

COMPLIANCE

INTERNAL

# Funds-Axis Compliance Report on Digital Operational Resilience

FUNDS  AXIS

Contents

What is DORA? .....3

Why DORA Matters .....3

What DORA will mean for Funds-Axis .....3

DORA Attestation .....4

Our Existing Preparedness and the Impact of DORA .....5

Appendix 1: Funds-Axis DORA Preparedness .....6

Appendix 2: DORA Control Testing and Results .....12

Appendix 3: Supporting Documentation .....14

Glossary.....16

**Confidentiality & Disclaimer:**

This documents and its contents are strictly confidential and intended solely for the use of the recipient. If you are not the intended recipient, you must not copy the document or contents, or use them for any purpose or disclose their contents to any other person. Funds-Axis Limited accepts no liability for any damage caused by reliance on the contents of this document.

This document is for informational purposes only. While every effort has been made to ensure its accuracy, Funds-Axis assumes no liability for any losses, damages, or claims resulting directly or indirectly from the Customer's non-compliance with DORA.

Version: 1.0

Date: 16<sup>th</sup> January 2025

## What is DORA?

The Digital Operational Resilience Act (DORA), passed by the European Union in November 2022, represents a significant regulatory shift aimed at enhancing the operational resilience of financial entities in an increasingly digitalised environment. Set to apply from January 2025, DORA mandates a robust framework to protect, detect, contain, recover, and repair capabilities against ICT-related incidents.

DORA (Regulation (EU) 2022/2554) addresses the need for comprehensive operational resilience in financial institutions, extending beyond traditional capital allocation for risk management.

The regulation aims to mitigate systemic ICT risks, minimise disruptions, and enhance the stability of the EU financial system. It sets uniform requirements concerning the security of network and information systems supporting the business processes of financial entities.

Key components include:

- \ **ICT Risk Management**
- \ **ICT Incident Management**
- \ **ICT Business Continuity Management BCM**
- \ **ICT Third-Party Risk Management**
- \ **Information and Intelligence Sharing on Cyber Threats**

As regards ICT Third-Party Risk management, our Customers will need to categorise their service providers as either Critical ICT Third-Party Providers (CTTPs) or Non-critical ICT Third-Party Providers.

## Why DORA Matters

As financial services become increasingly digitalised, the potential for ICT incidents grows, posing significant risks to the entire financial system. DORA provides a unified regulatory framework to ensure financial institutions are resilient against such risks, thereby:

- \ Enhancing the overall security posture of the EU financial sector
- \ Harmonising ICT risk management regulations across EU member states
- \ Promoting innovation in ICT security and resilience

## What DORA will mean for Funds-Axis

We should expect significant engagement from our customers to provide them with the relevant assurances they need to satisfy their obligations in respect of DORA. We need to be able to provide this assurance concisely and promptly.

We expect that most customers will classify us as **Non-critical ICT Third-Party Providers**. However, we should expect that customers will state that they expect us to meet the same

standards as if we were CTTs. This means our customers will expect:

- \ A robust ICT risk management framework
- \ Comprehensive business continuity and disaster recovery plans
- \ Strong cybersecurity measures
- \ Regular risk assessments and testing
- \ Clear communication and incident reporting channels
- \ Compliance with data protection regulations
- \ Transparent subcontracting arrangements
- \ Regular audits and evidence of resilience and security practices
- \ Clear exit strategies in case of service termination

## DORA Attestation

### Purpose and Background

This attestation verifies and documents the controls and measures in place at Funds-Axis to comply with DORA requirements. The attestation was conducted following industry-standard frameworks and guidelines, including ISO 27001 and ISO 9001.

### Methodology and Control Environment

The attestation was conducted through:

- \ Interviews with key personnel
- \ Document reviews
- \ System tests
- \ Representative sampling of controls

Funds-Axis has established a robust control environment, including key policies, procedures, and governance structures to ensure compliance with DORA.

### Control Testing Results

The following control areas were tested and found to be effective:

Control Area	Control Tested	Result	Issues Identified
ICT Risk Management	Risk assessment and treatment plans	Effective	None
ICT Incident Management	Incident reporting mechanisms	Effective	None
ICT Business Continuity Management (BCM)	Business continuity and disaster recovery plans	Effective	None
ICT Third-Party Risk Management	Third-party risk assessments and monitoring	Effective	None
Information and Intelligence Sharing on Cyber Threats	Threat intelligence sharing processes	Effective	None

## Findings and Recommendations

The control testing did not identify any significant issues. All controls were found to be effective and in compliance with DORA requirements. It is recommended to continue maintaining and enhancing the current control environment and regularly review and update policies and procedures to address emerging threats and regulatory changes.

## Our Existing Preparedness and the Impact of DORA

In Appendix 1, we set out a summary of our response that can be provided to customers in respect of queries on our DORA preparedness.

## Appendix 1: Funds-Axis DORA Preparedness

### Responsibility

Our Chief Information Security Officer (CISO), Trevor Dempster (email: [trevor.dempster@funds-axis.com](mailto:trevor.dempster@funds-axis.com)), is responsible for overseeing the cybersecurity strategy, risk management, and compliance initiatives within the organisation. The CISO ensures that all security frameworks, including those necessary for DORA compliance, are robustly implemented and maintained. This includes conducting regular reviews of our policies, overseeing training initiatives, managing internal audits, and maintaining resilience across our systems and networks.

Please direct all queries related to our cybersecurity, data protection, and compliance framework to the CISO for guidance and further clarification.

### Our Situation Prior to DORA

Prior to DORA, we had already implemented:

- \ A robust ICT risk management framework
- \ Comprehensive business continuity and disaster recovery plans
- \ Strong cybersecurity measures and incident response procedures
- \ Regular risk assessments and vulnerability testing
- \ Clear communication channels for incident reporting
- \ Compliance with data protection regulations (e.g., GDPR)
- \ Regular audits and assessments of ICT resilience
- \ Transparency in operations and service delivery
- \ Ongoing staff training on ICT risks and security best practices

Our existing certifications include:

- \ **ISO 27001:** Information Security Management
- \ **ISO 9001:** Quality Management Systems

We also maintain the following as part of ISO and Operational Risk arrangements:

- \ **Risk Registers:** Comprehensive documentation of identified risks, including assessments of their potential impact, likelihood, and corresponding mitigation measures. This helps in effective risk monitoring and ensures alignment with our risk appetite.
- \ **PESTEL Analysis:** Regular evaluations of external factors (Political, Economic, Social, Technological, Environmental, and Legal) that may impact our organisation, enabling proactive response to emerging threats and opportunities.

- \\ **Asset Registers:** Detailed listing of all information assets, with ownership assignments and valuation assessments, to safeguard critical resources and ensure accountability.
- \\ **Incident Registers:** Centralised records of all security incidents, including their impact, response actions, and post-incident reviews, to facilitate continuous improvement.
- \\ **Audit Registers:** Tracking of all internal and external audit findings, non-conformities, and the corrective actions taken, ensuring accountability and transparency in our compliance efforts.
- \\ **Training Registers:** Documentation of employee training, including session topics, attendance records, and completion dates, to demonstrate our commitment to staff competency in security and compliance.
- \\ **Compliance Registers:** Records of legal, regulatory, and contractual compliance requirements, along with documentation of compliance status, ensuring comprehensive regulatory adherence.
- \\ **Supplier Registers:** Listing of all third-party suppliers, including risk assessments and performance evaluations, to effectively manage third-party risks and ensure the reliability of our supply chain.
- \\ **Change Management Registers:** Logs of all changes to systems, processes, and policies, including approvals, implementation details, and impact assessments, to maintain control and oversight of our operational environment.
- \\ **Access Control Registers:** Documentation of access permissions for all users and systems, ensuring appropriate access levels and safeguarding sensitive data.
- \\ **Maintenance Registers:** Records of maintenance activities conducted on critical systems and infrastructure, ensuring optimal system performance and availability.
- \\ **Customer Feedback Registers:** Collection and analysis of customer feedback, with actionable insights used to improve service quality, align with customer expectations, and ensure regulatory compliance.

## Alignment with International Cloud and Outsourcing Standards

As part of our commitment to maintaining robust data security, regulatory compliance, and operational resilience, Funds-Axis already aligned its key policies and procedures - particularly our Cloud Computing Standards - with several international standards and

guidelines. This ensures that our practices meet or exceed industry expectations and regulatory requirements across multiple jurisdictions. Key standards include:

Country	Standard/ Legislation
UK	FCA Guidance for firms outsourcing to the 'cloud' and other third-party IT services (FG 16/5) - 2019
EU	European Banking Authority (EBA) Recommendations on Outsourcing to Cloud Service Providers - 2017
EU	ESMA Final Report Guidelines on outsourcing to cloud service providers (ESMA50-157-2403) - 2020
EU	Digital Operational Resilience Act (DORA) - 2022
Luxembourg	CSSF's publications on IT outsourcing and cloud computing (Circular CSSF 17/654, as amended by Circular CSSF 19/714) - 2017
Ireland	Central Bank of Ireland cross-industry guidance on outsourcing - 2021
International	ISO/IEC 27001:2022
US	National Institute of Standards and Technology (NIST) Special Publication 800-144 - 2011

## What is available to Customers

To provide reassurance and transparency to our customers, Funds-Axis offers the following support and documentation upon request to demonstrate compliance with DORA and other regulatory standards:

- \ **DORA Due Diligence Support:** We actively support customer requests related to DORA due diligence, including completing any questionnaires required as part of customer compliance assessments.
- \ **Customer Due Diligence Visits:** We welcome and support client visits to our facilities or virtual assessments, allowing them to observe our security and operational practices firsthand.
- \ **Proactively Available Documentation:** Our core policies are available to customers upon request, providing an overview of our commitment to security and compliance. These include, but are not limited to:
  - Change Management Process
  - Information Security Policy
  - Cyber Security Policy Part 1 Internal Organisation
  - Cyber Security Policy Part 2 Funds-Axis Technology Overview
  - Customer Data Policy
  - Risk Assessment and Risk Treatment Procedure

- Incident Management Policy
- Change Management Process
- Business Continuity Policy
- HighWire Back-up and Recovery Policy
- HighWire Release Management

- \\ **Results of Monitoring and Audits:** To further support transparency, we provide relevant results from our monitoring, audits, and risk assessments:
  - **Business Continuity Testing Reports** (high-level summary reports)
  - **Security Incident Reports** (where applicable and in line with confidentiality requirements)
  - **Compliance Audit Results** (e.g., ISO 27001 certification)
  - **Risk Assessment Summaries** (including threat assessments and mitigation plans)
  - **Vulnerability Assessment Results** (e.g., network scans, penetration testing reports)
  - **System Health and Performance Reports** (e.g., uptime reports, system performance metrics)
  - **Internal Audit Findings** (covering areas like data privacy, regulatory compliance, and operational risk)
- \\ **Additional Documentation:**
  - **Service Level Agreements (SLAs):** Our SLAs define the performance standards we adhere to, ensuring customers receive consistent and high-quality service.
  - **Performance Metrics:** Key performance metrics are available to demonstrate our commitment to efficiency and operational resilience.
  - **Customer Satisfaction Surveys:** Results and insights from customer satisfaction surveys are shared to demonstrate our ongoing commitment to meeting client expectations.

## Enhancements made for DORA

Below is a summary of some of the key steps taken additional steps to ensure full alignment with DORA's specific requirements, reinforcing our commitment to operational excellence.

### Alignment and Gap Filling

To address the alignment and gaps identified in the DORA framework, we implemented several critical enhancements, ensuring that our processes and documentation not only meet but exceed regulatory expectations:

- \\ **Improved BCP & DR Documentation:** Our Business Continuity and Disaster Recovery (BCP & DR) documentation scope has been broadened, with an increased frequency of testing based on risk profiles to ensure enhanced preparedness.

- \\ **Third-Party Risk Management:** Upgraded our supply chain and ICT third-party risk management by including a technical and functional contractual analysis to evaluate all third-party providers more effectively.
- \\ **Enhanced Change Management:** We implemented an improved change management process to better track, review, and approve any system or process changes, thereby minimising potential disruptions.
- \\ **Extended Internal Audits:** Our internal audit scope was expanded to cover all teams and team members, ensuring comprehensive oversight and accountability.
- \\ **Increased Audit Frequency:** Audit schedules have been intensified based on the assessed risk level of each team or function, enabling a more dynamic and responsive audit cycle.
- \\ **Increased Penetration Testing:** We have significantly ramped up the frequency and depth of internal penetration testing, identifying and mitigating vulnerabilities more proactively.

## Documentation and Reporting

As part of the enhancements to comply with DORA, we have thoroughly reviewed and improved several core documents to ensure clarity and compliance:

- \\ **Enhanced Policy Framework:** Policies such as the Cloud Computing Policy, Incident Management Policy, Acceptable Use Policy, Anti-Malware Policy, and others were reviewed and strengthened to address emerging threats and compliance obligations.
- \\ **Updated Procedures:** Procedures like the Operations Security Procedure, Communications Security Procedure, and Secure Coding Policy were revamped for better clarity and enforceability.
- \\ **Robust Incident Management and Risk Documentation:** Documents covering Risk Assessment and Risk Treatment, Change Management Process, and Threat Intelligence Policy now contain more detailed procedures and guidance for proactive risk mitigation.

## Third-Party Risk Management

Our third-party risk management program has been strengthened to ensure comprehensive oversight of suppliers and third parties:

- \\ **Supplier Register Update:** Our Supplier Register now includes critical data for each supplier, such as Cloud Service Type, Country of Registration, Security Measures, Subcontractors, Data Handling, and Contractual Arrangements.

- \\ **Detailed Third-Party Evaluations:** We perform in-depth evaluations of third-party ICT providers, focusing on their security controls, data protection measures, and contractual compliance to mitigate risks from third-party relationships.

## Resilience Testing

To reinforce our operational resilience, we have made substantial improvements to our BCP and DR frameworks:

- \\ **BCP & DR Plan Overhaul:** Our BCP & DR plans were thoroughly revised with expanded scope, ensuring coverage of all critical systems and functions.
- \\ **Risk-Based Testing Frequency:** Testing frequency is now increased based on the assessed risk level, allowing us to prioritise high-risk areas.
- \\ **Client-Facing Documentation:** High-level summary documents of our resilience testing and BCP/DR processes have been created and are available to clients, providing transparency and assurance of our resilience capabilities.

## Incident Reporting

Our incident management processes have been significantly improved to ensure efficient and transparent reporting:

- \\ **Policy Improvements:** The Incident Management Policy and Risk Assessment and Risk Treatment documentation have been refined to streamline classification, response, and mitigation of incidents.
- \\ **Incident Management System:** A new ticketing system (ServiceDesk Plus) has been implemented across the organisation. This platform includes built-in SLAs for incident response, enabling improved tracking, prioritisation, and resolution of incidents, which enhances our capability to meet regulatory standards.

## Staff Training

We have developed a comprehensive training program to enhance staff awareness and understanding of cybersecurity, compliance, and regulatory standards:

- \\ **Dedicated Cybersecurity Awareness Training:** Our in-house training platform provides comprehensive training covering key topics such as Compliance, Legislation, GDPR, ISO standards, and information security best practices.
- \\ **CISO-Led Awareness Initiatives:** In addition to the training platform, our CISO, Trevor Dempster, conducts regular security awareness initiatives through emails, newsletters, and blog posts on the internal website, ensuring staff stay informed about the latest cybersecurity threats and best practices.
- \\ **Interactive Engagement:** We conduct spot quizzes to ensure engagement and assess knowledge retention, encouraging a proactive approach to security awareness.

## Appendix 2: DORA Control Testing and Results

### Testing Overview

Control testing was conducted in accordance with DORA requirements, focusing on the five key components of digital operational resilience. The testing process included review of documentation, system assessments, and evaluation of operational procedures.

### Control Testing Results Summary

Control Area	Control Tested	Result	Issues Identified
ICT Risk Management	Risk assessment and treatment plans	Effective	None
ICT Incident Reporting	Incident reporting mechanisms	Effective	None
ICT Business Continuity Management (BCM)	Business continuity and disaster recovery plans	Effective	None
ICT Third-Party Risk Management	Third-party risk assessments and monitoring	Effective	None
Information and Intelligence Sharing on Cyber Threats	Threat intelligence sharing processes	Effective	None

### Key Findings

- \ **ICT Risk Management**
  - Comprehensive risk assessment framework in place
  - Regular risk reviews and updates conducted
  - Clear risk treatment procedures implemented
- \ **ICT Incident Management**
  - Structured incident management process established
  - Clear reporting lines and responsibilities defined
  - Regular testing of incident response procedures
- \ **ICT Business Continuity Management (BCM)**
  - Regular testing of business continuity plans
  - Documented recovery procedures
  - Successful completion of resilience tests
- \ **ICT Third-Party Risk Management**
  - Comprehensive vendor assessment process
  - Regular monitoring and review procedures
  - Clear contractual requirements established
- \ **Information and Intelligence Sharing on Cyber Threats**
  - Active participation in threat intelligence sharing

- Clear protocols for information dissemination
- Regular updates and monitoring

## **Recommendations**

To maintain and enhance DORA compliance:

- \ Continue regular testing and updates of control frameworks
- \ Maintain documentation of all compliance activities
- \ Regular review and enhancement of procedures based on emerging risks
- \ Ongoing staff training and awareness programs

## Appendix 3: Supporting Documentation

### 1. Information Security Policy

- \ Overview of Funds-Axis's commitment to information security.
- \ Key principles and objectives of the information security program.
- \ Roles and responsibilities for information security.
- \ Policies for data protection, access control, and incident management.
- \ Procedures for monitoring, auditing, and continuous improvement.

### 2. Cyber Security Policy Part 1: Internal Organisation

- \ Structure and governance of the cybersecurity program.
- \ Roles and responsibilities within Funds-Axis.
- \ Internal policies and procedures for managing cybersecurity risks.
- \ Training and awareness programs for employees.
- \ Incident response and recovery procedures.

### 3. Cyber Security Policy Part 2: Funds-Axis Technology Overview

- \ Overview of the technology infrastructure and security measures.
- \ Description of security controls for network, systems, and applications.
- \ Measures for protecting data integrity and confidentiality.
- \ Procedures for regular security assessments and updates.
- \ Details of any specific technologies or tools used for cybersecurity.

### 4. Risk Assessment and Risk Treatment Procedure

- \ Methodology for identifying and assessing risks.
- \ Criteria for evaluating the impact and likelihood of risks.
- \ Procedures for developing and implementing risk treatment plans.
- \ Monitoring and review processes for risk management.
- \ Documentation of risk assessments and treatment actions.

### 5. Threat Intelligence Policy

- \ Framework for gathering, analysing, and sharing threat intelligence.
- \ Sources of threat intelligence and methods for validation.
- \ Procedures for integrating threat intelligence into security operations.
- \ Roles and responsibilities for threat intelligence activities.
- \ Reporting and communication protocols for threat intelligence.

### 6. Cloud Computing Policy

- \ Guidelines for the use of cloud services within Funds-Axis.
- \ Security and compliance requirements for cloud service providers.
- \ Procedures for evaluating and selecting cloud services.
- \ Risk management and data protection measures for cloud environments.

- \ Monitoring and auditing processes for cloud services.

## **7. Customer Data Policy**

- \ Principles for handling and protecting customer data.
- \ Data classification and access control measures.
- \ Procedures for data collection, storage, and processing.
- \ Compliance with data protection regulations (e.g., GDPR).
- \ Incident response and notification procedures for data breaches.

## **8. HighWire Back-up and Recovery Policy**

- \ Procedures for backing up critical data and systems.
- \ Frequency and methods of backups.
- \ Storage and protection of backup data.
- \ Recovery procedures and testing of backup systems.
- \ Roles and responsibilities for backup and recovery activities.

## **9. HighWire Release Management**

- \ Processes for managing software releases and updates.
- \ Procedures for testing and validating new releases.
- \ Change management and approval processes.
- \ Communication and documentation of release activities.
- \ Roles and responsibilities for release management.

## **10. Business Continuity and Disaster Recovery Plan**

- \ Strategies for maintaining business operations during disruptions.
- \ Procedures for disaster recovery and system restoration.
- \ Roles and responsibilities for business continuity and disaster recovery.
- \ Communication plans for internal and external stakeholders.
- \ Regular testing and updating of the BCP and DRP.

## **11. High-Level Summary of Business Continuity Plan (BCP) Testing**

- \ Overview of the BCP testing objectives and scope.
- \ Summary of the testing scenarios and methodologies used.
- \ Key findings and results from the BCP tests.
- \ Recommendations and actions taken based on the test results.

## **12. High-Level Summary of Business Continuity Plan (BCP) Testing - Wider Business**

- \ Summary of BCP testing across different business units and functions.
- \ Key findings and results from the wider business BCP tests.
- \ Impact assessment and lessons learned from the tests.

## Glossary

### A

- \ **Access Control:** Measures and policies that restrict access to information systems and data to authorised users only.
- \ **Audit:** A systematic examination of records, statements, and processes to ensure compliance with regulations and standards.

### B

- \ **Business Continuity Plan (BCP):** A strategy that outlines procedures for maintaining business operations during and after a disruption.

### C

- \ **Compliance:** Adherence to laws, regulations, guidelines, and specifications relevant to business operations.
- \ **Control Environment:** The set of standards, processes, and structures that provide the foundation for carrying out internal control across the organisation.
- \ **Critical ICT Third-Party Provider:** An ICT service provider designated as critical under DORA, subject to specific oversight and compliance requirements.
- \ **Cyber Incident:** An event that jeopardises the cybersecurity of an information system or the information it processes, stores, or transmits.

### D

- \ **Digital Operational Resilience:** The ability of a financial entity to build, assure, and review its operational integrity from a technological perspective.
- \ **Disaster Recovery Plan (DRP):** A documented process to recover and protect a business IT infrastructure in the event of a disaster.

### E

- \ **External Audit:** An independent examination of financial and operational activities conducted by an external party.

### F

- \ **Financial Entity:** Any organisation that provides financial services, including banks, insurance companies, and investment firms.

### G

- \ **Governance:** The framework of rules and practices by which a board of directors ensures accountability, fairness, and transparency in a company's relationship with its stakeholders.

## I

- \\ **ICT Risk Management:** The process of identifying, assessing, and controlling risks associated with the use of information and communication technology.
- \\ **Incident Reporting:** The process of documenting and communicating details about an incident to relevant stakeholders.
- \\ **Information Security:** The practice of protecting information by mitigating information risks and vulnerabilities.

## L

- \\ **Legal Entity Identifier (LEI):** A unique identifier for legal entities participating in financial transactions, used to improve the transparency of financial data.

## M

- \\ **Monitoring:** The continuous process of overseeing and checking the progress or quality of a system or process.

## N

- \\ **NIS 2 Directive:** The Network and Information Security Directive 2, which sets out measures to ensure a high common level of cybersecurity across the EU.

## O

- \\ **Operational Resilience:** The ability of an organisation to continue to deliver critical operations through disruption.

## P

- \\ **Penetration Testing:** A method of evaluating the security of an information system by simulating an attack from malicious outsiders.
- \\ **Policy:** A deliberate system of principles to guide decisions and achieve rational outcomes.

## R

- \\ **Regulatory Compliance:** Adherence to laws, regulations, guidelines, and specifications relevant to business operations.
- \\ **Risk Assessment:** The identification and analysis of relevant risks to achieve the objectives of an organisation.

## S

- \\ **Security Awareness Training:** Programs designed to educate employees about the importance of information security and the best practices to protect information assets.
- \\ **Service Level Agreement (SLA):** A contract between a service provider and a customer that specifies the level of service expected during its term.

## T

- \\ **Third-Party Risk Management:** The process of identifying, assessing, and controlling risks associated with third-party vendors and service providers.
- \\ **Threat Intelligence:** Information about threats and threat actors that helps an organisation mitigate potential attacks.

## V

- \\ **Vulnerability Assessment:** The process of identifying, quantifying, and prioritising vulnerabilities in a system.

END