Questions and answers for Penetration Testing Platform

1. **Customer Channel Pentesting**

What are the exact components in scope?

- Service desk software
  - **Answer: Heat/Ivanti**
- Call center platform (e.g. Genesys, Cisco UCCX, Avaya)?
  - **Answer: RAF has outsourced the call center to a third-party service provider.**
- Self-service portals (web-based, mobile)? Web-based (hosted on premed)
  - **Answer: Multi-channel self-service touchpoints (Web, Chatbot and WhatsApp), hosted in a third-party location**
- Chatbots (web chat, whatsapp, internal tools)?
  - **Answer: Multi-channel self-service touchpoints (Web, Chatbot and WhatsApp), hosted in a third-party location**
- Are APIs or integrators also in scope?
  - **Answer: Yes. The call center integrates with RAF internal systems through an API gateway. A comprehensive pen test is required for the call center environment (holistically)**
- Are these systems hosted on-prem, in the cloud, or hybrid?
  - **Answer: Hybrid**
- Will test accounts be provided?
  - **Answer: Yes, if required, however bidders are expected to propose a methodology for conducting these penetration tests.**
- Is VPN or remote desk access needed to reach internal systems?
  - **Answer: Yes (Service Desk)**
  - **Answer: No (Call Center)**

2. **Mobile Pentest**

- Application name:
- IOS/Android:
- Available in App Store?
- Includes Web API?
- Login functions?
- Registration/Signup functions?
- Authenticated testing required?

Answer: The RAF currently does not have a mobile App. This is currently in development. Bidders are expected to propose a methodology for mobile app pen testing based on the quantities provided.

3. External Network Pentest

Number of external IPs and/or Network Ranges

- **Answer: Various public subnets in hybrid cloud/on premises environment 2 data centers, 3 cloud environments.**

How many of those are live assets?
Answer:

- **+- 30 websites**
- **+- 70 cloud resources**
- **+- 146 public IP addresses**

How many of these are web applications/websites:
Answer:

- **RAF has one 1 main website**
- **+- 29 other web services accessible**

4. Internal Network Pentest

Number of internal IPs and/or Network Ranges
Answer:

- **Subnet ranges cannot be shared.**
- **RAF has 2 on premises data centers and presence in AWS and Azure cloud environments. All these environments host internal systems.**

Approximate number of servers, workstations, and any other devices on the network:
Servers:
Answer:

- **+-436 (Including Linux and Windows)**
- **Workstations: +- 3500**
- **Other network-connected devices +- 500**

Is the network segmented?

- **Answer: Yes**

5. Web App Pentest

General function and overview of web apps

- **Answer: Every application serves a different purpose in the claim value chain e.g supplier claim systems.**

Classification of data used by the applications:?

- **Answer: Various classification levels from public to confidential (including personally identifiable information, financial information and health/medical information)**

Any browser requirements to access the applications:

- **Answer: This will be web application-dependent. Various browsers supported, however some web applications may require specific browsers.**

Are the applications behind a WAF:

- **Answer: Mostly but this depends on the web application and its criticality**
- If yes, is whitelisting allowed?
- **Answer: Yes**

Will it be unauthenticated or authenticated testing?

- **Answer: The bidder must propose a methodology that would simulate adversarial methods (authenticated and unauthenticated)**

How many unique user roles does the application have?

- **Answer: Varies per application**

User roles matrix / breakdown

- **Answer: Varies per application**

6. API Pentest

REST/SOAP/Other API

- **Answer: Mostly REST APIs**

How many APIs?

- **Answer: Refer to the RFB document for the number of API integrations per year**

How many requests per API?

- **Answer: Each API integration needs to be tested annualy as per the RFB document**

Authentication required?

- **Answer: Mostly yes but this will be engagement/scenario-specific**

Are the endpoints behind a WAF:

- **Answer: Yes**

7. Cloud Security Pentesting

Which cloud service provider are in use? AWS / Azure / GCP / Oracle / others?

Answer:

- **AWS and Azure (IaaS)**
- **Other SaaS providers**

What is the deployment model? Public cloud, private cloud, hybrid or multi-cloud:

- **Answer: Hybrid Multi-Cloud**

Are containers or Kubernetes used in the cloud environment?

- **Answer: No**

What services are in-scope for the test?

- Compute,
  - **Answer: Yes**
- Serverless
  - **Answer: Yes**
- Storage
  - **Answer: Yes**
- Databases
  - **Answer: Yes**
- Identity
  - **Answer: Yes**

Are SaaS, PaaS and/or IaaS included?

- **Answer: Yes, RAF is hybrid environment (PaaS, IaaS, SaaS).**

Are API endpoints or management interfaces in-scope?

- **Answer: API endpoints will be covered in the API testing section of the RFB**

What level of access will be provided for testing?

- Blackbox (no credentials)
- Greybox (limited IAM credentials)
- Whitebox (admin or root account)

Answer: This will depend on an agreed scope for each cloud pen testing engagement

8. Code Pentesting

What programming languages and frameworks are used?

- **Answer: Predominantly using C#**

What is the size of the codebases:

- **Answer: Will vary depending on specific engagements**

Are third-party or opensource libraries extensively used?

- **Answer: Yes**

Will we receive full access to the source code?

- **Answer: To be determined for specific testing scope**

Are there build or test environments available?

- **Answer: Yes**

Is documentation available?

- **Answer: Partially, some documentation on legacy systems is not available.**

Is sensitive data handled in the app:

- **Answer: Yes**

Are secure coding standards in place?:

- **Answer: Yes**

Should we check for compliance with standards like PCI-DSS, ISO, etc.?

- **Answer: Yes**

Are we allowed to run static analysis tools on the code?

- **Answer: Yes**

Are there CI/CD pipelines involved?

- **Answer: Not yet**

9. Wireless Pentest

How many SSIDs to be tested?

- **Answer: +- 4**

10. Red Teaming

We need to understand a bit more surrounding the objectives and narratives they want to follow for the red team.

What does “bi-annual” red teaming mean to you?

- **Answer: Test will be conducted twice a year. RAF intends to use these engagements to refine its cybersecurity controls**

Full-scope red team every six months?

- **Answer: No**

Smaller focussed simulations twice a year?

- **Answer: Yes**

How mature is your current blue team or SOC?

- **Answer: Intermediate to Mature**

Are you suing SIEM, SOAR, XDR/EDR?

- **Answer: Yes**

Whats’ the expected outcome of the engagement?

- Technical findings?
  - **Answer: Yes**
- Tactical and strategic recommendations?
  - **Answer: Yes**
- Purple team handover?

- **Answer: No**

What is the scope of systems and infrastructure that may be targeted?

- **Answer: Network endpoints, network infrastructure, servers, email/internet security systems; and identity and access management systems.**

Are physical facilities in-scope for social engineering or physical intrusion testing?

- **Answer: No**

Are we allowed to interact with production systems or should tests be confined to replicates/staging?

- **Answer: This will be based on each engagement scope, but the RAF would expect these engagements to also cover production systems, while balancing against undesired adverse impact on systems.**

Should this be a fully covert, partially covert, or collaborative (purple team) exercise?

- **Answer: Partially covert and Collaborative**

11. SAP Pentesting

What are the goals of the SAP pentest?

- Identify misconfigurations and vulnerabilities in SAP applications?
  - **Answer: Yes**
- Assess custom business logic or ABAP code security:
  - **Answer: Yes - customised development (ABAP)**
- Validate integration security?
  - **Answer: Yes - Process Integration/Process orchestration layers**
- Simulate unauthorised access or insider threats?
  - **Answer: Yes – This is extremely important**

Are we expected to simulate authenticated users, external attackers or both.

- **Answer: Both**

Will this include a combination of technical vulnerability discovery and business logic abuse testing?

- **Answer: Yes**

Which SAP applications are in scope?

Answer:

- **SAP ECC, SAP GRC, SAP BW, enterprise portal and SuccessFactors**
- **Bidders must also take note that RAF intends to migrate on premises SAP instances to SAP 4/HANA**

What is the architecture of the SAP landscape?

- Single system or distributed?
  - **Answer: Distributed**

- On-premises, cloud or hybrid?
- **Answer: Hybrid**

Are SAP interfaces integrated with third-party systems?

- **Answer: Yes**

If yes, which protocols? (SOAP, REST, RFC, OData)?

- **Answer: All the above-mentioned**

Are any SAP services or portals exposed to the internet?

- **Answer: Yes**

12. Database Pentesting

Main goals of the database pentest?

- Identify misconfigurations and weak access controls?
  - **Answer: Yes**
- Assess encryption, auditing, or data loss prevention controls?
  - **Answer: Yes**
- Simulate internal or external threat actors accessing sensitive data?
  - **Answer: Yes**
- Are the tests focused on unauthorised data access, privilege escalation, and lateral movement?
  - **Answer: Yes**
- Should we test both technical and procedural controls? (e.g. access provisioning, data retention, auditing)
  - **Answer: Yes**

How many instances of each database platform are in scope?

Answer:

- **Informix +- 3**
- **Oracle +- 9**
- **Microsoft SQL +- 8**
- **MySQL (RDS) +- 8**

What level of access will be provided for the test?

- **Answer: Read-only access**

Are the databases hosted on-premises, in the cloud or hybrid?

- **Answer: Hybrid**

Are the databases directly accessible on the network or through application layers?

- **Answer: Both**

Will we be testing databases directly or also via APIs and connected services?

- **Answer: Directly**

13. Under Point 4: Scope of Requirements and Point 5.2.2, there are references to the number of applications to be tested annually per area. For example, Code Penetration Testing states that 10 QA assessments are to be conducted on in-house applications per year, with billing applicable per application.

    However, under Section 3: Pricing Schedule Table, Code Penetration Testing reflects only 4 engagements per year. Similar inconsistencies appear in other service/scope areas as well.

    Could you please confirm whether pricing should be aligned with the quantities listed under *Points 4 and 5.2.2*, or with the figures presented in the Pricing Schedule Table?

    Answer: Pricing must be aligned with quantities listed in points 4 and 5.2.2.

14. Is the annual penetration testing exercise on Service Desk Systems and Call Centre Systems limited to vishing only, or may the service provider also attempt to exploit vulnerabilities identified within the Service Desk and Call Centre infrastructures?
    - **Answer: This will be guided by the pen testing engagement scope and rules of engagement per engagement. Bidders must propose a methodology for conducting these assessments.**

15. Could you clarify the meaning of "billed per service desk system penetration testing engagement" and "billed per customer channel penetration testing engagement"? **Please refer to the RFP document.**
    - **Answer: RAF has 1 service desk solution. There will be one pen test engagement per year against this system. The same for the outsourced contact centre, which will require one pen test engagement per year.**

16. On which operating systems are the two mobile applications in-scope running (Android, iOS, or HarmonyOS)?
    - **Answer: Already answered**

17. Are the two mobile applications in-scope available from app stores, and if so, will the links be provided?
    - **Answer: Already answered**

18. Do both mobile applications interact with back-end APIs?

- **Answer: Already answered**

19. For the external penetration test, what is the total number of external-facing IP addresses?
    - **Answer: Already answered**

20. For the internal penetration test, what is the total number of internal-facing IP addresses?
    - **Answer: Already answered**

21. Amongst the ten web applications in-scope, are any hosted by a cloud service provider:
    - **Answer: Yes**

22. Whether they are looking for blackbox, grey box or white box pentest services.
    - **Answer: This will vary depending on each engagement**

23. Number of public Ips
    - **Answer: Already answered**

24. Number of APIs and websites (subdomains/domains), apps included (internal/external):
    - **Answer: Already answered**

25. Number of mobile apps
    - **Answer: Already answered**

26. Number of servers/workstations in scope:
    - **Answer: Already answered**

27. Number of employees (social engineer):
    - **Answer: +- 200 users**

28. Number of SAP applications

- **Answer: Already answered**

29. Number of applications for SAST assessment:

- **Answer: As per the RFB document (10 per year)**

30. Consent Management

The Proposed solution should have consent management capabilities such as privacy permission, opt out and opt in requirements. The solution should have a compliance tracker for data privacy in line with consent management.

Q. Can you elaborate more the use case around Consent Management ? Do you need a Consent Management Platform to store all users' consents coming from Applications (Consumer applications) ? Can you provide an example of the use case of data privacy and consent management in line data?

- **Answer This is not related to nor contained in this RFP**

31. Privacy Management

The proposed solution should allow administrators to easily populate and publish privacy notice updates across various websites and applications.

- **Answer This is not related to nor contained in this RFP**

32. Do you need to centrally manage (create/update, publish, track users' acceptance) the Privacy Statements and/or Terms and Conditions of your consumer applications?

- **Answer This is not related to nor contained in this RFP**

33: In the case where penetration testing resources are offshore, would RAF accept equivalent background verification reports from internationally recognized vetting agencies in lieu of MIE checks, provided they cover qualifications, criminal, and integrity checks?

- **Answer: This will be informed by the RAF departments responsible for vetting/background checks during onboarding.**

34: Please confirm which cloud platform(s) (AWS, Azure,) are in scope and the estimated number of services/environments expected to be assessed.

- **Answer: Environment (AWS and Azure), 12 AWS accounts, +- 430 servers (UNIX, Linux and Windows) across cloud and on premises environments.**

35: Can you please provide the scope breakdown for SAP penetration testing and other areas. To quantify the effort required.

Answer: please refer to the similar question asked:

SAP Pentesting

- What are the goals of the SAP pentest?
    - Identify misconfigurations and vulnerabilities in SAP applications?
        - **Answer: Yes**
    - Assess custom business logic or ABAP code security:
        - **Answer: Yes - customised development (ABAP)**
    - Validate integration security?
        - **Answer: Yes - Process Integration/Process orchestration layers**
    - Simulate unauthorised access or insider threats?
        - **Answer: Yes – This is extremely important**
- Are we expected to simulate authenticated users, external attackers or both.
    - **Answer: Both**
- Will this include a combination of technical vulnerability discovery and business logic abuse testing?
    - **Answer: Yes**

Which SAP applications are in scope?

Answer:

- **SAP ECC, SAP GRC, SAP BW, enterprise portal and SuccessFactors**
- **Bidders must also take note that RAF intends to migrate on premises SAP instances to SAP 4/HANA**

What is the architecture of the SAP landscape?

- Single system or distributed?
    - **Answer: Distributed**
- On-premises, cloud or hybrid?
    - **Answer: Hybrid**

Are SAP interfaces integrated with third-party systems?

- **Answer: Yes**

If yes, which protocols? (SOAP, REST, RFC, OData)?

- **Answer: All of the above-mentioned**

Are any SAP services or portals exposed to the internet?

- **Answer: Yes**

36: Could RAF kindly confirm the expected team structure and time commitments for the engagement or its just the two resources named in the RFP document. For example, does RAF anticipate the need for a dedicated resource onsite or remote availability for certain phases?

- **Answer: There is no need for dedicated resources. Bidders will be engaged as and when certain penetration testing engagements are required. Bidders are, however, required to submit the 2 resources for evaluation purposes.**

37: Are there any preferred tools or platforms that RAF expects the service provider to use.

- **Answer: No**

38: Is it acceptable to deliver the penetration testing requirement as a service, driven by resource engagement based on your needs?

- **Answer: Yes**

39: Are we required to submit CV's for each cluster, or is the RAF seeking a single individual who possesses all the required experience and certifications?

- **Answer: Resources are not required for each cluster. Bidders must submit the resources requested in the RFB document, at a minimum. Bidders may submit additional resources based on their proposals.**

40: During the process of completing and compiling the tender documents, are walk-ins permitted for queries, or should all questions be addressed via phone call or email?

- **Answer: Please refer to the RFB document. All RFB-related questions are to be communicated via the stated email address.**

41: Can the tender be submitted before the closing date, or must it be submitted specifically on the closing date

- **Answer: Bidders can submit before the closing date**