GIPF House
Cnr. of Dr Kenneth David Kaunda/Goethe Street
PO Box 23500 Windhoek
Namibia
Tel. +264 61 205 1746
E-mail: gnaris@gipf.com.na

TERMS OF REFERENCE (TOR)

BID CS/RFP/GIPF-02/2026

VULNERABILITY ASSESSMENT AND PENETRATION TESTING CONSULTING SERVICES

Contents

1. EXECUTIVE SUMMARY

GIPF continues to strengthen its cyber security posture by ensuring the obligation to safeguard its Infrastructure and data against cyber threats. As digitalization continues to expand GIPF's operational footprint, the exposure to cybersecurity threats, system vulnerabilities, and potential data breaches has increased significantly. To ensure the FUND remains committed to ensuring a positive cybersecurity posture, GIPF deems it critical to proactively identify, assess and remediate security weaknesses which may compromise the confidentiality, integrity, and availability of information assets.

2. BACKGROUND & OBJECTIVE

2.1 Background

GIPF is leveraging on innovative technologies to enhance its operational efficiency, improve decision-making processes, and deliver superior products and services. The Vulnerability Assessment and Penetration Testing exercise aims to provide an independent and objective evaluation of GIPF's cyber security and associated defensive controls and where possible, recommend improvements.

2.2 Objective

The primary objective of this initiative is seeking the services of an experienced service provider to assess the GIPF's infrastructure to detect vulnerabilities in information systems, networks and applications by simulating real-world cyberattacks to test the organizations' cyber security robustness and resilience. This initiative is to further conduct and provide detailed risk analysis and prioritization.

3. SCOPE OF WORK

The appointed service provider shall perform a comprehensive Vulnerability Assessment and Penetration Testing exercise to evaluate the security posture of the organization's where:

The service provider will be responsible for:

1. **Project Initiation and Planning**: Project start and end dates. Project details. Project durations.
2. **Network Testing**: Internal and external networks, wireless networks,
3. **Application Testing**: Web applications, Mobile Apps, API's, Applications.

4. **Infrastructure Testing**: Servers, databases, firewalls, routers and where possible cloud environments
5. **Testing**: Conducting comprehensive testing to ensure the software is functioning as expected and is effective in detecting and preventing intrusions.
6. **Training**: Providing training to GIPF's IT staff on Vulnerability Assessment and Penetration Testing Services

4. METHODOLOGY

The proposed Vulnerability Assessment and Penetration Testing services should be a structured, risk-based approach designed to identify, analyze, and validate the security weaknesses across GIPF's information systems. The methodology may include, but not limited to the following phases:

4.1 Recognized Standards: Open Worldwide Application Security Platform (OWASP), Open Secure Security Testing Methodology Manual (OSSTMM), NIST SP 800-115, Penetration Testing Execution Standard (PTES).

4.2 Penetration Testing: Controlled and **NON-DESTRUCTIVE** exploitation of vulnerabilities to assess the impact.

4.3 Vulnerability Assessment:

4.4 Risk Rating: The risk rating to be based on the Common Vulnerability Scoring System (CVSS), or similar.

4.5 Testing Approach: The testing approach may be any of the following black-box, white-box, or grey-box.

5. DELIVERABLES

The following key diverables arising from the Vulnerability Assessment and Penetration Testing initiative, carried out to evalaute the effectiveness of current security controls, identify exploitable vulnerabilities and, assess GIPF's overall cyber-resillience posture.
The outcome of the Vulnerability Assessment and Penetration Testing initiative is designed to provide GIPF clear and implementable insights into the procedural and technical weakness across the in-scope applications, infrastructure, and systems as per below:

1. **Initial Engagement Plan: Includes the scope, testing methodology and timelines**
2. **Interim Updates: Intermittent progress reports during the testing.**

3. **Final Report: Includes but not limited to:**
    a An Executive Summary
    b Technical details of Vulnerabilities
    c Evidence of exploited vulnerabilities (logs, screenshots, dumps)
    d Risk ratings and prioritization
    e Remediation and mitigating controls
4. **Post-Engagement walkthrough**
5. **Optional Retest**

6. TIMELINE

The project is expected to be completed within specified time from the date of contract signing. The timeline should include all phases of the project, from supply to final testing and training.

7. REQUIREMENTS

Interested service providers are required to meet the below minimum requirements as part of the proposed submission.

7.1 A detailed proposal outlining their approach, methodology, and timeline.
7.2 A breakdown of costs, including licensing, installation, configuration, and support fees.
7.3 Company profile and relevant experience.
7.4 References from previous clients.

8. INSTRUCTIONS TO BIDDERS

Bidders are invited to submit their proposal(s) comprising of the following information:

8.1 Bidder and pricing information.
8.2 Technical proposal with value proposition.
8.3 Financial proposal clearly showing the cost for material and the work to be conducted.
8.4 All proposals are to be evaluated and the proposal with the highest cumulative score shall be deemed to be the “Successful Proposal” and awarded the proposed services.
8.5 GIPF is under no obligation to award the contract, nor is GIPF obliged to award the contract to the lowest bidder.

8.6 Where necessary, GIPF may invite shortlisted bidders for a demonstration of the services.

9. EVALUATION CRITERIA

The successful bidder will be appointed based on an implementation plan meeting the minimum requirements and instructions as outlined below.

	Description	Score
1.	Compliance with the technical requirements specified in the ToR	10
2.	Technical expertise and experience in Vulnerability Assessment and Penetration testing.	30
3.	The bidder has experience and provides a minimum of three (3) references or similar works demonstrating the undertaking of similar projects involving Vulnerability assessment and Penetration testing	15
4.	References from previous similar projects	5
5.	Quality of the proposal and approach	20
6.	Cost-effectiveness of the proposal.	20
Total Score		**100**

10. INCURRING COST

The Government Institutions Pension Fund assumes no responsibility or liability for costs incurred by the bidder for work performed in the preparation and production of their proposal or for any work performed prior to the signing of a contract.

11. ENQUIRIES

For all bid enquiries, contact the following person:

Ms. Gisela Naris
Procurement Officer
T +264-61-205-1746
E: gnaris@gipf.com.na

The last date for enquiries will be **20 March 2025.**

Business Hours are 08:00 to 16:30 (Monday to Friday).

12. CLOSING DATE AND SUBMISSION OF PROPOSALS

Proposals should be posted or hand delivered in sealed envelopes citing the bid number and detailing the services to be rendered as per details below:

The Chairperson: GIPF Procurement Committee

BID: CS/RFP/GIPF-02/2026: Vulnerability Assessment and Penetration Testing Consulting Services

GOVERNMENT INSTITUTIONS PENSION FUND
GIPF House, Ground Floor, Reception
Corner Dr Kenneth David Kaunda and Goethe Street
P.O. Box 23500
Windhoek, Namibia

Bidders are responsible for ensuring that their proposal reaches GIPF in good time.

Kindly provide your firm`s contact person details with the bid proposals to facilitate communication with our Procurement Office. Under no circumstances will GIPF be responsible for any late deliveries or loss of bid proposal documents.

The closing date for this bid is **27 March 2026 at 12:00 p.m.**

Proposals received after the deadline will not be considered.
