EMPLOYER	The Road Accident Fund
RFP NUMBER	RAF/2024/00014
DESCRIPTION	THE ROAD ACCIDENT FUND (RAF) SEEKS TO PROCURE DATA SECURITY PLATFORM COVERING DATA DISCOVERY AND CLASSIFICATION, DATA LEAKAGE PREVENTION, DATABASE ACTIVITY MONITORING, DATA ENCRYPTION, DATA MASKING AND TOKENISATION AND DATA PRIVACY AND DATA ACCESS GOVERNANCE FOR A PERIOD OF FIVE (5) YEARS
DATE OF PUBLICATION	28 March 2024
BID VALIDITY PERIOD	90 DAYS FROM THE BID CLOSING DATE
BID CLOSING DATE	26 April 2024
BID CLOSING TIME	11:00
TENDERS MUST BE HAND DELIVERED OR COURIERED TO	The Road Accident Fund (RAF) 420 Witch Hazel Avenue Eco Glades 2 Office Park, Block F (at reception into the Tender Box) Attention: RAF's Representative mentioned below
RAF'S REPRESENTATIVE	Shadi Matlou Shadim@raf.co.za

1. Is there a go-live implementation date in mind?
   A: This will be guided by SCM processes but as soon as contracting is concluded with the successful bidder, we will expect the engagement to start and be fast-tracked.

2. What is the end goal of the platform from a business requirements perspective – the document is more around technical requirements from a data platform but does not really give the end use case which would be helpful in responses.
   A: The primary use case is to enable to business to operate and leverage data that is adequately secured. Detailed use cases will be discussed with the successful bidder. Bidders are requested to submit a proposal based on the documented requirements and scope of work.

3. Is there an expectation for key personnel to be on site and if so is this just for any specific activities eg(Blueprint/Kickoff/UAT Testing) or would they need to be onsite for the total length of implementation?
   A: Resources will be required for the initial phase as well as the maintenance support phase. There is no hard requirement to have resources physically onsite.

   Initial/Project Management Phase

   a) Business requirements gathering
   b) Solution Design
   c) Integration Workshops
   d) Implementation

   Maintenance/Support Phase

   Resources will be required to support the deployed solutions. Bidders must include costing for support on a monthly basis (payable on a usage basis).

4. In order to design and size the solution license part in 4.10.1 Data Discovery and Classification, we would need to know:

   a) regarding structured data, the number of databases and

   b) for unstructured data the total volume (in TB) of unstructured data repositories (file systems, data lakes, blob storage - like S3 and OneDrive - and email stores).

   A: (a) Informix (4 environments one database on each environment)

   (b) 900 GB Informix

   1.4 TB (4 critical instance)

5. In order to design and size the solution license part in 4.10.2 Data Encryption and 4.10.3 Data Masking and Tokenisation, we would need to know the maximum number of data elements to protect. This could be the number of accounts, or customers, or users, or IDs , or entities that are being managed by the ecosystem of the applications in scope of the solution. The license is based on the largest of these numbers.

   A: Data level encryption

6. Regarding 4.10.2 Encryption, a) and b) are referring to files, correct? Or, are you also referring to other types of encryption, like volume level and others? Please define.

   A: This is referring to the encryption of data on data repositories (e.g. databases) and does not refer to file encryption on file shares for example.

7. Our solution can provide all the requested protection methods (encryption, masking and tokenisation) but we recommend using only tokenisation and masking for all structured and semi-structured data. This is because with our technology there is no keys distributed to users and applications which has the advantage of a) reducing the surface of attack and b) eliminate the administrative effort of key-lifecycle management. Would you be willing to consider a solution that implements only tokenisation and masking for structured and semi-structured data to take advantages of the benefits mentioned?

A: Please feel free to submit your solution as per the possible data protection methods but please take into consideration that there are points allocated to data encryption (both for Phase 3 and the demonstration phase). Points will be subtracted for any areas not covered in the bidders' responses.

8. Regarding 4.11.3 Security Requirements, b), ii) TLS. Is TLS v1.3 the only acceptable option? The modules of our solution communicate using SSH, which is an industry secure and accepted method. Would you accept that?
   A: Yes. SSH is perfectly fine as it falls into RAF-Approved standards.

9. Regarding 4.11.3 Security Requirements, a), i) MFA. Our protection solution does not interact directly with users (please see point 4 for an explanation). There is only one type of user that could directly interact with the cryptographic system (Admin) and for that we use a *Shamir's secret sharing scheme* implementing a model requiring the setup of a pool of unlock custodians and an unlock administrator, which eliminates the need for MFA implementation directly in the solution. For user and applications consuming the protection services, we integrate with IAM (Identity and Authorization Management) systems which, we assume, implement MFA. Can we than assume MFA is handled by the IAM system?

   A: MFA is handled by 3rd systems with RAF. We are happy with the explanation of users and applications consuming protection services. We require support for MFA for all administrative users. Please include the context provided for the admin account in the proposal for context.

10. 4.11.9. Interoperability. Integration with systems is required but we did not find a list of those systems. Could you please provide the list of the systems (including, vendor and version) the solution should be expected to integrate with? This shall include target systems for Discovery and Classification and Data Protection (like databases, operating systems and applications) but also supporting systems like SIEM, etc. (For example, SIEM is mentioned on page 25 but there is no definition of the SIEM in use).
    A: MS SQL 2016 and 2019, Oracle Enterprise Edition, Informix

11. Can you please advise on the following details :

- How many users = 4000
- How many DBS /Instances Informix (4 environments one database on each environment)
  SQL - 401 dbs including SharePoint Databases (5 instances Production) but 100 will be covered by the proposed solution.
- Training - Virtual Private Classes
- Virtual Public Classes
- In House/Onsite Training Classes

A: The solution should cater for around 4000 employees in general. From a data security platform perspective, please cater for 20 users. Training can be provided either as virtual classroom or in person classroom training. These classes must be ideally booked at the same time for RAF Personnel, to avoid individual self-paced training.

12. Number of AD users.

A:3200

13. Number of applications to be protected.

A: We have 34 on our catalogue

14. Number of databases to be protected.

A: Informix (4 environments one database on each environment)

SQL = **401** dbs (5 instances Production) but 100 will be covered by the proposed solution.

15. Number of servers with data to be protected

4 Servers on Informix

5 Instances SQL (4 Servers NB only critical systems)

16. What Structure data sources do RAF have e.g SQL, Oracle, Hadoop etc..?

A: SQL, Informix and Oracle

17. How many Databases do RAF have?

A: Informix (4 environments one database on each environment)

SQL - 401 dbs (5 instances Production)

18. How many Nodes per data base cluster do RAF have

A: SQL – N/A

19. How many Database tables across the RAF Structured data estate and how regular do you want to scan these tables?

A:Daily

20. How many TB of unstructured data do RAF have?

A: 900 GB Informix

1.4 TB (4 critical instance)

21. How many users will need to make use of the Multifactor solution.

    A: Multi-Factor is not part of this RFP scope and it will be provided for by RAF. Bidders only need to show that their proposed solution supports MFA.

22. Point 4.10.6 Privacy and Compliance how many end user will make use of Consent management?

    A: This will be a feature that would need to be phased in over time. We can start with at least 10 000 users.