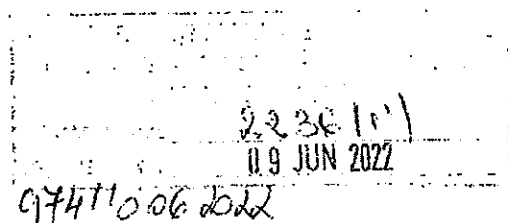


**OFICIUL NAȚIONAL DE PREVENIRE ȘI
COMBATERE A SPĂLĂRII BANILOR**



CAIET DE SARCINI
Servicii mentenanță și asistență tehnică SROL

1. Introducere

Oficiul Național de Prevenire și Combatere a Spălării Banilor cu sediul în Str. Ion Florescu, nr. 1, sector 3, București îndeplinește rolul de Autoritate contractantă pentru procedura de achiziție care face obiectul prezentului caiet de sarcini.

2. Contextul realizării acestei achiziții de produse

2.1. Informații despre Autoritatea contractantă

Oficiul Național de Prevenire și Combatere a Spălării Banilor este Unitatea de Informații Financiare a României de tip administrativ, cu rol de lider în elaborarea, coordonarea și implementarea sistemului național de combatere a spălării banilor și finanțării terorismului.

Funcțiile de bază ale Oficiului Național de Prevenire și Combatere a Spălării Banilor, în conformitate cu prevederile legale în materie, respectiv Legea nr. 129/2019 și H.G. nr. 491/2021, sunt următoarele:

- Primirea, analizarea, prelucrarea și diseminarea informațiilor cu caracter financiar, în condițiile în care din analiza datelor și informațiilor prelucrate la nivelul instituției, rezulta existența unor indicii de spălare a banilor sau de finanțare a terorismului, Oficiul informează de îndată Parchetul de pe lângă Înalta Curte de Casație și Justiție. Oficiul informează de îndată Serviciul Român de Informații cu privire la suspiciuni de finanțare a terorismului, sau informează organele de urmărire penală cu privire la indicii de săvârșire a altor infracțiuni decât cele de spălare a banilor sau de finanțare a terorismului, în conformitate cu prevederile legii speciale, fiind astfel conturată funcția de diseminare a informațiilor către autoritățile competente;
- Supravegherea și controlul entităților raportoare, conform legii, în scopul prevenirii și combaterii spălării banilor și finanțării terorismului;
- Oficiul este autoritate competentă în domeniul punerii în aplicare a sancțiunilor internaționale, în conformitate cu dispozițiile Ordonanței de Urgență a Guvernului nr. 202/2008 privind punerea în aplicare a regimului sancțiunilor internaționale, aprobată prin Legea nr. 217/2009 cu modificările și completările ulterioare;

- Prevenirea si combaterea finantarii actelor de terorism. Oficiul, prin atributiile conferite de legislatia in materie, are un rol important in prevenirea si combaterea finantarii actelor de terorism, fapt ce a determinat ca institutia sa fie parte componenta a Sistemului National de Prevenire si Combatere a Terorismului (S.N.P.C.T.), participand activ, potrivit competentelor sale, atat la activitatea de stopare a unor eventuale fluxuri de finantare a grupurilor teroriste, cat si la analiza si evaluarea riscurilor la care se expun entitatile raportoare.
- Primirea, procesarea si analiza cererilor de informatii. In scopul efectuării unor analize complexe, cat mai ample care implica tranzactii financiare cu elemente de extraneitate.

2.2. Informații despre contextul care a determinat achiziționarea produselor

Contractul de mentenanta si asistenta tehnica este necesar pentru a ne asigura buna functionare a sistemului pana la sfarsitul anului 2022 cu posibilitatea prelungirii prin act aditional pe o perioada de maxim 4 luni.

2.3. Informații despre beneficiile anticipate de către Autoritatea contractantă

Serviciile de mentenanta si asistenta tehnica vor mentine sistemul de raportare on-line complet funcțional, actualizat conform prevederilor legale și accesibil tuturor beneficiarilor, în permanenta, asigura evitarea pierderii informațiilor vitale, ce ar putea aduce instituției prejudicii de imagine, de ordin financiar sau de alta natura.

3. Descrierea produselor solicitate

3.1. Descrierea situației actuale la nivelul Autorității/entității contractante

Sistem Electronic de Transmitere Date on-line al ONPCSB are doua componente: una accesibila prin internet care este destinata raportorilor non-bancari si una accesibila in rețeaua de comunicatii interbancare, destinata raportorilor bancari. Sistemul de operare al celor doua servere corespunzatoare celor doua componente este Windows 2008 R2. Aplicatia Sistem Electronic de Transmitere Date a fost pusa in functiune in anul 2010, a fost dezvoltata utilizand PHP, Zend Framework, Java, si utilizeaza ca baza de date MySQL.

De-a lungul timpului au fost incheiate contracte pentru mentenanta si dezvoltare cu diverse firme astfel incat in momentul de fata structura sistemului este una eterogena ca urmare a viziunilor diferite pe care le-au avut prestatorii acestor servicii.

3.2. Obiectivul general la care contribuie furnizarea produselor

Prin contractarea serviciilor de mentenanta si asistenta tehnica cerute prin prezenta documentatie de achizitie, ONPCSB urmareste asigurarea securitatii sistemului de raportare on-line, actualizarea conform prevederilor legale, mentinerea acestuia in conditii optime de functionare si adaptarea lui la tehnologiile actuale.

3.3. Obiectivul specific la care contribuie furnizarea produselor

Conform legii nr. 129/2019, ONPCSB pune la dispozitia entităților raportoare un canal prin care acestea sa transmita rapoartele prevazute de lege, numai în format electronic. Acest

sistem trebuie sa fie functional, adaptat specificului fiecarei categorii de entitati raportoare si disponibil permanent.

3.4. Produsele solicitate și operațiunile cu titlu accesoriu necesar a fi realizate

Produselor care vor fi achiziționate sunt servicii de mentenanța și asistența tehnică pentru sistemul de raportare on-line.

3.4.1. Principalele activități care se prestează sunt:

3.4.1.1. Mentenanță

3.4.1.1.1. Servicii de mentenanță preventivă

Activitățile de mentenanță preventivă au ca scop prevenirea apariției oricărui inconvenient sau a oricărei întreruperi în funcționarea sistemelor. Activitățile de mentenanță preventivă sunt activități planificate periodic de verificare a stării de funcționare a serverelor, a aplicațiilor și a bazelor de date utilizate, precum și de realizare a copiilor de siguranță ale acestora.

Înainte de efectuarea operațiunilor de mentenanță preventivă, contractantul comunică autorității contractante lista operațiunilor de mentenanță care trebuie efectuate. Este posibil ca mentenanța preventivă să trebuiască a fi realizată în afara orelor normale de lucru sau la sfârșit de săptămână sau în sărbători legale. Operațiunile de mentenanță preventivă care necesită o oprire a funcționării, se efectuează în zile și intervale de timp ce vor fi agreeate de comun acord.

După fiecare intervenție preventivă, contractantul trebuie să efectueze teste de funcționare ale produsului și să prezinte un raport care să includă activitățile realizate și rezultatele testelor.

3.4.1.1.2. Servicii de mentenanță corectivă

Activitățile de mentenanță corectivă sunt activități derulate pentru corectarea unei defecțiuni manifestate sau în curs de manifestare în cadrul sistemelor. Au rolul de a reduce cât mai mult posibil timpii de nefuncționare sau de funcționare defectuoasă a sistemelor și de a înlătura deserviciile cauzate utilizatorilor finali de anomalii existente la nivelul sistemului. Furnizorul va investiga erorile și dificultățile care apar în funcționarea aplicației informatice pentru identificarea cauzelor care le determină, în vederea remedierii acestora.

Mentananta corectiva pentru sistemul de raportare poate include activitati precum cele exemplificate in continuare, fara a se limita la acestea:

1. Operationalizarea transmiterii rapoartelor de transferuri externe de corectie si de completare
2. Aplicarea in mod unitar a regulilor de validare a informatiilor similar din sectiuni diferite ale rapoartelor
3. Rezolvarea problemelor generate de numele utilizatorilor (de exemplu: nume care contin spatii sau utilizatori care au acelasi nume)
4. Corectarea modului de editare al anumitor sectiuni din raportul de tranzactii suspecte in sensul permiterii stingerii si/sau modificarii informatiilor introduse

Exemplele sunt prezentate pentru ca ofertantii sa evalueze corect complexitatea si volumul activitatilor pe care urmeaza sa le desfasoare.

Dacă este cazul, furnizorul va folosi copiile de siguranță pentru restaurarea bazei de date și a aplicațiilor.

Furnizorul va asigura menținerea instrucțiunilor de folosire a aplicațiilor (Ajutor) în conformitate cu modul curent de funcționare.

3.4.1.1.3. Servicii de mentenanță evolutivă

Activitățile de mentenanță evolutivă sunt activități de actualizare a aplicațiilor care constau în furnizarea de versiuni noi, în vederea satisfacerii solicitărilor de implementare a unor noi funcționalități, reguli de business noi sau modificate, precum și alte adaptări necesare datorită schimbărilor legislative, administrative sau procedurale legate de funcționarea sistemelor.

Mentenanța evolutivă pentru sistemul de raportare poate include activități precum cele exemplificate în continuare, fara a se limita la acestea:

1. Adaptarea modului de înregistrare pentru transmiterea automata a credentialelor de acces; trimiterea parolelor catre entitatile raportoare neactivate pana in prezent pe adresele de e-mail completate la înregistrare de catre acestea.
2. Actualizarea formularelor generate la înregistrare pentru alocare cont si comunicare credentiale de acces
3. Implementarea unei proceduri de editare, upload si validare pentru raportul de transfer de fonduri
4. Implementarea unui modul de interfata pentru editarea unui format simplificat de raport de tranzactii suspecte destinat entitatilor nonbancare

Exemplele sunt prezentate pentru ca ofertantii sa evalueze corect complexitatea si volumul activitatilor pe care urmeaza sa le desfasoare.

Modificările vor fi dezvoltate într-un mediu de test și vor fi aplicate în mediul de producție după acceptarea acestora de către reprezentantii beneficiarului.

Documentația „Ajutor” a sistemului va fi actualizată în concordanță cu modificările efectuate.

3.4.1.1.4. Servicii de mentenanță adaptivă

Activitățile de mentenanță adaptivă sunt activități de adaptare a software-ului aferent sistemelor care constau în actualizarea acestora, cu scopul de a le păstra funcționalitatea, disponibilitatea și de a le îmbunătăți performanțele în condițiile unor modificări intervenite în mediul în care rulează. Modificările pot fi la nivelul platformei hardware și/sau software pe care este instalată soluția.

3.4.1.2. Activități de instalare și configurare

În vederea îndeplinirii obiectivului prevăzut de contract, în situațiile în care activitățile de mentenanță sunt însoțite de actualizări ale sistemelor dezvoltate, vor fi desfășurate activități de instalare și configurare a soluției, ori de câte ori este necesar.

De asemenea, Contractantul va realiza actualizarea certificatelor de Securitate pe serverele care fac obiectul contractului.

3.4.1.3. Activități de testare

După fiecare modificare minoră sau majoră care are loc în program se va realiza testarea unor aspecte cum ar fi: funcționarea, integritatea, performanța, securitatea aplicației, etc.

3.4.1.4. Servicii de suport tehnic

Serviciile de suport tehnic sunt activități de preluare și soluționare a tuturor cererilor de suport care apar în contextul derulării contractului.

Pe toata durata contractului, în perioada de garanție, Contractantul va asigura suport tehnic pentru problemele aparute în exploatarea sistemelor, atât la nivelul Autorității contractante cât și la nivelul entităților raportoare.

Contractantul va asigura un punct de contact dedicat personalului autorizat al Autorității/entității contractante unde se poate semnală orice problemă/defecțiune care necesită suport tehnic în gestionarea unui incident, disponibil, pentru a se asigura că orice situație semnalată este tratată cu promptitudine. Pentru buna gestionare a activităților și incidentelor se va utiliza un sistem de ticketing care va asigura notificarea în timp real (prin e-mail sau sms).

Contractantul va răspunde în timp util la orice incident semnalat de Autoritatea contractantă, în funcție de nivelul de prioritate. Fiecare incident este caracterizat de un nivel de prioritate, care va evidenția impactul acestuia asupra funcționalităților produsului.

Contractantul trebuie să asigure disponibilitatea serviciilor de suport tehnic. În cazul incidentelor cu prioritate "urgent" intervenția va fi asigurată 24 x 7, din momentul primirii sesizării și până la remedierea definitivă a problemei și asigurarea funcționalității integrale a produsului.

Contractantul va trebui să respecte următorii timpi de răspuns, corelați cu nivelul de prioritate a incidentului:

Nivel prioritate	Timp de răspuns	Timp de implementare soluție provizorie	Timp de rezolvare
Urgent	30 minute	4 ore	24 ore
Critic	2 ore	24 ore	48 ore
Major	4 ore	Următoarea zi lucrătoare	Următoarea zi lucrătoare
Minor	6 ore	Următoarea zi lucrătoare	Următoarea zi lucrătoare

Nerespectarea timpilor de mai sus dă dreptul Autorității/entității contractante de a solicita penalități/daune interese în conformitate cu clauzele contractului de achiziție publică/sectorială de produse.

În cazul intervențiilor onsite, contractantul va asigura prezenta experților desemnați în termen de maxim 60 de minute de la semnalarea incidentului de către beneficiar.

3.4.1.5. Servicii de optimizare

Serviciile de optimizare constau în îmbunătățirea performanței aplicațiilor. Furnizorul va face recomandări pentru a îmbunătăți performanțele aplicațiilor și va stabili modificările de software și de hardware necesare, estimând costurile pe care le presupun aceste modificări.

Serviciile de optimizare pentru sistemul de raportare vor include simplificarea modului de transmitere a rapoartelor de corecție, fara a se limita la aceasta.

3.4.2. Securitatea informației

Furnizorul va respecta Politica de securitate a resurselor informatice și de comunicații a ONPCSB.

În relația dintre Beneficiar și Furnizorul de servicii se stabilește contractual faptul că toate informațiile Beneficiarului la care furnizorul are acces sunt CONFIDENȚIALE.

Informațiile vor fi folosite numai în scopul îndeplinirii sarcinilor contractuale și nu vor fi divulgate unor terți.

3.4.3. Prestarea serviciilor

Autoritatea contractanta solicita disponibilitatea on-line sau on-site, după caz, în zilele lucrătoare, de luni până vineri, timp de 4 ore, a unui specialist care să asigure serviciile mai sus menționate și respectarea, fără excepție, a termenelor de remediere a incidentelor, pe perioada derulării contractului.

Pentru expertii care vor asigura serviciile solicitate se vor prezenta documente care să ateste studiile și experiența în proiecte similare, pe tehnologia folosită la nivelul sistemului de raportare.

DEFINIȚII

Politica de securitatea resurselor informatice și de comunicații reprezintă totalitatea măsurilor necesare pentru asigurarea integrității, confidențialității și disponibilității informației.

- Integritatea se referă la măsurile și procedurile utilizate pentru protecția datelor împotriva modificărilor sau distrugerii neautorizate;
- Confidențialitatea se referă la protecția datelor împotriva accesului neautorizat;
- Disponibilitatea se asigură prin funcționarea continuă a tuturor componentelor sistemului.

Timp de remediere. Prin timp de remediere părțile înțeleg timpul scurs între momentul în care BENEFICIARUL notifică FURNIZORUL asupra apariției unui incident în legătură cu sistemul de raportare on-line și/sau a website-ului și momentul în care Furnizorul repune sistemul în stare de funcționare la parametrii conveniți.

Incident de nivel minor reprezintă o eroare care afectează o funcție sau proces, dar funcționarea întregului sistem nu este afectată sau este afectată nesemnificativ. Impactul este minim, riscul ca activitatea să nu se desfășoare normal este practic inexistent.

Incident de nivel major reprezintă o eroare apărută la o funcție sau proces, care afectează într-o mare măsură funcționarea întregului sistem de raportare on-line și/sau a website-ului. Poate avea impact asupra proceselor de business ale Beneficiarului. Există riscul ca incidentul să se extindă.

Incident de nivel critic reprezintă o eroare care afectează majoritatea funcționalităților sistemului de raportare on-line sau a funcțiilor principale. Impact foarte mare asupra mediului intern și extern. Risc mare privind: neexecutarea în termen a activităților specifice Beneficiarului, deteriorarea imaginii Beneficiarului în relațiile cu entitățile raportoare.

Incident de nivel urgent reprezintă un incident de nivel critic pentru care nu există soluții alternative (workaround) care pot fi aplicate. Impact foarte mare asupra mediului intern și extern. Risc mare privind: neexecutarea în termen a lucrărilor, deteriorarea imaginii Beneficiarului în relațiile cu instituțiile partenere și entitățile raportoare.
