Clear.Bank

Business Continuity and Operational Resilience

Angela Candlin-Evans, Head of Business Continuity and Resilience - 2026





Introduction

At ClearBank we are committed to providing excellent service and support to our customers and partners. At the heart of that approach is ensuring we protect our stakeholders and minimise any unexpected interruption to our services.

We recognise that unexpected events may affect the way we operate, and we accept our responsibility to customers and partners to continue providing our services to the best of our ability.

To meet this obligation to our customers, partners, our employees and the communities we operate in, we aim to implement both Operational Resilience and Business Continuity Management as a good management practice that adds value and goes beyond our regulatory requirements. We believe that these practices not only makes us more resilient as a company, but also helps to continually examine and evaluate our key business processes and practices, increasing our efficiency and innovation.

At ClearBank we are ISO22301 accredited. This means we are certified at the highest level in Business Continuity. We also have a dedicated Business Continuity and Operational Resilience team, keeping us up to date and accountable for our overall resilience.

Business Continuity

We consider business continuity to be a fundamental embedded business process. That's why we are ISO22301 certified and maintain our high certification standard with regular external audits.

We have a structured and centrally managed Business Continuity Management Programme that encompasses both business continuity planning and crisis management and follows the industry standard Business Continuity Management lifecycle.

We've developed an internal policy and maintain business continuity plans which provide not only effective responses to a wide variety of disruptive events but enables us to continue our critical functions and processes during an interruption to our normal business operations.

Business Impact Analyses (BIA's) for all departments help us to determine our critical processes and what factors contribute to enable these to operate effectively. These include technology, interdependencies, inputs and outputs, regulatory obligations, and a threat assessment.

Annual testing takes place to ensure our plans are fit for purpose with the results documented in reports with action owners and deadlines to strengthen our plans for all scenarios.

We prepare for



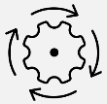
Loss of People



Premises disruption



Technology outages and total loss



Key Supplier disruption



Cyber disruption



Crisis Management invocation

Operational Resilience

Operational resilience can be defined as the ability of firms – and the financial system as a whole– to prevent, adapt, respond to, recover, and learn from operational disruption to achieve the prevention of harm to the consumer and ensure financial stability.

The FCA and PRA take an increasingly proactive role in challenging the operational resilience of a wide range of firms, including banks, insurers, and payment services firms, requiring clear demonstration of their protection against incidents. These firms need to identify their important business services and what controls they have in place to manage them. When these controls start to fail, firms need to advise the regulator straight away.

At ClearBank we have clearly defined [customer centric] Important Business Services, with each of those having an impact tolerance agreed by our Board. These are tracked constantly, ensuring the relevant areas of our business comply with the regulation at all times. In conjunction with our severe but plausible testing scenarios we ensure ClearBank's operational resilience is robust.

We have an experienced and dedicated Head of Business Continuity and Operational Resilience with a dedicated team overseeing and managing all of our operational resilience obligations.

Important Business Services

These are defined as any service to one or more clients which, if disrupted, could:

- cause intolerable levels of harm to one or more of the firm's clients, or
- pose a risk to the soundness, stability or resilience of the UK financial system.
- All banks, building societies, designated investment firms, insurance firms, e-money and payment services firms need to be able to identify their important business services. They must have indicators in place to identify when there is an increased risk of the firm being unable to perform these services, and to report this to the regulator.

Disaster Recovery

Disaster recovery testing is an essential part of ClearBank's operational resilience framework.
The objective is to demonstrate the ability of the technical team to recover services in the event of a disaster, implementing any improvements and lessons learnt identified during the testing. This testing ensures that the respective teams are familiar with the processes and, more importantly, confident in their capabilities in an actual disaster scenario.

ClearBank performs disaster recovery testing annually in line with our policy. during which we simulate faults in every internal connection alongside testing for:

- data centre network failover (annually);
- backup and restore (regularly);
- zone failure and regional failures availability; and
- restoration from backups.

Our applications and core banking systems are hosted on multiple nodes within MS Azure on a high availability cluster across 3 sites and can tolerate multiple node failures without causing interruption to payment flows.
ClearBank's MS Azure Private Infrastructure connects to data centres via redundant active-active express route connections.
Our aim is to ensure our technology has high availability, high resilience with a 99.7% uptime SLA which is against the API availability 24/7 -365 days a year.