Development Bank of Nigeria

Integrated Management System (ISO 27001:2022, ISO 22301:2019 & ISO 20000:2018)

At the Development Bank of Nigeria (DBN), we are committed to upholding international standards to enhance operational efficiency, protect information assets, ensure business continuity, and deliver high-quality IT services. Our Integrated Management System (IMS) aligns with the principles of ISO 27001:2022, ISO 22301:2019, and ISO 20000:2018.

Information Security Management System (ISO 27001:2022)

Policies

- DBN will protect the confidentiality, integrity, and availability of all information assets.
- Access to information and systems will be based on business need and least privilege.
- All employees and contractors will be aware of and comply with information security requirements.
- DBN will implement risk-based controls to mitigate information security threats.
- Information security incidents will be reported, investigated, and resolved in a timely manner.
- The ISMS will be continually improved to respond to changes in technology, regulation, and threats.

Objectives

- Maintain zero major information security breaches annually.
- Ensure 100% of staff complete annual information security awareness training.
- Achieve closure of 95% of identified ISMS-related corrective actions within 90 days.
- Conduct Bi-annual vulnerability assessments and annual penetration testing.
- Ensure access reviews for critical systems are conducted quarterly.
- Perform annual ISMS internal audit and management review to confirm effectiveness.

Business Continuity Management System (ISO 22301:2019)

Policies

- DBN will ensure the continuity of critical business functions during and after any disruptive incident.
- A risk-based approach will be applied to identify and mitigate potential business disruptions.
- All critical functions will have documented and tested Business Continuity and Disaster Recovery Plans.
- The BCMS will be integrated with risk management and information security processes.
- The Bank will train staff and create awareness on their roles during business disruptions.
- BCMS effectiveness will be reviewed and improved continuously to ensure resilience.

Objectives

- Conduct annual Business Impact Analysis (BIA) for all critical functions.
- Test 100% of critical business continuity and disaster recovery plans at least once per year.
- Ensure recovery of critical IT systems within approved RTOs and RPOs.
- Achieve closure of all BCMS corrective actions within 30 days of identification.
- Maintain zero downtime exceeding RTO limits for critical systems annually.
- Conduct annual BCM training and simulation exercises with participation from all key departments.

Service Management System (ISO 20000:2018)

Policies

- DBN will deliver reliable, efficient, and customer-focused IT and business services aligned with ISO 20000-1.
- All services will be governed by defined SLAs and performance targets.
- Incidents and service requests will be managed to ensure timely resolution.
- Continuous service monitoring and reporting will be performed to support improvement.
- Customer and stakeholder feedback will be reviewed regularly to improve service quality.

- The SMS will be reviewed and improved periodically to ensure continued alignment with business goals.

Objectives

- Maintain service availability of at least 98% for all critical IT services.
- Resolve 90% of incidents within agreed SLA timeframes.
- Achieve at least 90% customer satisfaction in annual service performance surveys.
- Conduct quarterly service performance reviews and trend analysis.
- Complete 100% of change requests following the approved change management process.
- Perform annual internal audits and management reviews to assess SMS effectiveness.

Leadership Commitment and Policy Review

Our leadership team is fully committed to the implementation, maintenance, and continual improvement of the Integrated Management System. This policy is:

- Communicated to all employees and made accessible to interested parties.
- Reviewed periodically to ensure its relevance, effectiveness, and alignment with organizational goals.