Anexa nr.3
la Caietul de sarcini

Cerințele cu privire la serviciile de audit comprehensiv de securitate IT pentru soluția de plăți instant

I. CERINȚE FAȚĂ DE OFERTA TEHNICĂ ȘI FINANCIARĂ

1.1. Prevederi generale

1.1.1. Acest capitol descrie cerințele referitoare la formatul și structura ofertei.

1.1.2. Este necesar ca Ofertantul să facă cunoștință cu toate instrucțiunile, formularele, condițiile incluse în prezentul document.

1.1.3. Ofertele trebuie să fie complete și suficient de detaliate, astfel încât să îi ofere Autorității contractante posibilitatea de a înțelege cu ușurință toate aspectele. Ofertele vor include secțiunile descrise mai jos, fiind întocmite în conformitate cu cerințele față de oferta tehnică.

1.2. Oferta tehnică

Oferta tehnică va cuprinde următoarele elemente, dar fără a se limita la acestea:

a. Înțelegerea obiectivelor proiectului de către Ofertant, precum și a perspectivei asupra modului în care acestea pot fi realizate, perimetrul proiectului, delimitarea activităților din afara perimetrului.

b. Sumar executiv - privire de ansamblu asupra procedurii de evaluare a testării securității sistemului informatic al BNM: etape, livrabile, limitări, etc., inclusiv opinia Ofertantul cu privire la dificultăți/probleme întâlnite de obicei în astfel de evaluări și modul în care abordarea propusă și alte măsuri pot asigura o bună evaluare a securității unui sistem informatic.

c. Ipoteze de lucru pentru proiect în general și pentru fiecare etapă sau aspect în parte, după cum se consideră necesar.

d. Descrierea abordării, metodologiilor, tehnicilor și standardelor utilizate în efectuarea evaluării și testării pentru fiecare etapă în parte (pre-evaluare, evaluare, post-evaluare), precum și o scurtă prezentare a acestora (ex. NIST, OSSTM, ISACA, ISSAF, ISO, COSO ERM). Ofertantul va oferi exemple de livrabile pentru fiecare etapă care vor respecta cerințele din prezentul caiet de sarcini. De asemenea, Ofertantul va descrie pentru fiecare etapă: obiectivele, principalele activități, precum și instrumentele și mijloacele specifice utilizate pentru a le realiza.

e. Răspunsul la cerințele specificate din prezentul caiet de sarcini. În această secțiune, Ofertantul trebuie să includă toate informațiile tehnice și profesionale care vor îndeplini toate cerințele descrise în Caietul de sarcini. Întru asigurarea unei înțelegeri complete de către Ofertant și Autoritatea contractantă a cerințelor și răspunsurilor, Ofertantul trebuie să ofere răspunsuri detaliate la toate cerințele înaintate. Răspunsurile trebuie să fie însoțite de dovezi corespunzătoare, documente care să descrie livrabilele aferente proiectului, explicații, extrase din documentația de însoțire, modele care vor respecta cerințele din prezentul caiet de sarcini, etc, exemple de livrabile aferente etapelor de proiect (plan de acțiuni, raport de analiză, plan de testare, raport de testare,raport de audit).

f. Descrierea managementul proiectului:

- Structura organizatorică a proiectului;
- Abordarea de gestionare a proiectului, inclusiv abordarea de asigurare a calității;
- Plan de management al proiectului, care să acopere cel puțin următoarele elemente inițiale: planul proiectului (etapele, durata, responsabilități etc.), plan de management al calității, plan de gestionare a riscurilor, plan de gestionare a resurselor, planul de comunicare. Planul de management va include în anexă la documentele de inițiere a proiectului și registrele de riscuri, probleme, livrabile, comunicare, modelele rapoartelor aferent etapelor, de excepție, de închidere a proiectului; modelele proceselor verbale urmare a ședințelor, etc.

1.3.Oferta financiară

1.3.1. Oferta financiară trebuie să fie întocmită conform Anexei nr. 2 ”Specificații de preț” al prezentului Caiet de sarcini. Acest proiect este un proiect cu preț fix cu toleranța zero de cost (buget), respectiv solicitări de mărire sau revizuire a prețului nu vor fi admise.

1.3.2. Oferta financiară trebuie să fie clar întocmită, care ar asigura o bună înțelegere de către Autoritatea contractantă în ceea ce privește oferta formulată.

II. CERINȚE FAȚĂ DE SERVICIILE ACHIZIȚIONATE

2.1. Obiectul achiziției

Obiectul achiziției reprezintă contractarea serviciilor de audit comprehensiv de securitate IT pentru soluția de plăți instant prin:

- Analiza de riscuri de securitate aferent soluției de plăți instant;
- Servicii de audit a securității soluției de plăți instant, inclusiv testarea controalelor de securitate implementate.

Analiza de riscuri de securitate aferent soluției de plăți instant va evalua riscurile operaționale și de securitate asocitate soluției de plăți instant.

Auditul securității presupune formarea concluziilor relevante privind suficienţa şi eficienţa măsurilor de securitate implementate aferente utilizării soluției de plăți instant. Se vor simula valabilitatea contoalelor de securitate implementate aferent soluției de plăți instant prin exploatarea vulnerabilităților existente și cunoscute într-un mod asemănător încercărilor de exploatare realizate de către un atacator, cu diferența că acestea vor fi efectuate într-un mod etic, cu permisiunea Beneficiarului. Procesul implică o analiză activă a sistemelor informatice pentru orice vulnerabilități existente care ar putea rezulta din configurația inadecvată și din breșe cunoscute sau necunoscute, hardware și software.

2.2. Scopul serviciilor prestate

2.2.1. Scopul serviciilor este să prezinte asigurări privind gestionarea eficientă a riscurilor TIC și gestiunea eficientă a atacurilor cibernetice și de a analiza comportamentul sistemelor informatice în contextul diferitelor atacuri informatice, fiind analizate inclusiv vulnerabilitățile care pot exista în cadrul soluției de plăți instant.

2.2.2. Ofertantul trebuie să descrie activitățile ce vor fi desfășurate de acesta pentru a răspunde acestor cerințe. Ofertantul trebuie să prezinte informație despre modul în care intenționează să

presteze serviciile solicitate la nivelul cerut, precum și informație privind capacitățile sale tehnice, organizatorice și de competența, ce confirmă capacitatea sa de a presta la nivelul cerut.

2.3. Cerințele față de analiza de riscuri

2.3.1. Analiza de riscuri va fi efectuată conform celor mai bune practici în domeniu (ISO, NIST, COSO ERM).

2.3.2. Furnizorul trebuie să demonstreze realizarea analizelor de riscuri pentru soluții similare.

2.3.3. Analiza de riscuri identifice, să evalueze și să prioritizeze riscurile identificate și va conține cel puțin:

a) descrierea riscurilor identificate ce ar putea compromite confidenţialitatea, autenticitatea şi integritatea datelor aferente utilizării soluției de plăți instant și nonrepudierea tranzacţiilor;

b) impactul în cazul materializării riscurilor identificate;

c) descrierea măsurilor de control implementate pentru diminuarea impactului, clasificate după modul de organizare (tehnice, organizatorice, normative) şi după modul de acţiune (preventive, detective, corective);

d) riscurile reziduale (care rămîn după implementarea măsurilor de control), sau reevaluarea acestora cu aplicarea măsurilor de control adiţionale pentru diminuarea impactului acestora pînă la un nivel acceptabil.

2.3.4. Domeniul de aplicare a analizei de riscuri va acoperi, dar fără a se limita la:

a) Infrastructura IT;

b) Aplicația soft;

c) Mediul operațional;

d) Riscuri de integrare.

2.3.5. Cerințe privind identificarea riscurilor vor include, dar nu se vor limita la:

e) Identificarea vulnerabilitatilor tehnice și organizaționale asociate soluției de plăți instant;

f) Evaluarea riscurilor externe (atacuri cibernetice, amenințări naturale sau de mediu);

g) Identificarea riscurilor umane;

h) Identifcarea riscurilor asociate furnizorilor de servicii.

2.4. Cerințe față de serviciile de audit a securității soluției de plăți instant

2.4.1. Auditul urmează să se desfășoare conform standardelor internaţionale de audit în domeniul sistemelor informaţionale, va exprima opinia de audit privind suficienţa şi eficienţa măsurilor de securitate implementate aferente utilizării soluției de plăți instant, gestiunea atacurilor cibernetice și conformarea cu standardele internaționale și cele mai bune practici în domeniu.

Raportul de audit va conţine referinţe la probele de audit utilizate, precum şi concluziile pentru cel puţin următoarele obiective de audit:

- Cadrul normativ intern aferent soluției de plăți instant;
- Securitatea datelor;

- Identificarea și autentificarea utilizatorilor;
- Performanța și scalabilitatea soluției;
- Confidentialitatea, integritatea, disponibilitatea și non-repudierea tranzacțiilor;
- Managementul identităților și segregarea responsabilităților;
- Mijloace de control pentru autorizarea la nivelul sistemelor, bazelor de date și aplicației;
- Fraude interne și externe;
- Jurnale de audit;
- Confidențialitatea informației în procesul transportului de date;
- Riscul de securitate aferent terțelor părți;
- Securitatea fizică;
- Gestionarea incidentelor;
- Gestiunea vulnerabilităților;

  Continuitatea funționării sistemului.

2.4.2. O opinie separată urmează a fi expusă referitor la procesele pe partea dezvoltatolului și al BNM referitor la guvernanța procesului de dezvoltare (metodologie, standardizare, echipe și responsabilități), livrarea și gestionarea pachetelor de implementare (controlul versiunilor, validarea pachetelor, procesele de rollback), testarea pachetelor de dezvoltare (testarea funcțională, testarea de securitate, mediile de testare), procesul de implementare în producție (controlul schimbărilor, proceduri de implementare, monitorizare post-implementare), gestiunea schimbărilor și ciclul de viață al soluției (planificarea schimbărilor, conformitate cu reglementările în vigoare, retestare și revalidare), securitatea procesului de dezvoltare și implementare (DevSecOps, protecția mediilor de dezvoltare și testare), documentați și auditabilitate (trasabilitate, probe de audit).

2.4.3. În cadrul misiunii de audit se va evalua eficiența controalelor de securitate implementate prin teste specifice de securitate testînd eficacitatea măsurilor de securitate control implementate pentru reducerea riscurilor identificate ca urmare a analizei de riscuri efectuate prin simularea unor atacuri specifice riscurilor identificate.

Testele ce urmează să se desfășoare se vor efectua conform celor mai bune practici în domeniu (OWASP, NIST, PTES, OSSTMM, CREST, ISO, CIS, MITRE ATT&CK Framework) și vor implica:

a) teste efectuate din rețeaua externă a BNM;
b) teste efectuate din rețeaua internă a BNM;
c) evaluări ale vulnerabilităților;
d) teste de reziliență operațională:
e) simulări privind volumul de tranzacții;
f) simulări are căderilor de sistem și recuperarea acestora;
g) simularea atacurilor de tip DoS/DDoS.

Testele se vor derula în trei etape distincte, și anume:

1. Pre-evaluare (Pre-assesment)

2. Evaluare (Assesment)

3. Post-evaluare (Post-assesment)

2.4.4. ***Etapa de Pre-evaluare (Pre-assesment)*** – reprezintă faza premergătoare evaluării și este importantă pentru determinarea specificațiilor precise și a regulilor de desfășurare a evaluării.

În această etapă se vor stabili și elabora Planul de testare, Planul de acțiuni (SOW – State of Work), precum și, scenariile de atac, și se vor obține autorizațiile necesare desfășurării testelor.

Această etapă se va desfășura pe parcursul numărului de zile lucrătoare stabilit în cadrul planului de proiect și se va finaliza cu elaborarea Planului de testare și a Planului de acțiuni (SOW – State of Work) în care se vor înscrie cel puțin:

- activitățile întreprinse;
- resursele incluse în activitatea de testare;
- termenul propus de realizare;
- persoane responsabile atît din partea Beneficiarului, cît și a Prestatorului.

2.4.5. ***Etapa de Evaluare (Assesment)*** – reprezintă etapa de derulare proriu-zisă a testelor de securitate.

Această etapă a testării include evaluarea conectivității între sistemele utilizate pentru test și sistemele testate, culegerea informațiilor despre sistemele testate, descoperirea sistemelor și serviciilor active, precum și, scanarea sistemelor pentru descoperirea vulnerabilităților.

Utilizînd informațiile descoperite în evaluarea vulnerabilităților, se vor construi arbori de atac și se vor implementa acțiunile definite în aceste structuri.

Testele efectuate vor fi făcute urmărind scenarii de atat din externul rețelei BNM și din rețeaua internă a BNM. De asemenea, scenariile vor include atacuri la nivelul tuturor utilizatorilor ce au acces la soluția de plăți instant.

De asemenea, va avea loc simularea de atacuri cibernetice asupra sistemului folosind tehnici avansate de compromitere a securității informației, pentru a identifica vulnerabilități și potențiale breșe de securitate, evaluarea configurărilor de securitate, a politicilor de acces și a altor măsuri de protecție existente.

În același context se va face documentarea vulnerabilităților detectate, gradul de severitate al acestora și riscurile asociate.

Nu în ultimul rînd va avea loc testarea masurilor de control recomandate și reconfigurărilor propuse în cadrul etapei de pre-evaluare.

2.4.6. ***Etapa de Post-evaluare (Post-assesment)*** – această etapă se va desfășura pe parcursul numărului de zile lucrătoare stabilit în cadrul planului de proiect și se va finaliza cu elaborarea de către Prestator a rapoartelor de analiză, a rezultatelor testelor efectuate în care se vor identifica și vor fi incluse cele mai bune măsuri și metode de remediere a problemelor și vulnerabilităților descoperite, în funcție de severitate și impact.

În această etapă Prestatorul va acorda suport Beneficiarului pentru înțelegerea deplină a problemelor identificate și recomandarea măsurilor/metodelor aplicabile pentru remedierea acestora (din cadrul celor propuse), în scopul minimizării riscurilor de securitate informatică asociate problemelor și vulnerabilităților descoperite. Totodată Prestatorul var-testarea anumitor componente, pentru a verifica aplicarea corectă a măsurilor de remediere recomandate.

2.5. Cerințe față de livrabilele proiectului

Ca urmare a serviciilor prestate, Ofertantul selectat va oferi cel puțin următoarele livrabile:

- Plan de proiect;
- Plan de analiză de riscuri/testare/audit;
- Planul de acțiuni (SOW – Scope of Work);
- Rapoartele privind analizele de riscuri trebuie să fie detaliate și să asigure acoperirea completă a domeniului soluției de plăți instant.
- Rapoarte care vor include toate problemele și vulnerabilitățile detectate pe parcursul testării, catalogate în funcție de gravitatea lor.
- Rapoarte de analiză, ce vor conține analiza rezultatelor testelor efectuate prin care se vor identifica și vor fi incluse recomandări de remediere conținând cele mai bune acțiuni/măsuri/metode ce trebuie întreprinse/luate/folosite pentru eliminarea sau micșorarea riscului generat de vulnerabilitățile detectate.
- Raportul de audit va fi exhaustiv și va include, fără a se limita la: rezumatul executiv, scopul și obiectivele auditului, metodologia și standardele utilizate, observații și constatări, recomandări, probe de audit.
- Rapoarte de follow-up, ce va include evaluarea repetată riscurilor identificate în cadrul raportului primar și a eficienței măsurilor de control implementate.

Digitally signed by Sidorov Vladimir
Date: 2025.03.17 09:38:29 EET
Reason: MoldSign Signature
Location: Moldova
MOLDOVA EUROPEANĂ

Semnat: Numele, Prenumele: Sidorov V. În calitate de: director

Ofertantul: Elince SRL Adresa: mun. Chișinău, str. A. Sciusev 111