborate with the various business units to raise awareness of business continuity protocols and provide training to ensure staff understand their roles and responsibilities in the event of a crisis.
Continuous Improvement	<ul style="list-style-type: none"> Monitor and review existing business continuity plans, identify areas for improvements and make recommendations for enhancing the organisations resilience to potential threats. Horizon scanning any analysis to business continuity regulations relevant in our various jurisdictions.
Communication and Coordination	<ul style="list-style-type: none"> Establish communication channels and coordinate with internal and external stakeholders (in conjunction with the Vendor Managers) to ensure a coordinated response to disruptions, including maintaining relationships with external partners and emergency services.

Business Incident Management	<ul style="list-style-type: none"> Working closely with the Head of Operations help develop and implement a business incident management framework to dovetail with the IT Major Incident Management framework. This should include BIRA, BCP and the Organisations Incident Management Control Team
Response Co-ordination	<ul style="list-style-type: none"> Under direction of the Head of Operations be a point of contact during incidents, assisting with communications and actions Liaise closely with the IT Major Incident Management taking into account the type of incident and who will lead etc. Collaborate with relevant departments to ensure a swift and effective response to incidents. Support the Head of Operations in the co-ordination of the incident response team, ensuring adherence to established protocols.
Post Incident Reviews	<ul style="list-style-type: none"> With the exception of IT related incidents, ensure post incident reviews involving stakeholders from across the organisation. Following review, produce a detailed report, including action and recommendations. Ensure all actions and recommendations are completed and introduced as appropriate.

Functional or Technical Knowledge and Skills Required

- Professional certifications in business continuity management is desirable (e.g. MBCI).
- Proven experience in business continuity, disaster recovery, or risk management, preferably in a regulated financial services environment, minimum of 3 years is desirable.
- Strong analytical and problem-solving skills, with the ability to conduct risk assessments and business impact analyses, and able to proficiently analyse incidents, identifying root causes and implementing corrective actions.
- Technical Knowledge in relation to IT systems, cybersecurity and business continuity planning
- Knowledge of relevant regulations, standards and best practices in business continuity and disaster recovery planning for an international savings, protection and pensions market.

Personal Capabilities Required, e.g. skills, attitude, strengths

- Takes initiative to identify and address potential issues before they escalate
- Detail orientated with a strong understanding of business operations.
- Excellent communications skills, both written and verbal – be able to work and modify communication style as appropriate when dealing with members of staff from across the organisation at all levels and in different locations.
- Adaptable, be able to adapt quickly to evolving incidents and changing business environments.
- A good listener, who has the ability to understand information provided and identify what is important.
- Strong understanding of business operations and a commitment to ensure the organisation's resilience in the face of potential disruptions.
- Resilient, maintains composure under pressure and can effectively manage stressful situations.

People, Budget and Project Scope

- Reports to the Head of IT Operations
- Works closely with the IT Resilience Analyst, Vendor Management and representatives from across the organisation