

Tender Announcement

Procurer:	ProCredit Bank AD Skopje
Name of tender:	Penetration testing of Bank's IT Systems and social engineering
Number of tender:	02/2017
e-mail:	tenders@procreditbank.com.mk
Fax:	+389 (02) 321 99 01

Date of announcement of tender: 01.06.2017
Final date for sending offers: 15.06.2017

PROCREDIT BANK MACEDONIA

Penetration testing of Bank's IT systems and social engineering

1. INTRODUCTION

INSTRUCTIONS TO BIDDERS

ProCredit Bank, hereinafter the Bank, is planning to conduct penetration testing of its information technology systems (for website, e-banking, remote access & other internet facing applications), 24/7 zones (Financial Kiosk) and social engineering, and is hereby looking for a company to conduct this security check on its behalf. The goal of this project is to get a picture of any vulnerability the Bank's systems may be exposed to, and to remediate the vulnerabilities (if any) before there is any attempt to exploit them. As this is an annual

ProCredit Bank
Manapo 7
1000 Skopje, Macedonia
S.W.I.F.T.: PRBUMK22

Phone +389 2 244 60 00
Fax +389 2 321 99 01
info@procreditbank.com.mk
www.procreditbank.com.mk

Members of Managing Board:
Jovanka Joleska Popovska, General Manager
Emilija Spirovska, Member of Managing Board
Mimoza Godanci Aliu, Member of Managing Board



Confidential

exercise, the Bank is soliciting proposals for 1-3 years, and would require the bidder to provide financial quotes for all options. If a contract longer than a year is awarded, then the bidder will provide the Bank with an annual report for the duration of the contract identifying areas of weakness that should be addressed, as per scope agreed upon.

Penetration testing will be performed either by the bidder separately (always with a prior notification and provision of testing details to the Bank) or in cooperation with authorized Bank representatives.

2. TESTING SCENARIOS

This bid package includes delivery of a specific report to the Bank.

A. Penetration testing scenario

Description: All companies should present a proposal for the penetration testing scenario which has partial input from the Bank, i.e. the company will perform the testing by fully coordinating all actions and notifying the Bank in advance for the time, details of scanning, and testing, however the Bank will give many details of IT infrastructure inside the Bank, including provisioning of user access to its e-banking or e-signing platform to perform tests as an insider. In the technical proposal, please specify what information will be required by you to complete this scenario. In the financial proposal, please specify the price separately for this scenario. Assessment should include:

- Performing internal and external vulnerability testing, including Network layer penetration test, application layer penetration test and the social engineering vector.
- Comparison of current security measures with best practices, business objectives and regulatory requirements.
- Review of technical controls in place.

B. Penetration testing documentation

The bidder should agree to deliver at the end of testing a full report to the Bank. The report should contain, but not limited to, the following information:

- Executive summary
- Detailed Summary (Issue/Vulnerability/Threat Types, Identified issues/ vulnerabilities/ threats Risk Rating Remediation Tasks, Total Risk Rating)
- Description of the methodology, which will be used
- Project Management Approach
- Scope, Approach and Methodology





ProCredit Bank

Macedonia

ProCredit Bank, Manapo 7, 1000 Skopje, Macedonia

Confidential

- Planning
- Exploitation
- Reporting
- Detailed findings (High Severity Issues, Medium Severity Issues, Low Severity Issues, findings, including assessment of level of vulnerabilities, potential impact, likelihood of occurrence, risk analysis and evaluation, rating calculation including the types of risk identified, recommendations).
- Detailed proposal for remediation tasks
- References for recommendations or findings.
- Position of the organization based on the identified findings

C. General points

Time: Time of testing should always be coordinated with the Bank in order to minimize any disturbances to daily business operations, and a sufficient period should be specified to meet all the expectations of the proposal.

Impact: Testing scenarios should not affect or disrupt regular activities of tested system.

List of applications used: The Company should present the list of all tools and applications that will be used during the testing.

Subcontracting: Not preferred

D. Appendix

Timeline

Project Team Staffing

Company Overview

Company References

*ProCredit Bank
Manapo 7
1000 Skopje, Macedonia
S.W.I.F.T.: PRBUMK22*

*Phone +389 2 244 60 00
Fax +389 2 321 99 01
info@procreditbank.com.mk
www.procreditbank.com.mk*

*Members of Managing Board:
Jovanka Joleska Popovska, General Manager
Emilija Spirovska, Member of Managing Board
Mimoza Godanci Aliu, Member of Managing Board*



Confidential

F. Ownership and confidentiality agreement

All information included in this technical specification, as well as a result of penetration testing belongs to ProCredit Bank Macedonia. This RFP is both confidential and proprietary to the Bank and is solely for your company's use in preparation of a proposal. ProCredit Bank Macedonia shall be direct and sole owner of all information, and companies obtaining this document, as well as the one selected to perform penetration testing should fully preserve the security of information, and be classified as Confidential as per Bank's Information Security

Policy. You agree that such information will be kept confidential and will not, without prior written consent of the Bank be disclosed by you in any manner whatsoever, in whole or in part. Target audiences for report distribution should be strictly agreed upon with authorized Bank representatives.

The selected company need to sign Non-disclosure agreement prior beginning of any activities that are subject to this engagement.

Form and contents of the offer:

1. The offer is prepared in written form
2. The offer should contain:
 - a. Name, address and place of residence of the Bidder, telephone numbers and fax numbers, e-mail addresses and contact persons
 - b. Price of the bid, with separately calculated VAT. The price should be expressed in local currency- denars.
 - c. Manner of payment
 - d. Evidence of quality (certificate of quality)
 - e. Reference List
 - f. "Tekovna sostojba" issued by the Central Registry- for local bidders
 - g. Anticorruption statement signed by the bidder
 - h. **In case a foreign legal or physical entity is a bidder, he submits an audit report from the legal entity issued by a renowned audit house;**

The documents are submitted in original form or copies and should not be older than 6 (six) months.

The offer and the documents should be written in Macedonian or English Language.

G. Scoring

Scoring of qualifying proposals will be as follows:

- Overall cost of proposal (pricing) 55 points



Confidential

- Expertise, quality and relevant certificates of the bidder and the team that will perform the testing 15 points
- Experience of the bidder with engagements as required, through appropriate reference list of performed penetration tests of web applications 15 points
- Approach, methodology and Project Plan (including project schedule and description of deliverables) 05 points
- Cooperation with the Bank 10 points

The selected suppliers are obliged to open accounts in ProCredit Bank AD Skopje.

The payment will take place in a time period established by law.

They should be sent in closed envelope, labeled “Do not open” and “For tender” to the below given address:

Str. Manapo 7, Skopje

Labeled: **Tender for penetration testing of Bank’s IT systems and social engineering num. 02/2017.**

The offers which have arrived by e-mail or fax, and offers that have arrived after the period has expired, offers addressed to employees of ProCredit Bank shall not be considered valid during the deciding upon the tender.

The envelope must not contain any label thereby the submitter can be identified.

The arithmetic errors will be corrected according to certain rules in line with the practice. It is possible that in some cases there might be an error in the sum, meaning that the price for one unit and the price in total are not corresponding. In this case the price for one unit will be considered correct and the price in total will be adjusted. In other cases there might be a mismatch between the price expressed in numbers and the price expressed in letters, if so the price expressed in letters is considered correct, or there could be mismatch between the price for one unit with VAT included and the price for one unit without VAT, in this case the price for one unit without VAT will be considered correct.

