**CAIET DE SARCINI**
**Servicii**

Obiectul: ***Achiziționarea serviciilor de testare informatica pentru identificarea și evaluarea vulnerabilităților a infrastructurii IT externe al CNAS pentru anul 2022.***

Autoritatea contractantă: *Casa Națională de Asigurări Sociale*

1. **Descriere generală. Informații privind serviciul solicitat:**

| Lotul nr 1 | Servicii testare informatica pentru identificarea și evaluarea vulnerabilităților a infrastructurii IT externe al CNAS | Termen de prestare |
|---|---|---|
| **1** | **Cerințe pentru servicii de testare informatica pentru identificarea și evaluarea vulnerabilităților a infrastructurii IT externe al CNAS.**<br><br>**1. Scopul și aria de acoperire a serviciilor de pentest:**<br>1.1.Testarea securității a CNAS se va realiza din extern la nivel de site oficial al organizației, sistemele informaționale publice, are ca scop obținerea unei perspective asupra daunelor potențiale și a riscului de bussines-procesele pe care vulnerabilitățile existente le-ar putea provoca.<br>1.2.Resursele care sunt expuse testelor de penetrare sunt:<br>1.2.1. 43 IP adrese externe, oficiile teritoriale.<br>1.2.2. 8 aplicațiilor web.<br><br>1.3. Testele de penetrare externe presupun scopul evaluarea securității a perimetrul extern (expus în Internet) al CNAS, în special pentru sistemele critice conectate la Internet sau accesibile din exteriorul infrastructuri a organizației. În cadrul acestor teste vom evalua orice tip de acces unic din exterior la infrastructura privată al CNAS, inclusiv serviciile care au acces limitat la adrese IP externe individuale.<br>1.4.Testele de penetrare vor include in mod minimal:<br>a. Obținerea informațiilor din domeniul public<br>b. Scanarea sistemelor din scop<br>c. Tehnici de enumerare<br>- Identificarea sistemelor de operare<br>- Identificarea patch-urilor de securitate lipsa pe un anumit sistem de operare.<br>- Determinarea vulnerabilităților cunoscute la nivelul sistemelor de operare<br>- Identificarea tuturor porturilor deschise<br>- Identificarea serviciilor care rulează pe un anumit port<br>- Determinarea vulnerabilităților cunoscute la nivelul serverelor de aplicații<br>- Determinarea vulnerabilităților cunoscute pentru bazele de date<br>- Determinarea vulnerabilităților cunoscute la nivelul serviciilor active identificate<br>- Identificarea problemelor de configurare<br>- Exploatarea vulnerabilităților identificate<br>d. Obținerea accesului neautorizat prin exploatarea vulnerabilităților respectiv a problemelor de configurație<br>e. Consolidarea accesului<br>1.5.Metodologia de testare elaborata si folosita de către ofertant va fi în conformitate cu bunele practici internaționale precum: (OWASP, OSSTMM, ISSAF, NIST, ISACA, etc).<br>1.6.In realizarea testelor de penetrare, ofertantul va realiza următorii pași:<br>a. Construirea unui model al amenințărilor. Investigarea arhitecturii infrastructurii si a tehnologiei. Identificarea specificațiilor cheie de securitate și | **la solicitare Autorității contractante valabil până la 31.12.2022** |

a amenințărilor. Crearea unui model al amenințărilor care documentează activele care trebuie protejate, potențialele amenințări la adresa acestor active, atacuri care ar putea fi realizate, precum si condițiile care ar duce la atacuri de succes.

b. Construirea unui plan de evaluare și acțiune. Convertirea amenințărilor posibile în atacuri care vor fi realizate de ingineri de securitate. Condițiile unui atac, descrise in modelarea amenințărilor, sunt testate.

c. Executarea evaluării. Executarea atacurilor, așa cum sunt descrise în planul de acțiune. Descoperirea vulnerabilităților și a variațiilor acestora.

d. Raportarea rezultatelor. Documentarea problemelor identificate și prezentarea unor recomandări pentru remediere.

1.7.Cerințe fața de testele de penetrare pentru aplicațiile web. Testarea de securitate la nivelul aplicațiilor web este realizata în concordanță cu metodologia OWASP, certificata la nivel mondial. Atacurile din planul de testare vizează în principal următoarele aspecte:

a. Testarea mecanismelor de păstrare a confidențialității si integrității datelor
b. Testarea procesului de Management al Identitarii
c. Testarea mecanismelor de Management al configurațiilor
d. Testarea mecanismelor de Autentificare
e. Testarea mecanismelor de Autorizare
f. Testarea mecanismelor de Management al Sesiunilor
g. Testarea mecanismelor de Validare a Datelor
h. Testarea mecanismelor de management al Excepțiilor (erorilor)
i. Testarea mecanismelor Criptografice
j. Testarea problemelor de Logica de Business.

1.8.Cerințe fata de descrierea vulnerabilităților identificate. Partea executiva va conține descrierea pe scurt a problemelor si vulnerabilităților identificate si va utiliza metode grafice (cel puțin diagrame, grafice sau harți). Partea tehnica va detalia din punct de vedere tehnic problemele și vulnerabilitățile identificate. Raportul va conține cel puțin următoarele capitole:

a. Sumar executiv;
b. Obiectivele și scopul evaluării;
c. Prezentare succinta a metodologiei utilizate in cadrul testării;
d. Descrierea contextului în care s-a desfășurat testarea;
e. Prezentarea individuala a vulnerabilităților descoperite, după cum urmează:
- Descrierea vulnerabilității;
- Catalogarea vulnerabilității;
- Descrierea tehnica;
- Analiza severității si probabilității;
- Calcularea riscului;
- Contramăsuri recomandate pentru remediere.

e. Alte detalii si recomandări;
f. Anexa cu lista testelor de securitate efectuate.

1.9.Cerințe fata de analiza de risc. In vederea realizării acestei analize de risc, se realizează următoarele:

a. Identificarea elementelor analizate: sisteme, aplicații, procese, oameni
b. Identificarea vulnerabilităților și a amenințărilor;
c. Cuantificarea și măsurarea scenariilor de risc;
d. Identificarea controalelor aplicabile;
e. Stabilirea registrului de riscuri și identificarea riscurilor reziduale sau a scenariilor necontrolate.

1.10. Cerințe fața de raportul de prezentare și follow-up. Raportul are ca scop prezentarea concluziilor primare și a analizelor rezultate din datele culese în procesul de testare. În urma finalizării activităților de testare, în cadrul unei

| | | |
|---|---|---|
| | ședințe de închidere tip workshop, ofertantul va prezenta concluziile activității de testare și va realiza agrearea cu observațiile beneficiarul testării pe principalele domenii funcționale. De asemenea, în cadrul ședinței va fi prezentat, în forma draft, "Raportul de testare", raport care va fi îmbunătățit pe baza rezultatelor dezbaterilor. Raportul de testare va include:<br>a. Limitări privind divulgarea și utilizarea raportului de testare a vulnerabilităților;<br>b. Introducere (rezumat al serviciilor prestate, aria de acoperire și perioada);<br>c. Sumar executiv:<br>- Obiectivele și scopul testului de scanare a vulnerabilităților;<br>- Descrierea contextului în care s-a desfășurat testul de penetrare;<br>d. Prezentarea individuala a vulnerabilităților descoperite, după cum urmează:<br>- Descrierea vulnerabilității;<br>- Catalogarea vulnerabilității;<br>- Descrierea tehnica;<br>- Analiza severității si probabilității;<br>- Calcularea riscului;<br>- Contramăsuri recomandate pentru remediere.<br>- Alte detalii si recomandări;<br>e. Identificarea vulnerabilităților precum:<br>- Generale;<br>- Clasificate pe categorie;<br>- Clasificate pe risc;<br>- Raport al vulnerabilităților în detaliu care va conține: un sumar, scoring-ul de risc, descrierea riscului, descrierea tehnică.<br>f. Anexa cu lista testelor de securitate efectuate.<br>1.11. După confirmarea remedierii vulnerabilităților identificate de către beneficiar, ofertantul va realiza o retestare pentru a confirma închiderea vulnerabilităților identificate.<br><br>**2. Cerințe față de membrii echipei de proiect:**<br>2.1. Compania care va presta serviciile de penetrare trebuie să prezinte dovezi că poate pune la dispoziție un număr minim de experți-cheie precum:<br>**a. Manager de proiect –** responsabil de coordonarea echipei de experți și managementului proiectului în sine.<br>1. Experiență de cel puțin 3 ani în proiecte similare ca și complexitate și arie. Se va/vor prezenta CV-ul acestuia.<br>**b. Expert Securitate sisteme informaționale –** responsabil de coordonarea echipei de experți în realizarea testelor de penetrare:<br>1. Experiență de cel puțin 3 ani în proiecte similare ca și complexitate și arie. Experiența va fi dovedită prin certificat internațional acreditat în calitate de auditor intern securitate informațională ISO 27001, (CISA) sau echivalentul. Se va/vor prezenta CV-ul acestuia/ora.<br>**c. Expert testare securitate infrastructură rețea –** responsabil de testarea de penetrare a infrastructurii de rețea:<br>1. Experiență de cel puțin 3 ani în proiecte similare ca și complexitate și arie.<br>2. Cunoștințe privind testarea de securitate a infrastructurilor de rețea din punct de vedere a securității informaționale dovedite prin diplome sau certificate precum: Offensive Security Certified Professional (OSCP) sau echivalentul. Se va/vor prezenta CV-ul acestuia/ora.<br>**d. Expert testare securitate sisteme informatice –** responsabil de testarea de penetrare a aplicațiilor web:<br>1. Experiență de cel puțin 3 ani în proiecte similare ca și complexitate și arie.<br>2. Cunoștințe privind testarea de securitate a sistemelor informatice din punct de | |

| | | |
|---|---|---|
| | vedere a securității informaționale dovedite prin diplome sau certificate precum: Licensed Penetration Tester (LPT) sau echivalentul, GIAC Cloud Penetration Tester (GCPN) sau echivalentul. Se va/vor prezenta CV-ul acestuia/ora.<br>3. Cunoștințe avansate privind sisteme de operare, baze de date, sisteme de virtualizare dovedite prin diplome sau experiența – CV.<br><br>**3. Alte cerințe minim obligatorii față de ofertant:**<br>3.1. Compania ce va presta serviciile de penetrare trebuie să posede o experiență specifică în prestarea serviciilor similar de cel puțin 3 ani în domeniu și minim 3 recomandări (sau 3 contractare similare) pe piața locala din R. Moldova în ultimii 3 ani.<br>3.2. Compania ce va presta serviciile de penetrare trebuie să dețină competență în domeniul de activitate în servicii privind asigurarea securității informației, teste de penetrare și auditarea sistemelor informatice.<br>3.3. Semnarea acordului de confidențialitate ((NDA) Non-Disclosure Agreement) cu compania și echipa de implementarea serviciilor. | |
| **Valoare estimativă a achiziției lei fără TVA** | | **350000,00** |
| **Pasul minim de licitare (lei)** | | **3500,00** |

**2. Condiții de prestare și achitarea serviciilor**

Beneficiarul va solicita Prestatorului să furnizeze serviciile în limita sumei prevăzute, Părțile vor stabili de comun acord, bazându-se pe principiul «de la caz la caz», achitarea se va efectua pentru serviciile prestate de facto, după prestarea serviciilor, după semnarea de către ambele Părți a documentației conform efortului stabilit de ambele Părți şi în timp de 15 zile după prezentarea rapoartelor detaliate, care vor include descifrarea efortului exprimat, reieșind din volumul preconizat pentru Servicii.

**3. Obligațiile Prestatorului privind executarea contractului.**

a) să semneze Acordului privind asigurarea securității datelor şi utilizarea accesului de la distanţă la resursele informaţionale CNAS ((NDA) Non-Disclosure Agreement) în termen de două zile lucrătoare din data întrării în vigoare a contractului și să respecte condițiile stipulate.

b) de a presta serviciile în concordanţă cu obligaţiile asumate prin Contract în baza legislaţiei existente, recomandărilor şi cerinţelor software-lui de sistem;

c) serviciile de testare informatica pentru identificarea și evaluarea vulnerabilităților a infrastructurii IT nu vor perturba funcționarea neîntreruptă a sistemelor aplicative CNAS;

d) să prezinte Beneficiarului lista persoanelor autorizate din partea Prestatorului în grupul de proiect calificat, conform criteriilor și cerințelor de calificare stabilite în documentația procedurii de achiziție publică;

e) să asigure integritatea și calitatea serviciilor prestate.

**4. Obligațiile Beneficiarului privind executarea contractului**

a) să prezinte, in termen de 5 (cinci) zile calendaristice Prestatorului, toată: informația, documentele şi materialele necesare pentru prestarea serviciilor;

b) să prezinte Prestatorului lista persoanelor autorizate din partea Beneficiarului, responsabile pentru coordonare prestării serviciilor;

c) să primească şi să achite costul serviciilor în ordinea şi termenele, prevăzute în prezentul Contract şi anexele lui.

**5. Operatorul economic în momentul întocmirii ofertelor trebuie să țină cont de următoarelor acte normative:**

a) Legea nr. 133/2011 privind protecţia datelor cu caracter personal
b) Hotărîrea Guvernului nr. 1123/2010 privind aprobarea Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal
c) Hotărîrea Guvernului nr. 1176/2010 pentru aprobarea Regulamentului cu privire la asigurarea regimului secret în cadrul autorităţilor publice şi al altor persoane juridice
d) Politica de securitate privind protecția datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale gestionate de Casa Națională de Asigurări Sociale aprobată prin ordinul directorului general nr.138 – A din 04.06.2021.

**6. Documente obligatorii la depunerea ofertei**

(La punctul dat autoritatea contractantă indică care documente sunt obligatorii de a fi prezentate la depunerea ofertei prin intermediul **SIA RSAP**. La fel, tot aici se indică documentele ce conțin date cu caracter personal, care nu se depun prin intermediul SIA RSAP și nu sunt publice pentru toți.)

| Nr. d/o | Descrierea documentului | Mod de demonstrare a îndeplinirii: | Nivelul minim/ Obligativitatea |
|---|---|---|---|
| 1. | Prezentarea Cererii de participare conform ***Anexei nr.7*** din Ordinul MF 115/2021**.** | Cerere de participare confirmată prin semnătura electronică | ***Da*** |
| 2. | Prezentarea Declaraţiei privind valabilitatea ofertei conform ***Anexei nr.8*** din Ordinul MF 115/2021 | Declaraţia privind valabilitatea ofertei confirmată prin semnătura electronică | ***Da*** |
| 3. | Prezentarea Specificații de preț conform ***Anexei nr.23*** din Ordinul MF 115/2021 | Specificații de preț, confirmat prin semnătura electronică | ***Da*** |
| 4. | Prezentarea Specificații tehnice conform ***Anexei nr.22*** din Ordinul MF 115/2021 | Specificații tehnice, confirmată prin semnătura electronică . | ***Da*** |
| 5. | Prezentarea Formularul standard al Documentului Unic de Achiziții European completat | Formularul standard al Documentului Unic de Achiziții European confirmat prin semnătura electronică | ***Da*** |

**8. Documente obligatorii la evaluarea ofertelor**

(La punctul dat autoritatea contractantă indică care documente sunt obligatorii de a fi prezentate **în SIA RSAP** la evaluarea ofertei. La fel, tot aici se indică documentele ce conțin date cu caracter personal, care nu se depun prin intermediul SIA RSAP și nu sunt publice pentru toți, ele se prezintă la etapa de evaluare direct autorității contractante.)

| Nr. d/o | Criteriile de calificare și de selecție (Descrierea criteriului/cerinței) | Mod de demonstrare a îndeplinirii criteriului/cerinței: | Nivelul minim/ Obligativitatea |
|---|---|---|---|

| | | | |
|---|---|---|---|
| 1. | Documente ce atestă eligibilitatea ofertantului - Certificatul de efectuare regulată a plăţii impozitelor, contribuţiilor, ori link-ul la accesarea unei baze de date naționale disponibile gratuit pentru autoritatea contractantă care deține informațiile privind lipsa/existența restanțelor | -Certificat de efectuare regulată a plăţii impozitelor, contribuţiilor (valabil la data deschiderii ofertei) Eliberat de inspectoratul fiscal principal de stat, confirmat prin semnătura electronică sau<br>- Link-ul la accesarea unei baze de date naționale disponibile gratuit pentru autoritatea contractantă care deține informațiile privind lipsa/existența restanțelor | ***Obligatoriu*** |
| 2. | Documente ce atestă capacitatea economică şi financiară ofertantului - Declaraţii privind cifra de afaceri în domeniul de activitate aferent obiectului contractului (prestarea serviciilor similare) într-o perioadă anterioară care vizează activitatea pentru ultimii 3 ani - a cîte min 350000,00 lei pentru fiecare din ultimii 3 ani original confirmat prin semnătura electronică a participantului: (la solicitare se va prezintă documente primare de confirmare copiile contractelor, raport financiar etc.) | - Declaraţie privind lista principalelor prestări de serviciul efectuate în ultimii 3 ani de activitate similare obiectului de achiziție confiorm ***Anexei nr.12*** din Ordinul MF 115/2021 - confirmată prin semnătura electronică | ***Obligatoriu*** *în cazul existenței datelor cu caracter personal sau informațiilor care prezintă secret comercial informația se remite direct autorității contractante pe poșta electronică achizitiicnas@cnas.gov.md* |
| 3. | Documente ce atestă Capacitatea tehnică şi profesională<br>- existenţa grupului de proiect calificat asigurat pentru îndeplinirea serviciilor relevante.<br>- minimum 3 ani de experiența similară. | - Lista principalelor prestări similare efectuate în ultimii minim 3 ani, conținînd valori, perioade de prestare, beneficiari, prezentare minimum 3 recomandări (sau 3 contractare similare) pe piața locala din R. Moldova în ultimii 3 ani<br>- Declarația de proprie răspundere conform ***Anexei nr.14*** din Ordinul MF 115/2021 privind:<br>- dispunerea echipei de proiect calificat asigurat pentru îndeplinirea serviciilor relevante.<br>**Cerințe față de membrii echipei de proiect:**<br>2.1. Compania care va presta serviciile de penetrare trebuie să prezinte dovezi că poate pune la dispoziție un număr minim de experți-cheie precum:<br>**a. Manager de proiect –** responsabil de coordonarea echipei de experți și managementului proiectului în sine.<br>1. Experiență de cel puțin 3 ani în proiecte similare ca și complexitate și arie. Se va/vor | ***Obligatoriu*** *în cazul existenței datelor cu caracter personal sau informațiilor care prezintă secret comercial informația se remite direct autorității contractante pe poșta electronică achizitiicnas@cnas.gov.md* |

| | | | |
|---|---|---|---|
| | | prezenta CV-ul acestuia.<br>**b. Expert Securitate sisteme informaționale** – responsabil de coordonarea echipei de experți în realizarea testelor de penetrare:<br>1. Experiență de cel puțin 3 ani în proiecte similare ca și complexitate și arie. Experiența va fi dovedită prin certificat internațional acreditat în calitate de auditor intern securitate informațională ISO 27001, (CISA) sau echivalentul. Se va/vor prezenta CV-ul acestuia/ora.<br>**c. Expert testare securitate infrastructură rețea –** responsabil de testarea de penetrare a infrastructurii de rețea:<br>1. Experiență de cel puțin 3 ani în proiecte similare ca și complexitate și arie.<br>2. Cunoștințe privind testarea de securitate a infrastructurilor de rețea din punct de vedere a securității informaționale dovedite prin diplome sau certificate precum: Offensive Security Certified Professional (OSCP) sau echivalentul. Se va/vor prezenta CV-ul acestuia/ora.<br>**d. Expert testare securitate sisteme informatice –** responsabil de testarea de penetrare a aplicațiilor web:<br>1. Experiență de cel puțin 3 ani în proiecte similare ca și complexitate și arie.<br>2. Cunoștințe privind testarea de securitate a sistemelor informatice din punct de vedere a securității informaționale dovedite prin diplome sau certificate precum: Licensed Penetration Tester (LPT) sau echivalentul, GIAC Cloud Penetration Tester (GCPN) sau echivalentul. Se va/vor prezenta CV-ul acestuia/ora.<br>3. Cunoștințe avansate privind sisteme de operare, baze de date, sisteme de virtualizare dovedite prin diplome sau experiența – CV | |
| 4. | DECLARAŢIE privind confirmarea identității beneficiarilor efectivi și neîncadrarea acestora în situația condamnării pentru participarea la activităţi ale unei organizaţii sau grupări criminale, pentru corupţie, fraudă și/sau spălare de bani | Declaraţie în conformitate cu **Anexa nr. 1** autentificată prin aplicarea semnăturii electronice a Participantului – depunere obligatorie după desemnare în calitate de ofertant/ofertant asociat desemnat câștigător; | ***Da*** *– depunere obligatorie după desemnare în calitate de cîștigător* |

*- în cazul existenței datelor cu caracter personal informația se remite direct autorității contractante pe poșta electronică achiziţtiicnas@cnas.gov.md .*

Digitally signed by Moraru Maia
Date: 2022.11.03 11:01:18 EET
Reason: MoldSign Signature
Location: Moldova

**Președintele grupului de lucru:_____ Maia Moraru**

**L.Ș.**

**Anexa nr. 1**
**la Caietul de sarcini**

APROBAT
prin Ordinul
Ministrului Finanțelor
nr. 145 din 24 noiembrie 2020

**DECLARAŢIE**
**privind confirmarea identității beneficiarilor efectivi și neîncadrarea acestora în situația condamnării pentru participarea la activităţi ale unei organizaţii sau grupări criminale, pentru corupţie, fraudă şi/sau spălare de bani.**

Subsemnatul, _____ reprezentant împuternicit al _____ *(denumirea operatorului economic*) în calitate de ofertant/ofertant asociat desemnat câștigător în cadrul procedurii de achiziție publică nr. _____ din data __/__/___, declar pe propria răspundere, sub sancţiunile aplicabile faptei de fals în acte publice, că beneficiarul/beneficiarii efectivi ai operatorului economic în ultimii 5 ani nu au fost condamnați prin hotărâre judecătorească definitivă pentru participarea la activităţi ale unei organizaţii sau grupări criminale, pentru corupţie, fraudă şi/sau spălare de bani.

| Numele și prenumele beneficiarului efectiv | IDNP al beneficiarului efectiv |
|---|---|
| | |
| | |
| | |

Data completării: _____
Semnat: _____
Nume/prenume: _____
Funcţia: _____
Denumirea operatorului economic _____
IDNO al operatorului economic _____