

Contact Person: C. Zlatinis
Tel.: +30 210 320 2829

Open Tender No PU.2024.09A – Clarifications #1

Regarding the Open Tender with Reference Number PU.2024.09A, please find below the questions of some bidders and their respective answers.

Question #1:

What specific data sources does the Bank of Greece prefer for vulnerability assessment and monitoring?

Answer #1:

Assets faced to Internet.

Question #2:

Are there existing systems or tools the platform must integrate with?

Answer #2:

SIEM: IBM Qradar.

Question #3:

The SLA's are to be applied on the platform, platform support, or the protection and support services?

Answer #3:

Protection and support services.

Question #4:

Can you clarify the different user roles that will need access to the platform, and any specific permissions required for each?

Answer #4:

Admin role / viewer role.

Question #5:

What format for training (on-site, remote, hybrid) is preferred by the Bank? Are there specific training topics of priority?

Answer #5:

Remote training on the platform.

Question #6:

What procedures does the Bank currently have in place for responding to cybersecurity incidents?

Answer #6:

Approved and published to internet Policy and Procedure / csirt team.

Question #7:

How often (on average) are the third-party scans and risk scorings required to be executed (i.e. monthly, quarterly)?

Answer #7:

Daily is acceptable.

Question #8:

Do you accept a single price for each of the 5 years which would take all your requirements and offer them as a service? Therefore, not having a separate implementation cost, platform cost, or service, but a single total price?

Answer #8:

BoG will accept a single price; however, it will be depended on the range of third parties.

Question #9:

Appendix A, #7: Do you expect the proposed list of actions stemming from findings to be executed by the platform or by a security analyst as part of the protection and support service?

Answer #9:

Either a platform or a security analyst.

Question #10:

Appendix A, #10: Do you expect the platform to have a predefined list of third parties (e.g. System Integrators, Payment Processors, Acquirers, Software Vendors)? Do you allow the manual addition of 3rd party vendors (e.g. local vendors)?

Answer #10:

Both, but it is not a critical issue.

Question #11:

Appendix A, #29: The term "Organization's Portfolio" refers to the third parties that are to be monitored/evaluated?

Answer #11:

Both organization and third parties.

Question #12:

Appendix A, #29: Will the alerts be viewed directly by the proposed platform, or will it be integrated with the Bank's SIEM platform?

Answer #12:

Both.

Question #13:

Appendix A, #33: Is integration with the BoG SIEM required to monitor the proposed platform, or specific data collected by the platform regarding BoG and its third-party vulnerabilities?

Answer #13:

Specific data collected by the platform.

Question #14:

Appendix A, #34: Which Ticketing Systems is employed by BoG?

Answer #14:

SMax.

Question #15:

Appendix A, #43: Is the designated advisor required on a full-time basis?

Answer #15:

Negative! Just for explaining findings and actions & onboarding third parties.

Question #16:

Appendix A, #43: Based on your current baselines, how many reports do you expect to be generated daily/weekly/monthly that the designated advisor will need to handle?

Answer #16:

Weekly, but in case of upgrade/downgrade it would be useful to have a report.

Question #17:

Appendix A, #46: Which type of service do you require 24/7 support for? for the platform or for the services requested in #43 & #44?

Answer #17:

24/7 refers to platform availability.

Question #18:

Payment: What are the typical payment terms the Bank of Greece supports (after the approval from the designated Commission)? Are 30 days payment after approval accepted by the Bank of Greece?

Answer #18:

If there are user licenses will be processed immediately upon receipt otherwise payment for the implementation, protection and support services will be subject to approval by a Commission designated by the Bank or by the pertinent business unit, after completion of the relevant implementation work, and the corresponding tests and one month of proper production operation. Paragraph 22.

Question #19:

Payment: Can the same payment terms be applied to the protection and support services?

Answer #19:

We may discuss it after the bulk onboarding of third parties.

Question #20:

What is Bank of Greece Vulnerability product that we need to interface with?

Answer #20:

There is no such need. We are expecting the platform to scan the assets public to internet.

Question #21:

Section 22 – Right to increase / Decrease quantity

The Bank reserves the right to modify the quantity of items supplied (licenses, implementation, protection, and support services) by a percentage not exceeding 30% or not less than 50% of the total quantity originally awarded or of the quantity of each item, without any right or claim by the participant for compensation, price increase, etc.

- *If the bank decides to decrease by 50% the quantity, our company will not be deducted with any amount due to this reduction and receive the full 100% as it will offer?*

Answer #21:

The Bank is only going to increase the quantity and not to decrease. The modification concerns only the number of third parties.

Question #22:

Section 26.1.1 : Penalty Clause

- *What does the rate for each day that will be calculated is based on? (SW licenses, Implementation, Support , Other)?*

Answer #22:

On the delivery of SW licenses and the support services depending on your delay.

Question #23:

Regarding the Bid Bond title. Should it read:

«FOR TENDER PROCEDURE No. PU.2024.09A OF THE BANK OF GREECE REGARDING THE “PROCUREMENT OF A CYBER RISK PLATFORM TO COLLECT VULNERABILITY DATA OF THE BANK’S PUBLIC INFRASTRUCTURE AND MANAGE THIRD PARTY RISK FROM CYBER THREATS”»?

Answer #23:

Affirmative, the description is correct.

Question #24:

Date of Bid Bond expiration, should it be 8th October 2024 + 90 days = 8th January 2025?

Answer #24:

The expiration of Bid Bond should be on 7th January 2025 or later.

Question #25:

Should all documents and statement be signed electronically? Should hard copies be submitted as well?

Answer #25:

All documents and statement must be signed electronically and submitted via the CosmoOne platform. No hard copies will be accepted at any point of the tender process.

Question #26:

What is the total number of third parties the bank engages with and how many will be in scope for the specific project?

Answer #26:

You should provide us with the cost depending on the range of vendors’ number (it is referred in the RFP) that the Bank will choose.

Question #27:

Is there a breakdown of numbers of vendor based upon tiering?

Answer #27:

It is in progress.

Question #28:

Do you have existing questionnaires in use to assess third parties?

Answer #28:

No but we have included in our contracts SLAs, security requirements and certifications.

Question #29:

Do you have an existing third-party security due-diligence process?

Answer #29:

We do not have something more than the above for security due-diligence process.

Question #30:

Which other applications/tooling do you utilise for procurement?

Answer #30:

No other applications are used for procurement, except the CosmoONE platform.

Question #31:

We assume that documents extracted by the Greek public authorities do not need to be signed electronically. Please confirm.

Answer #31:

The documents that bear a unique authentication stamp (i.e. QR code), do not require any type of signature.

Dimitrios Verginis
Director
Procurement Unit