May 2026

INTERNAL

Business Continuity, Contingency Management, and ICT Security Measures Attestation

FUNDS AXIS

Date:	May 2026
Attested by:	Trevor Dempster, Chief Information Security Officer (CISO)
Company:	Funds-Axis Limited
Office Location:	60 Cannon Street, London, EC4N 6NP, United Kingdom
Certifications:	ISO/IEC 27001:2022, ISO 9001:2015
Frameworks:	DORA, NIS2, GDPR, UK DPA 2018

1. Executive Summary

Funds-Axis Limited confirms its commitment to maintaining robust business continuity, contingency management, and ICT security practices in accordance with Good Industry Practice and Applicable Laws, including the Digital Operational Resilience Act (DORA), GDPR, and ISO 27001.

This attestation outlines the measures in place to ensure service continuity, data protection, and regulatory compliance for all services provided to our customers.

2. Attestation Statement

Funds-Axis certifies that:

- It has implemented and regularly tests appropriate **Business Continuity and Contingency Management Plans**.
- These plans are aligned with **Good Industry Practice**, ISO 27001, and DORA requirements.
- Documentary evidence of such plans and associated testing is available to Customers upon request.
- It has implemented **ICT security measures, tools, and policies** that provide an appropriate level of protection for the provision of services to Customers.
- These measures are aligned with **Applicable Laws and regulatory requirements**, including GDPR, UK DPA 2018, and DORA.

3. Business Continuity & Disaster Recovery Overview

- **Policy Framework:** Funds-Axis maintains a formal BCP & DR Policy (Ref: A1.8), reviewed annually.
- **Testing Programme:**
  - Six-monthly recovery drills
  - Annual alternative working tests

- Telecoms failure simulations

- **Recovery Objectives:**
  - RTO: <3 hours
  - RPO: <12 hours
- **Governance:** Overseen by the ISO, with board-level visibility and reporting.

4. ICT Security Framework

Funds-Axis maintains a layered security architecture including:

- **Encryption:**
  - AES-256 at rest
  - TLS 1.2+ in transit
  - BitLocker on endpoints
- **Access Controls:**
  - Role-based access
  - Multi-Factor Authentication (MFA)
  - VPN and IP restrictions
- **Monitoring & Detection:**
  - Sumo Logic, Defender, AWS CloudWatch, etc
  - Automated alerts and anomaly detection
- **Policies & Procedures:**
  - Password Protection Policy
  - Device Management Policy
  - Web Filtering and DLP
  - Incident Management Policy
- **Compliance Tools:**
  - Monthly control testing
  - Internal audits
  - Supplier SLAs and BCP reviews

5. Governance and Compliance

- **Certifications:**
  - ISO/IEC 27001:2022 – Information Security Management
  - ISO 9001:2015 – Quality Management
- **Legal Compliance:**
  - GDPR
  - UK Data Protection Act 2018
  - Digital Operational Resilience Act (DORA)
- **Oversight:**
  - CISO-led programme
  - Monthly board reporting

- Annual staff training and declarations

6. Appendices

- A1.8 Business Continuity & Disaster Recovery Plan
- High-Level Summary of BCP Testing - March 2026
- A1.01 Cyber Security Policy Part 1
- A1.02 Cyber Security Policy Part 2
- Threat Intelligence Policy
- Incident Management Policy
- Compliance Report on Digital Operational Resilience