DoraDocs
DORA COMPLIANCE, SIMPLIFIED

DORA COMPLIANCE PACK

Regulation (EU) 2022/2554 — Digital Operational Resilience Act

Organisation	Meridian Fund Management Limited
Entity Type	Pension fund / IORP
Regulator	Central Bank of Ireland (CBI)
DORA Tier	**Out of Scope — Proportionate Application**
Documents	5 Documents
Date Generated	12 April 2026
Version	1.0

Executive Summary

DORA Classification: Out of Scope — Proportionate Application — As an IORP, this entity is not directly in scope of DORA as a financial entity under Art. 2(1). However, CBI supervisory expectations align with DORA principles for operational resilience, requiring proportionate application based on scheme complexity and outsourcing arrangements. The entity must demonstrate how DORA standards inform ICT risk management under IORP II governance requirements.

While not directly subject to DORA compliance obligations, this IORP faces significant indirect impact through outsourced ICT service providers who must comply with DORA. CBI expects ICT governance proportionate to scheme complexity, with particular focus on member data integrity, benefit calculation systems, and third-party dependency management. The entity must integrate ICT risk into overall risk management framework per CBI Cross Industry Guidance, demonstrating active board engagement with operational resilience.

This document is a compliance starting point and does not constitute legal advice. Review with qualified legal counsel before adoption as a regulatory document.

1. ICT Risk Management Framework

Meridian Fund Management Limited · Version 1.0 · 12 April 2026 · Ref: DORA Arts. 5–15 & CDR 2024/1774

This IORP's business model centres on safeguarding member benefits through accurate record-keeping, contribution processing, and benefit payments. ICT dependency includes Google Workspace for administration, Bloomberg Terminal for investment data, and critical outsourced pension administration systems supporting approximately 500-2000 members across defined benefit and defined contribution arrangements.

ICT Risk Appetite Statement

Ref: Art. 6(8)(b) — ICT risk tolerance and appetite

The IORP maintains zero tolerance for ICT incidents affecting member benefit payments or contribution processing, with maximum tolerable disruption of 4 hours for pension benefit calculations during business hours and 24 hours for member portal access. No single ICT provider may support more than 60% of Critical or Important Functions without documented and annually tested exit arrangements. ICT incident threshold: maximum 1 major incident per annum affecting member services, monitored via monthly ICT Risk Dashboard reported to Board by Head of Operations. Key Risk Indicators include: system availability (99.5% minimum for CIFs, measured monthly), third-party SLA compliance (95% minimum, reported quarterly), cyber security incident frequency (zero tolerance for data breaches affecting member records, monitored continuously). Breach of risk appetite triggers immediate escalation to CEO within 2 hours, Board notification within 24 hours, and mandatory remediation plan within 5 business days. Investment Committee receives quarterly ICT risk reports including concentration analysis and emerging technology risks.

ICT Governance and Board Accountability

Ref: Art. 5 & Art. 6 — ICT risk management framework applied proportionately

Board maintains ultimate accountability for ICT risk through quarterly reporting from Head of Operations covering critical system performance, third-party risk, and cyber security posture. Three Lines of Defence operates with first line (scheme administration team) conducting daily system monitoring, second line (compliance function) providing monthly challenge on ICT controls, and third line (internal audit) conducting annual ICT risk assessment. CEO designated as accountable person for operational resilience, reporting semi-annually to Board on ICT risk appetite compliance and emerging technology risks affecting member services.

ICT Risk Identification and Classification

Ref: Art. 8 — ICT risk identification and classification

ICT risks classified using impact tolerance methodology covering member data integrity, benefit payment processing, contribution allocation accuracy, and regulatory reporting capability. Risk register updated monthly identifying threats to Critical or Important Functions including cyber attacks on member data, system failures during benefit payment runs, third-party service disruptions, and data corruption affecting member records. Risk assessment methodology considers financial impact (benefit payment delays), operational impact (member service disruption), and reputational consequences (trustee liability and member confidence).

Third-Party ICT Service Provider Management

Ref: Art. 28-44 — ICT third-party risk applied proportionately

All 8 ICT third-party providers subject to due diligence covering operational resilience, data security, and business continuity arrangements. Critical third-party relationships (pension administration system, member portal, payroll

interface) governed by service level agreements specifying 99.5% availability, maximum 4-hour response times, and annual penetration testing requirements. Exit strategies documented for each critical provider with alternative supplier identification and data portability assessments conducted annually. Concentration risk monitored quarterly with no single provider supporting more than 60% of member-facing services without Board-approved mitigation.

Critical or Important Functions (CIF) Register

Ref: Art. 8(1) — Identification of assets supporting CIFs

CIF	Supporting Systems	Key Dependencies	Max Tolerable Disruption	RTO	RPO	Owner
Pension Benefit Calculation Engine	Outsourced pension administration platform, actuarial calculation modules, benefit payment interface	Third-party administrator, banking payment rails, member database	No pension payment delayed beyond 1 business day from scheduled payment date	4 hours during business hours	24 hours maximum data loss	Head of Operations
Member Record Management System	Member portal, contribution tracking database, beneficiary management module	Cloud hosting provider, identity management system, GDPR compliance controls	No member record corruption affecting benefit entitlements	8 hours for portal access, 4 hours for critical record updates	4 hours maximum data loss for contribution records	Head of Operations
Investment Valuation and Reporting	Bloomberg Terminal, investment accounting system, performance reporting dashboard	Market data feeds, custodian interfaces, regulatory reporting platforms	No delay in monthly unit pricing affecting member account values	12 hours for investment data, 24 hours for member reporting	24 hours for transaction records	Investment Manager

Three Lines of Defence

Ref: Art. 6(4) — Internal governance and control framework

First Line — Business / ICT Operations

Scheme administration team conducts daily monitoring of pension calculation systems, member portal performance, and contribution processing accuracy. First line maintains incident logs, performs daily reconciliations of member data, and executes business continuity procedures during system disruptions.

Second Line — Risk & Compliance

Compliance function provides independent monthly assessment of ICT control effectiveness, third-party risk management, and regulatory reporting system integrity. Second line challenges first line risk assessments and validates incident response procedures through quarterly walk-throughs.

Third Line — Internal Audit

Internal audit conducts annual comprehensive ICT risk assessment covering cyber security controls, third-party governance, and business continuity arrangements. Audit programme includes testing of critical system recovery procedures and evaluation of member data protection controls.

2. Incident Response & Reporting Procedure

Meridian Fund Management Limited · Version 1.0 · 12 April 2026 · Ref: DORA Arts. 17–23, CDR 2024/1772, CIR 2024/2956

While not directly subject to DORA incident reporting under Arts. 17-23, this IORP adopts proportionate incident management aligned with CDR 2024/1772 criteria to meet CBI supervisory expectations and ensure robust governance of ICT disruptions affecting member services.

Incident Classification Criteria

Ref: CDR 2024/1772 — Classification of major ICT-related incidents and cyber threats

Major incidents defined as: ICT disruptions affecting more than 100 members' ability to access pension benefits or contribution records, system outages preventing pension payments for more than 4 hours during business hours, cyber security incidents resulting in unauthorised access to member personal data, or complete failure of pension calculation systems during benefit payment cycles. Financial impact thresholds: incidents causing potential benefit payment delays exceeding €50,000 aggregate value, or requiring manual intervention affecting more than 20% of monthly pension payments. Minor incidents include: temporary member portal unavailability under 2 hours, non-critical system performance degradation not affecting benefit calculations, or isolated access issues affecting fewer than 10 members. Data loss incidents classified as major if affecting member benefit entitlements or historical contribution records essential for benefit calculations.

Regulatory Notification Timeline

Stage	Deadline	Article	Content Required
Internal Escalation	Within 1 hour of incident identification	Internal governance requirement	Initial impact assessment, affected systems identification, and immediate containment actions
Board Notification	Within 4 hours for major incidents affecting Critical or Important Functions	Board accountability requirement	Incident classification, member impact assessment, recovery timeline, and reputational risk analysis
Regulatory Notification	Within 24 hours for incidents affecting member benefits or data security	CBI supervisory expectation	Formal incident report including root cause analysis, member impact quantification, and remediation plan

Internal Escalation Path

ICT incidents identified by scheme administration team immediately escalated to Head of Operations (within 30 minutes), who assesses impact and notifies CEO for major incidents within 1 hour. CEO determines Board notification requirement and initiates crisis management procedures if member benefits affected. Board Chair notified within 4 hours for major incidents, with emergency Board meeting convened if incident threatens scheme operations or member data integrity.

ITS Reporting Template Guidance

Ref: CIR 2024/2956 — ITS on reporting templates for major ICT incidents

Incident reports follow three-stage structure: initial notification within 1 hour covering incident scope and immediate actions, intermediate report within 24 hours providing impact analysis and recovery progress, and final report within 10 business days including root cause analysis, lessons learned, and control enhancement recommendations. Reports specifically address member impact, trustee liability implications, and regulatory notification requirements under IORP governance framework.

3. Third-Party ICT Risk Register

Meridian Fund Management Limited · Version 1.0 · 12 April 2026 · Ref: DORA Arts. 28–30, CDR 2024/1773

Under DORA Articles 28-30 and CDR 2024/1773, Meridian Fund Management Limited must maintain comprehensive third-party provider documentation covering all ICT services supporting critical or important functions. For IORPs, this includes pension administration, member data processing, and contribution management systems with proportionate risk assessment reflecting scheme complexity.

Provider Category	CIFs Supported	Criticality	Art. 30 Contractual Requirements	Exit Strategy
Pension Administration System Provider	Pension benefit calculation, member data management, contribution processing, regulatory reporting	Critical	Service level guarantees (99.5% uptime), audit rights including sub-processors, 24-hour incident notification, data portability in open format, exit assistance minimum 12 months, sub-outsourcing pre-approval requirements	18-month transition to alternative provider with parallel running period; tested migration procedures for member data and benefit calculation engines; backup administration capability through trustee services provider
Cloud Infrastructure Provider (Google Workspace/GCP)	Business communications, document management, data backup and recovery	Important	Data residency within EU, encryption at rest and in transit, audit rights, incident notification within 4 hours, data export capabilities, termination assistance	6-month migration to alternative cloud provider with documented data export procedures and tested email migration processes
Financial Data Provider (Bloomberg Terminal)	Investment valuation, asset pricing for pension fund portfolios	Important	Data accuracy guarantees, real-time feed availability, audit trails for data lineage, incident notification procedures, alternative data provision during outages	3-month transition to alternative data providers (Refinitiv/S&P) with parallel data feeds during transition

Sub-Outsourcing Chain

Ref: CDR 2024/1773 Art. 5 — Sub-outsourcing of CIFs

Per CDR 2024/1773 Article 5, Meridian Fund Management Limited requires written notification and approval for all material sub-outsourcing arrangements. Documentation must include sub-processor risk assessment, contractual flow-down of DORA requirements, and direct audit rights where sub-outsourcing supports critical functions. Particular focus on pension administration provider's use of cloud infrastructure and data processing sub-contractors.

Concentration Risk Assessment

Concentration risk assessment identifies pension administration provider supporting 80% of CIFs exceeding internal appetite threshold of 50% dependency on single provider. Mitigation requires development of backup administration capability and enhanced contractual protections including guaranteed exit assistance.

4. Business Continuity & Recovery Plan

Meridian Fund Management Limited · Version 1.0 · 12 April 2026 · Ref: DORA Arts. 11–12, Arts. 24–25

Business Continuity Planning under DORA Articles 11-12 focuses on ensuring continuity of pension administration, member services, and fiduciary obligations. For IORPs, emphasis on member data integrity, contribution processing continuity, and benefit payment systems with impact tolerances reflecting pension scheme obligations.

Impact Tolerances & Recovery Objectives

Ref: Art. 11(5) — Maximum tolerable disruption thresholds for CIFs

Critical/Important Function	Maximum Tolerable Disruption	RTO	RPO	Owner
Pension Benefit Calculation and Payment Processing	No pension benefit payment delayed beyond 2 business days; member queries resolved within 3 business days	4 hours for critical payment processing; 24 hours for member enquiry systems	24 hours maximum data loss acceptable	Chief Operations Officer
Member Data Management and Contribution Processing	No contribution allocation delayed beyond 5 business days; member data access restored within 8 hours	8 hours for member data access; 24 hours for contribution processing	4 hours maximum data loss acceptable	Head of Pensions Administration

Backup Procedures

Ref: Art. 12 — ICT backup policies, procedures and methods

Daily automated backups of member data with weekly full system backup; offsite storage at geographically separated facility minimum 100km distance; monthly restoration testing with documented recovery procedures; annual full disaster recovery test with results reported to Board Audit Committee

Scenario-Based Testing Programme

Ref: Arts. 24–25 — Digital operational resilience testing

Annual scenario-based testing programme: (1) Ransomware attack on pension administration system - quarterly tabletop exercises with full system recovery test annually; (2) Critical third-party provider failure - biannual testing of backup administration procedures; (3) Member data corruption and integrity failure - quarterly data restoration testing; (4) Google Cloud outage affecting operations - annual cloud failover testing. All scenarios require Board Risk Committee sign-off on test results and remediation actions.

Crisis Communications

Crisis communication led by CEO with CBI notification within 4 hours for major incidents; member communication via backup channels (post, alternative email) within 24 hours; employer notification procedures through scheme administrator backup systems; media relations through designated communications firm

Annual Testing Schedule

Q1: Ransomware tabletop exercise; Q2: Third-party provider failure simulation; Q3: Data restoration testing and cloud failover; Q4: Full BCP exercise with Board participation. All results documented with lessons learned report to Board Risk Committee within 30 days

5. DORA Gap Analysis & Remediation Roadmap

Meridian Fund Management Limited · Version 1.0 · 12 April 2026

Gap analysis reflects current partial DORA documentation status with significant gaps across all five pillars requiring immediate remediation ahead of January 2025 enforcement. Assessment identifies material gaps in ICT risk management framework, incident reporting procedures, and third-party risk management documentation.

Gap Analysis by DORA Pillar

Pillar	Article	Requirement	Current State	Gap	Action
ICT Risk Management	Art. 6(1)	ICT risk management framework as integral part of financial entity's overall risk management system	ICT risk managed separately within IT function; no integration with overall risk framework	High	Chief Risk Officer to develop integrated ICT risk framework with Board Risk Committee oversight by Month 2
ICT-Related Incident Management	Art. 17(1)	Comprehensive ICT-related incident management process	Basic IT incident procedures; no DORA-compliant classification or reporting structure	High	Head of Operations to implement DORA incident classification system and CBI reporting procedures by Month 1
ICT Third-Party Risk	Art. 28(1)	ICT third-party risk management strategy covering third-party providers arrangements	Basic vendor management; no DORA-compliant third-party risk assessment	High	Chief Operations Officer to complete Article 30 contractual review and risk register by Month 3
Digital Operational Resilience Testing	Art. 24(1)	Digital operational resilience testing programme based on risk analysis	Annual DR testing only; no scenario-based or advanced testing programme	Medium	Head of IT to develop scenario-based testing programme aligned with threat landscape by Month 6
Information and Intelligence Sharing	Art. 32(1)	Arrangements for information sharing on cyber threats and vulnerabilities	No formal threat intelligence arrangements or information sharing mechanisms	Low	Head of IT to establish threat intelligence sharing arrangements with industry bodies by Month 6

Remediation Roadmap

Phase 1 — Critical Compliance Foundation

Month 1-2
Articles 6, 17 - Core ICT risk management and incident procedures

- CRO implements integrated ICT risk framework
- COO establishes DORA incident reporting procedures
- Board Risk Committee approves ICT risk appetite statements

Phase 2 — Third-Party Risk Framework

Month 3-4
Articles 28-30 - Third-party risk management and contractual requirements

- COO completes third-party risk register and criticality assessment
- Legal review and update Article 30 contractual clauses
- Procurement implements DORA-compliant vendor onboarding

Phase 3 — Operational Resilience Enhancement	**Month 5-6** *Articles 11-12, 24-25 - Business continuity and resilience testing*

- Head of IT implements scenario-based testing programme
- COO updates BCP with DORA-compliant impact tolerances
- Board approval of annual resilience testing schedule