ORION
REAL ANSWERS TO REAL NEEDS

Orion Namibia Pension & Provident Funds
Mutual Tower, 223 Independence Avenue
PO Box 165, Windhoek, Namibia
T. +264 81 9561013/ 128 9720
E. NAM-OrionPO@oldmutual.com

REQUEST FOR PROPOSAL (RFP)

Development of a Cybersecurity Policy and Business Resilience Policy for the Orion Namibia Pension and Provident Funds (Fund):

Issue Date: 03 August 2026
Closing Date:25 August 2026

---

1. Introduction

The Fund invites qualified and experienced service providers to submit proposals for the development of:

1.1 A comprehensive Cybersecurity Policy, and
1.2 A comprehensive Business Resilience Policy (including Business Continuity & Disaster Recovery components).

These policies must align with industry best practice, NAMFISA expectations, and the Fund's governance framework (FIMA and retirement fund related legislation). The selected provider will deliver policies that strengthen the Fund's security posture, operational resilience, and regulatory compliance.

2. Objectives of the Assignment

The Fund seeks a service provider capable of:

2.1. Assessing current cybersecurity and resilience gaps
2.2. Developing policies aligned with global standards
2.3. Ensuring policies are practical, implementable, and tailored to the Fund's environment
2.4. Providing templates, frameworks, and implementation guidance
2.5. Supporting the Fund with stakeholder workshops and training

3. Fund Information

The Fund operates within the physical and information technology infrastructures of Old Mutual. The Old Mutual Information Security Risk Policy establishes a comprehensive governance framework to protect the confidentiality, integrity, and availability of information and technology assets across the organization.

The policy is aligned to internationally recognized standards and frameworks, including the NIST Cybersecurity Framework, and defines minimum requirements for managing cyber security risks, protecting sensitive information, ensuring system resilience, and maintaining regulatory compliance. It applies across all technology environments, including on-premises systems, cloud services, third-party providers, contractors, and outsourced partners. The policy emphasizes clear accountability, risk-based decision-making, security governance, control assurance, incident management, continuous monitoring, and regular policy review to ensure cyber risks remain within the organization's risk appetite.

The Fund should consider incorporating similar principles to establish a structured, scalable, and governance-driven cyber security framework.

Similarly to the above, the Fund should also consider the existence of and dependencies on the Old Mutual Business Resilience Policy in formulating its business resilience framework.

4. Scope of Work

4.1. Cybersecurity Policy Development that must cover:
- 4.1.1. Trustee and Fund Governance and roles
- 4.1.2. Threat identification and risk management
- 4.1.3. Access control and authentication
- 4.1.4. Network and infrastructure security
- 4.1.5. Data protection and privacy
- 4.1.6. Incident response and escalation
- 4.1.7. Monitoring and logging
- 4.1.8. Vendor and third-party security
- 4.1.9. Cyber awareness and training
- 4.1.10. Compliance with Namibian regulatory expectations

4.2. Business Resilience Policy Development that must include:
- 4.2.1. Business continuity planning
- 4.2.2. Disaster recovery planning
- 4.2.3. Crisis management framework
- 4.2.4. Recovery time objectives (RTO) and recovery point objectives (RPO)
- 4.2.5. Communication protocols during disruptions
- 4.2.6. Testing and simulation requirements
- 4.2.7. Dependencies and critical process mapping
- 4.2.8. Resilience governance and reporting

5. Deliverables

5.1. Cybersecurity Policy
5.2. Business Resilience Policy
5.3. Implementation roadmap
5.4. Training session(s) for Trustees, Fund officials and Fund Service Providers
5.5. Supporting templates (risk registers, incident logs, continuity checklists, reporting templates)

6. Proposal Submission Requirements

Bidders must include:

6.1. Company profile and relevant experience
6.2. Proposed methodology and work plan
6.3. Project timeline
6.4. Team qualifications
6.5. Examples of similar work delivered with references from comparable clients
6.6. Pricing structure (fixed fee preferred)
6.7. Risk mitigation approach

7. Evaluation Criteria

Proposals will be evaluated using the weighted scoring matrix below.

Evaluation Scoring Matrix (Weighted)

Evaluation Category	Weight (%)	Description	Scoring Scale 1–10
Technical Approach	30%	Quality of methodology, alignment with standards, depth of analysis	
Experience & Track Record	20%	Relevant projects, sector experience, references	
Team Qualifications	15%	Expertise in cybersecurity, resilience, governance	
Project Plan & Timeline	15%	Realistic timelines, milestones, deliverables	
Cost & Pricing Structure	10%	Transparency, value for money, fee structure	
Risk Mitigation Approach	10%	Identification of risks and proposed mitigations	

8. Reservation of Rights

The Fund reserves the right to:

- not appoint any service provider applying;
- request clarification or presentations;
- negotiate with one or more shortlisted service providers;
- verify references and submitted information;

- conduct interviews;
- amend or withdraw this tender process; and
- appoint in whole or in part, if this is in the Fund's best interests.

9. Submission Instructions

Proposals must be submitted electronically to NAM-OrionPO@oldmutual.com
Subject Line: RFP – Cybersecurity & Business Resilience Policies

Deadline: 17h00 on 25 August 2026
Late submissions will not be considered.

Contact for Queries

Ramon Hansen, NAM-OrionPO@oldmutual.com