GIPF
Government Institutions
Pension Fund

To guard, and to grow.

RRP 003/2018

TERMS OF REFERENCE

GIPF ORACLE AUDIT VAULT AND DATABASE FIREWALL IMPLEMENTATION

Approval

	NAME	DESIGNATION	SIGNATURE	DATE
Originator:	Mrs Rebekka Murorua	Senior Database Administrator		
Recommended by:	Mr Ruben Ndjibu	Manager: IS Applications		
Executive Approval:	Mr Onno Amutenya	GM: Information Systems		

Revision History

Date	Version	Description	Author

Table of Contents

1. Summary

Oracle Audit Vault and Database Firewall (AVDF) can be defined as an enterprise data security and auditing software solution/framework that secures databases and other critical components of IT infrastructure (such as operating systems).

Within the scope of the Government Institutions Pension Fund (GIPF), the implementation of Oracle Audit Vault and Database Firewall solution is vital to providing first line defense of the Fund's relational databases and IT components to detect and mitigate IT security threats and risks in a timely manner.

The implementation is also essential to employing an on-premise solution that consolidates audit data from the different sources which includes databases, operating systems and directories; while making these audits available and accessible from a central repository.

2. Purpose

This document provides the scope and specification of the implementation of GIPF Oracle audit vault and database firewall solution. The implementation is regarded fundamental to achieving the following strategic objectives of the GIPF:

1. Enhance IS Governance, Risk and Compliance
    a. Implement information and data security management policy

3. General Statement

The specifications outlined in the context of the document do not necessarily provide a complete GIPF data and information security model but rather the general principles directing the configuration and implementation of the Oracle Data vault and Database Firewall solution including its supported software and hardware components within the GIPF environments.

The implementation should meet the minimum requirements and must be aligned to the conceptual design, technical specifications, training specifications and implementation strategies (scope of work) that are outlined in the context of the document. It is the objective of the implementation to fully realize the benefits of the solution including all functions and capabilities.

4. Background

Deliberating on the adaptation of relational databases and related products for the management of enterprise data and information within the GIPF, the implementation of the Oracle Data Vault and Database

Firewall Solution is vital to creating a platform for monitoring the traffic to/from the databases and related IT components in order to detect and block data security threats including improving compliance reporting by consolidating audit data from different databases, operating systems, directories, and other IT components.

The need to secure GIPF's valuable data and information is driven by the expansion of privacy and regulatory environment coupled with the rapid expansion of access to sensitive data of the Fund by the internal software development and support team, the Internet, increasingly dangerous world of hackers, insider threats, organized crime, groups with intentions of stealing valuable data. In addition there is a drive towards achieving greater efficiencies through emerging technologies, cloud computing and service oriented technologies.

The data security and compliance of the GIPF requires a defense-in-depth, multi-layered, security model that must include preventive, detective, and administrative controls that are aligned with the sensitivity of the data, location, environment, and applicable regulations.

In response to increased threats to the data and information of the Fund, GIPF have acquired a Oracle Audit Vault and Database Firewall Solution towards addressing the data and information security needs of the Fund and is now ready to acquire a suitable Oracle partner to assist in implementing the solution, training the internal staff and supporting the internal staff with the pre and post implementation activities.

The solution is intended to allow the Fund to detect timely questionable user errors or fraudulant intentions. In addition to allow auditors and IS Security officer to perform audits, queries and extract audited information that they need (ability to produce own reports).

5. Conceptual Design

The high-level configuration and implementation strategy of the GIPF Oracle Data Vault and Firewall Solution should adopt the standardized conceptual design and architecture recommended by Oracle (Figure 1).

The implementation should be deployed in a manner such that the solution is able to monitor the traffic from all core databases and IT components of the Fund and should be able to consolidate activity logs from both the production and data recovery sites into a central repository.

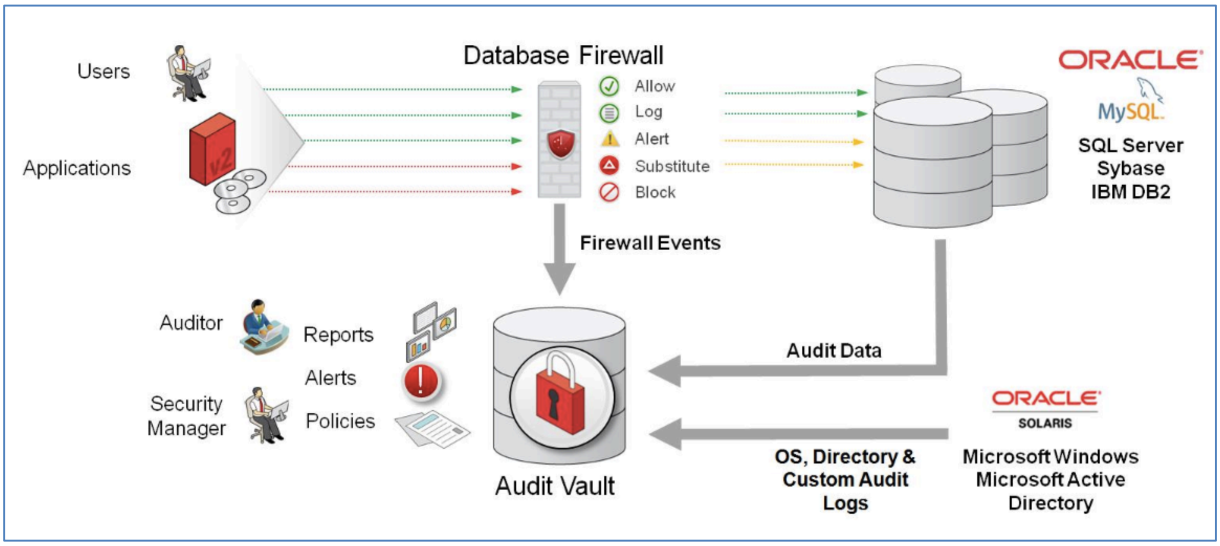

Figure 1: Conceptual design of the Oracle Audit Vault and Firewall Database solution

6. Technical specifications

The configuration and implementation should include the following minimum analysis, documentation and technical tasks:

6.1. Installation and configuration of the Database Firewall
6.2. Installation and activation of host monitoring
6.3. Installation and configuration of alerts and notifications
6.4. Development and configuration of custom collection add-ons
6.5. Deployment of Audit Vault Agents
6.6. Installation and configuration of the Audit Vault Server

7. Training specifications

As part of the internal staff development and skils acquisition, GIPF requires from the preffered service provider to facilitate, organise or provide training services to minimum ten (10) internal staffs in the following domains areas related to Oracle Audit vault and Database Firewall solution development, configuration, implementation and administration:

7.1. Implementing Oracle Audit Vault
7.2. Oracle Audit Vault and Database Firewall: Install & Configure
7.3. Oracle Audit Vault and Database Firewall: Policies & Reports Ed 1

8. Scope of work

The preffered Oracle parner is expected to conduct or provide the following services and task to the GIPF:

8.1. Collaborate with the internal software development, auditors, information security officer and management in defining and documenting the security standards and specification that will be adopted during the implementation.

8.2. Collaborate with the internal software development team (system developer, database administrator, business analyst, application administrator) in configuring and implementing the Oracle Audit vault and Database Firewall solution as per the defined conceptual, technical and training specifications.

8.3. Compile project documentation (project plan, activity plan, test plan, etc.)

8.4. Conduct training and transfer of skills to the internal software development team.

9. Expected Deliverables and Outcomes

The preferred Oracle partner is expected to deliver the following minimum deliverables to the GIPF:

9.1. A documentation of the Oracle AVDF architecture and process flow as implemented in the GIPF environment.

9.2. A documentation of the data security standards and procedures to be adopted by the GIPF.

9.3. Must deliver user and configuration manuals to be used by the internal team in supporting and maintenance of the solution.

9.4. All other deliverables required by this RFP.

10. General Terms and Conditions

All interested Oracle partners are expected to provide the following Project-related submissions:

10.1. A proposed implementation methodology, training schedule and proposed tasks during the pre and post implementation phase.

10.2. A proposed alternative Oracle database system deployment within GIPF and make appropriate recommendation.

10.3. Deliver a documentation outlining the project management team, skills and knowledge and costing for the post implementation support for period of 12 months.

10.4. CV/Resumes of all team members, highlighting experience relevant to this exercise. Individual CVs should not exceed 3 pages along with confirmation that the proposed team members will in fact be available to undertake this exercise at the appropriate time.

10.5. A project plan outlining the schedule of the implementation milestones including due dates for the implementation of Oracle Audit Vault at GIPF. The project plan should indicate a project start date as of 01 July 2018.

10.6. A fee structure and project duration for the Implementation must be attached.

Project-Related Submission Requirements.

10.7. Vendor's response must include: An overview that reflects the vendors' understanding of the efforts described in this Request for Proposals;

10.8. A detailed explanation of how the Vendor proposes to meet the Project objectives and requirements set forth above, including descriptions of the methodology that will be used and the deliverables that will be produced;

10.9. At least three (3) client references with appropriate contact information that the Vendor has performed work for in the past three (3) years and that can attest to vendor's ability to complete similar work at GIPF;

10.10. Brief company profile, ownership, as relevant to the above mentioned terms of reference.

10.11. Obligatory Original Certificate of Good Standing with the Social Security Commission. **(Original Stamp) Failure to do so will render the tender invalid.**

10.12. Obligatory Original Certificate of Good Standing with the Inland Revenue. **(Original Stamp) Failure to do so will render the tender invalid.**

10.13. All other information required by this RFP.

Kindly submit your tender to the Mr. E. Job, 3rd floor, GIPF House, in a sealed envelope marked:

The Chairperson: Procurement Committee
TENDER: RFP 003/2018 - GIPF Oracle Audit Vault and Database Firewall Implementation
GIPF House
Cnr Dr Kenneth David Kaunda & Goethe Streets
Windhoek
Namibia

Or e-mail to: ejob@gipf.com.na

Closing date and time: Thursday, 28 June 2018 at 12h00 p.m.

Late proposals will not be accepted or considered.