Business Continuity Management System Policy

Access Bank (SL) Ltd is committed to ensuring the resilience and continuity of its operations, services, and critical business functions in the face of disruptive incidents, in accordance with applicable laws, regulatory requirements, and international best practices, including ISO 22301:2019.

Business continuity is recognized as a vital component of our operational integrity, customer trust, and long-term sustainability.

To this end, the Bank's management is committed to ensuring that:

- All business continuity policies, plans, and procedures are developed and managed centrally by the Business Continuity Management (BCM) function, under the leadership of the Risk Management Unit, and aligned with the enterprise-wide governance framework.
- All staff, including third-party service providers and key business partners, are made aware of their roles in business continuity and receive periodic training to strengthen preparedness, recovery competence, and response capability.
- The Bank maintains full compliance with all relevant legal, regulatory, and contractual obligations related to business continuity, including directives from the Bank of Sierra Leone and industry standards such as ISO 22301.
- Business Continuity Management System (BCMS) objectives are defined, measurable, monitored, and supported with adequate resources to ensure timely recovery of critical operations and minimal impact to stakeholders.
- Continual improvement is embedded into the BCMS through structured activities such as regular business impact analyses (BIAs), risk assessments, testing and simulation exercises, post-incident reviews, internal audits, and management reviews.

Business Continuity Management Objectives

- Ensure 100% readiness of critical business functions by conducting quarterly business continuity risk assessments, ensuring that these functions can be restored within agreed Recovery Time Objectives (RTO) to minimize operational disruptions and support uninterrupted service delivery.
- Maintain 99.9% uptime of critical banking systems and services annually by testing and updating disaster recovery plans (DRPs) to ensure timely recovery from major incidents, ensuring minimal disruption to customers
- Ensure 99% availability of mission-critical services and applications through continuous monitoring, risk mitigation strategies, and implementing robust business continuity plans that guarantee business operations during unforeseen events
- Achieve 100% compliance with business continuity-related regulatory and legal requirements, including ISO 22301 and applicable national regulations, ensuring the Bank is legally prepared to handle major disruptions without risk to customers or stakeholders
- Conduct at least one full-scale disaster recovery test annually to ensure recovery strategies are effective, involving all critical business units and vendors to simulate a real-world event, assessing the performance of the BCMS.
- Achieve 90% participation in business continuity training and awareness programs for employees and third parties, ensuring that staff is adequately prepared to respond to and manage crises, minimizing human error in recovery efforts.
- Review and update the BCMS plan at least annually or following significant business or operational changes, ensuring the continuity plans remain relevant to new risks, technological advancements, and regulatory changes.