**CONTRACT DE PRESTARI SERVICII**
nr. achizitor **67** din **07.11.2024**
nr. prestator **4521** din **07.11.2024**
***Nr. atribuire achzitie in SEAP: DA36855621/06.11.2024)***

**PREAMBUL**

Prezentul contract se încheie în temeiul:

- **art. 12 alin. (4)** din **Legea** nr. **99/2016** care prevede: *„Entităţile contractante au dreptul de a achiziţiona direct produse sau servicii în cazul în care valoarea estimată a achiziţiei, fără TVA, este mai mică de 270.120 lei, respectiv lucrări, în cazul în care valoarea estimată a achiziţiei, fără TVA, este mai mică de 900.400 lei."*
- **art. 1270 Cod Civil** şi cu respectarea principiilor instituite de **art. 2, alin. (2) din Legea nr. 99/2016**, nerestricţionând accesul operatorilor economici la procedurile de achiziţie sectoriala

**1. Partile contractante**

**S.C. AEROPORTUL ARAD,** cu sediul in localitatea Arad, str. Aleea Aeroport nr. 4, judetul Arad, telefon/fax: 0257 339010/ 0257 254482, CUI:5752187, inregistrata la ORC sub nr. J02/772/1998, reprezentata legal prin **Vasile Ovidiu Mosneag**, având funcţia de **Director General**, în calitate de **achizitor,** pe de o parte

şi

**S.C. CERTINSPECT REGISTER S.R.L.**, cu sediul în municipiul Bucureşti, Str. Zambilelor nr. 96, Etaj 1, secor 2, jud. Bucureşti Cod postal:023783, e-mail:***office@certinspect.ro,*** tel: +40 726368707, având CIF: RO37991905, înregistrată la ORC sub nr. J40/ 13045/2017, cont bancar nr. RO32CECEB41730RON4444491, deschis la C.E.C. Bank - Sucursala Theodor Pallady, reprezentată legal de dl. **Răzvan Cristian Ionescu**, având funcţia de **Administrator**, denumită în continuare **prestator,** pe de alta parte.

**2. Definiţii**

In prezentul contract urmatorii termeni vor fi interpretati astfel:
***contract*** - reprezinta prezentul contract si toate anexele sale;
***achizitor şi prestator*** - partile contractante, asa cum sunt acestea numite in prezentul contract;
***pretul contractului*** - pretul platibil prestatorului de catre achizitor, in baza contractului, pentru indeplinirea integrala si corespunzatoare a tuturor obligatiilor asumate prin contract;
***servicii*** - activitati a caror prestare fac obiect al contractului;
***forta majora*** – este orice eveniment extern, imprevizibil, absolut invincibil şi inevitabil;
***caz fortuit*** – eveniment care nu poate fi prevăzut şi nici împiedicat de către cel care ar fi fost chemat să răspundă dacă evenimentul nu s-ar fi produs.
***zi - zi calendaristica;***
***an – 365 de zile.***

**3. Interpretare**

3.1. In prezentul contract, cu exceptia unei prevederi contrare cuvintele la forma singular vor include forma de plural si vice versa, acolo unde acest lucru este permis de context.
3.2. Termenul *„zi"* sau *„zile"* sau orice referire la zile reprezinta zile calendaristice daca nu se specifica in mod diferit.

***Clauze obligatorii***

**4. Obiectul contractului**

4.1. Obiectul contractului consta în prestarea **Serviciilor de audit de securitate a reţelelor sistemelor informatice,** servicii clasificate confom **CPV (Rev. 2)**: 72810000-1 **Servicii de audit informatic,** 72800000-8 **Servicii de audit informatic si de testări informatice.**
**4.2.** Serviciile de audit se vor efectua la faţa locului sau audit de la distanţă, de către auditorii atestaţi de către CERT-RO (DNSC) angajati ai prestatorului **S.C. CERTINSPECT REGISTER SRL.**
**4.3.** Detaliile cu privire la infrastructura Achizitor (exemplu:adrese IP, URL, domenii, retele, echipamente, localizarea acestora, datele de contact ale reprezentanţilor Achizitorului care pot furniza informaţii şi acces la această infrastructură, perioada calendaristică şi de timp în care Achizitorul permite efectuarea Serviciilor) vor fi puse de Achizitor la dispoziţia Prestatorului într-un document care va deveni Anexa 2 la acest contract.

**4.4** La finalul auditului, Prestatorul va livra un raport de audit care va urma să fie analizat de către autoritatea competentă. Raportul de audit va conține concluziile echipei de audit, rezultatele testelor efectuate și recomandările acesteia.

**5. Pretul si plata contractului**

5.1. Prețul convenit pentru îndeplinirea contractului este de **29.500,00 lei**, la care se adaugă cota de TVA prevazuta de lege.

5.2. Pentru serviciile prestate în baza prezentului contract, factura va fi emisă de către prestator dupa finalizarea si receptionarea serviciilor, respectiv predarea de către Achizitorul Raportului de audit prezentat sub forma unui rezumat, însoțit de o analiza tehnică detaliată.Raportul va cuprinde, de asemenea, recomandări tehnice cu privire la măsurile necesare a fi implementate pentru asigurarea protecției informatice.

5.3. Factura emisa de către prestator va fi însoțită în mod obligatoriu de o anexă în care se vor menționa succint serviciile care s-au prestat si pentru care se emite factura, anexa in lipsa careia achizitorul nu va dispune plata facturii emise de către prestator.

5.4. Plata facturii emise urmeaza a se efectua in termen de **30 zile** de la data inregistrarii facturii cu respectarea **Legii nr. 72/2013**.

**6. Durata si executarea contractului**

6.1. Prezentul produce efecte începând cu data semnării și până la data ducerii la îndeplinire a tuturor obligațiilor asumate de părți prin contract.

6.2. Prestatorul se obligă să asigure prestarea serviciilor asumate prin prezentul contract începând cu data semnării contractului si il va finaliza până cel târziu în data de **13.12.2024**.

**7. Obligatiile prestatorului**

7.1. Prestatorul are obligatia de a presta serviciile prevazute în contract cu profesionalismul si promptitudinea cuvenite angajamentului asumat la standardele si performantele asumate prin prezentul contract.

7.2. Prestatorul este pe deplin responsabil pentru prestarea serviciilor in conformitate cu obligatiile asumate prin contract si cu respectarea legislatiei in materie. Totodata este răspunzator și de calificarea personalului folosit în realizarea obiectului contractului, conform atestarilor in domeniu.

7.3. Prestatorul se obliga sa despagubeasca achizitorul impotriva oricaror daune-interese, costuri, taxe si cheltuieli de orice natura, aferente, cu exceptia situatiei in care o astfel de incalcare rezulta dintr-o dispozitie expresa a achizitorului.

7.4. Prestatorului i se va imputa contravaloarea eventualelor amenzi aplicate Achizitorului, din vina exclusivă a Prestatorului, sarcina dovedirii culpei Prestatorului revenind Achizitorului.

**7.5. Pachetul de servicii oferit de către Prestator** cuprinde:

7.5.1.1. **Analiza inițială de securitate cibernetică**, care constă în:

a) Analiza serviciilor esențiale a infrastructurii OSE/FSD necesare pentru prestarea acestor servicii;

b) Analiza politicilor, procedurilor și a măsurilor tehnice organizatorice implementate de către OSE/FSD:

c) Identificarea procesului de comunicare cu CERT-RO (DNSC), a responsabilităților și atribuțiilor Responsabilului NIS cadrul OSE/FSD;

d) Gestionarea schimbărilor la nivelul serviciilor esențiale furnizate.

7.5.1.2. **Activitățile de audit tehnic de securitate cibernetică:**

Auditul tehnic de securitate cibernetică poate constă în următoarele servicii:

a) auditul arhitecturii [AS1]
b) auditul de configurare [AS2]
c) auditul codului sursă [AS3]
d) auditul de penetrare sau testarea de penetrare [AS4]
e) auditul securității organizației [AS5]
f) auditul sistemelor de control industrial [AS6]

**7.5.1.2.2. Testele de penetrare**

7.5.1.2.2.1. Evaluarea securității infrastructurii IT va fi completată în această ultimă etapă, prin efectuarea de teste de penetrare, doar pentru aplicațiile critice expuse la internet, care se bazează pe încercarea unor scheme cunoscute de penetrare a sistemelor de calcul prin intermediul exploatării vulnerabilităților de securitate identificate.Anumite testări, ce vor fi agreate cu Achizitorului, se vor realiza în afara programului de lucru, pentru prevenirea întreruperii activităților.

7.5.1.2.2.2. Întrucât precizările legale prevăd posibilitatea realizării unui eşantion în cazul testelor de penetrare, pentru zonele echipamentele cu risc ridicat de defectare/afectare a functionalităţii şi datelor în cazul efectuării auditului tehnic, auditorul va efectua acest audit tehnic pentru un eşantion reprezentativ.
Se recomandă ca pentru evitarea aparitiei acestor riscuri de securitate si de Achizitor să asigure un mediu de test similar cu cel de producţie (operaţional).
7.6.Rezultatele scanărilor de securitate vor fi centralizate într-un raport scris, prezentat sub forma unui rezumat, însoţit de o analiza tehnică detaliată.
7.7. Raportul va cuprinde, de asemenea, recomandări tehnice cu privire la măsurile necesare a fi implementate pentru asigurarea protecţiei informatice.
7.8. Să presteze Serviciile care fac obiectul prezentului contract cu obiectivitate, imparţialitate şi cu respectarea termenelor prevăzute în prezentul contract.
7.9. Să respecte programul de activităţi stabilit de comun acord cu Achizitorul, conform planului de audit şi conform prezentului contract. Auditul va începe cu o sedinţă de deschidere prin care Achizitorul va confirma menţinerea solicitărilor sale conform Chestionarului care a stat la baza elaborării Ofertei şi că sunt oferite condiţiile de realizare ale auditului. În cadrul auditului, Prestatorul va folosi cel puţin următoarele metode de analiză:
- interviuri cu reprezentanţii Achizitorului care cunosc procedurile dezvoltate de catre acesta, conform Legii nr. 362/2018 şi care au acces la sistemele, reţelele şi echipamentele sale informatice. Interviurile pot avea loc la sediul Achizitorului şi/sau on-line (ex: prin utilizarea de mijloace de comunicare la distanta: Microsoft Teams, Zoom).
- analiza proceselor, politicilor şi procedurilor dezvoltate de Achizitor pentru conformarea la Legea nr. 362/2018. Documentaţia Achizitorului poate fi pusă la dispoziţia Prestatorului printr-una dintre opţiunile alese de Achizitor (ex: transmitere securizată prin e-mail, furnizarea accesului la documentaţie aflată pe un echipament controlat de Achizitor);
- testarea sistemelor informatice, conform celor solicitate de Achizitor în cadrul Chestionarului care a stat la baza elaborării Ofertei.
La finalul auditului Prestatorul va ţine o sedinţă de închidere în care va prezenta rezultatele auditului efectuat şi care sunt paşii următori. Auditul se va finaliza cu un raport de audit care va fi pus la dispoziţia Achizitorului şi a Directoratului Naţional de Securitate Cibernetică (DNSC). Clientul este informat că prevederile legale impun transmiterea concluziilor raportului de audit către DNSC şi nu se poate îndrepta împotriva Prestatorului pentru încîlcarea obligaţiilor de confidentialitate.
7.10. Prestatorul este responsabil pentru execuţia Serviciilor menţionate în Anexa 1 la prezentul contract în condiţiile prevăzute de lege. În măsura în care pentru executarea unui Serviciu, Prestatorul depinde de îndeplinirea unor obligaţii de către Achizitor faţă de Prestator, conform prezentului contract, iar Achizitorul nu le îndeplineşte, Prestatorul va notifica Achizitorul asupra acestui aspect şi se va menţiona care sunt consecinţele neîndeplinirii acestei obligaţii.
7.11. Prestatorul nu va putea fi făcut răspunzător de omisiuni sau întârzieri datorate lipsei de informaţii din partea Achizitorului asupra proceselor, documentelor, echipamentelor si aplicatiilor existente care vor fi necesar a fi puse la dispoziţie de Achizitor pentru efectuarea Serviciilor de către Prestator.
7.12. Serviciile menţionate în Anexa 1 vor fi efectuate prin eşantionare. Prin urmare, Prestatorul nu va putea fi ţinut răspunzător pentru eventuale omisiuni sau erori cauzate de modalităţile de aplicare a procedurilor interne, zone în care nu a avut acces sau de organizarea internă a Achizitorului, precum şi pentru orice aspecte neprezentate sau prezentate eronat de Achizitor în cursul prestării Serviciilor, sau/şi pentru orice modificare intervenită după prestarea Serviciilor care ar putea să influenţeze validitatea sau acurateţea Serviciilor prestate sau concluziile raportului de audit.
7.13. Printre mijloacele tehnice (echipamente şi instrumente) şi organizaţionale implementate de Furnizor ca parte a auditului se numără: utilizarea unor echipamente securizate, conectarea prin canal securizat la echipamentele care urmează sa fie verificate/testate, solicitarea ca Achizitorul sa dispună de un mediu de test (similar cu mediul de operaţional prin care sunt livrate Serviciile) pe care să fie efectuate testele. În lipsa unui mediu de test care să reproducă identic echipamentele, serviciile şi infrastructura prin care sunt gestionate şi livrate Serviciile în mediul operaţional real, Achizitorul înţelege şi acceptă că există un risc semnificativ ca în cazul testelor efectuate de Prestator direct pe mediul operaţional, acesta să fie afectat din punct de vedere al funcţionării sale în mod normal. Prestatorul nu poate fi ţinut responsabil pentru daunele suferite de Achizitor/terţi, ca urmare a testării sistemelor, echipamentelor informatice direct în mediul operaţional, în lipsa existenţei unui mediu de testare separat;

7.14. Prestatorul își rezervă dreptul de a desemna anumiți auditori atestați, care dețin atestate de auditor de securitate cibernetică valabile eliberate de autoritatea competentă la nivel national, care să presteze Serviciile, în funcție de disponibilitatea acestora privind perioada de desfășurare a auditului dorită de Achizitor, dar și în funcție de competențele tehnice necesare desfășurării lucrării. Numele auditorilor care vor fi selectați de Prestator pentru prestarea Serviciilor conform Ofertei vor fi menționate în planul de audit care va fi transmis și agreat cu Prestatorul înainte de audit; Auditorii atestati desemnați să presteze serviciile nu vor putea subcontracta activitățile pentru care au fost desemnați. Prestatorul are dreptul de a utiliza și experți, în funcție de specificul obiectului de activitate al Achizitorului, în limita a 10% din activitățile de audit. Numele expertilor va fi indicat în planul de audit. Achizitorul va avea dreptul de a solicita recuzarea unui expert numai dacă acesta are legături profesionale cu unul dintre concurenții directi ai Achizitorului. În acest caz, expertul va fi înlocuit cu unul cu aceeași competență profesională, la alegerea Prestatorului.
7.15. Să efectueze auditul numai după o autorizare formală (scrisă) din partea Achizitorului;
7.16. Să informeze Achizitorul despre situațiile care au condus la încălcarea acestui contract;
7.17. Prestatorul se angajează ca acțiunile întreprinse ca parte a auditului de securitate să rămână strict conforme cu obiectivele auditului;

**8. Obligatiile achizitorului**

8.1. Achizitorul se obliga să receptioneze serviciile prestate in termenul convenit prin contract.
8..2. Achizitorul se obliga să plătească prețul contractului conform **art. 5** din acesta.
8.3. Achizitorul se obligă să pună la dispozitia prestatorului orice facilități și/sau informații pe care acesta le consideră necesare pentru îndeplinirea contractului.
8.4. Achizitorul va fi pe deplin responsabil de informațiile/documentele puse la dispoziția prestatorului.
8.5. Să respecte legislatia aplicabilă acestuia precum și angajamentele asumate față de codurile de bună practică, standardele, procedurile pe care le-a dezvoltat, aprobat și s-a angajat ca le respectă.
8.6 Să nu contacteze direct sau indirect personalul Furnizorului (ex: membrii echipei de audit, personal administrativ) pentru alte scopuri în afara celor convenite în cadrul acestui contract (ex: propuneri de angajare/colaborare);
8.7 Să precizeze perioada de timp și condițiile în care pot fi prestate Serviciile, sub forma unei autorizări scrise, adresate Prestatorului;
8.8. Achizitorul autorizează temporar Prestatorul, cu scopul unic de a efectua auditul (Serviciile), să:
- acceseze și să efectueze prelucrarea datelor accesate, indiferent de natura acestor date;
- reproducă, colecteze și să analizeze, în scopul efectuării auditului, date aparținând rețelelor și sistemelor informatice auditate.Toate sistemele accesate, data și ora accesării, precum și testele efectuate vor fi precizate fie într-o **anexă distinctă** a raportului de audit, fie într-un **proces verbal întocmit în acest sens**. De la data semnării raportului de audit/proceselor verbale, acestea vor dobândi data certă și valoare probatorie în privința conținutului.
8.9. Achizitorul înțelege că Prestatorul trebuie să aibă acces la infrastructura auditată pentru a stabili nivelul de conformare a acesteia cu legislația aplicabilă. Lipsa acordării/facilitării accesului deplin la toate datele/informațiile/documentele/infrastructura care constituie domeniul auditului, poate afecta rezultatele auditului sau conduce la imposibilitatea îndeplinirii contractului, această ne-executare neputând fi imputată Prestatorului.

**9. Confidențialitatea si prelucrarea datelor cu caracter personal**

9.1 Fiecare parte este de acord să ia toate măsurile necesare pentru menținerea confidențialității tuturor informațiilor, inclusiv a datelor cu caracter personal, primite, care vor fi cel puțin la nivelul măsurilor luate pentru a proteja propriile informații, inclusiv a datelor cu caracter personal. În cazul în care se constată încălcarea confidențialității, se va informa prompt cealaltă parte și se vor lua măsurile adecvate. Furnizorul declară că pentru îndeplinirea obligațiilor în legătură cu executarea prezentului contract, Furnizorul trebuie să obțină din partea Achizitorului anumite Informații confidențiale și date cu caracter personal.
Termenii acestui paragraf cu privire la Informațiile confidențiale nu se aplică nici unei informații, date, document care:
- la momentul comunicării se află în domeniul public;
- devine ulterior publică, în mod natural și legal, fără a fi încălcate clauzele prezentului contract;
- dezvăluirea este impusă de normele legale în vigoare.

9.2. Achizitorul este informat că, pentru îndeplinirea obiectului prezentului contract:
- este necesar să transmită Prestatorului mai multe categorii de date cu caracter personal (ex: nume, prenume, funcție, telefon, e-mail ale reprezentanților Achizitorului - angajați proprii și/sau reprezentanți ai furnizorilor Achizitorului, implicați în desfășurarea activităților prevăzute în acest contract);

- va primi din partea Prestatorului mai multe categorii de date cu caracter personal (ex: nume, prenume, funcție, telefon, e-mail ale reprezentanților Prestatorului implicați în derularea contractului).
În toate cazurile, Achizitorul se angajează să obțină consimțământul persoanelor ale căror date cu caracter personal va decide să le pună la dispoziția Prestatorului și sa-l informeze pe acesta despre orice schimbare a datelor cu caracter personal colectate, precum și despre orice solicitare venită din partea acestor persoane cu privire la Datele cu Caracter Personal puse la dispoziția lui.
9.3. Părțile se angajează ca, pe întreaga durată de valabilitate a contractului încheiat între ele, precum și pe o perioadă de 3 ani de la data încetării contractului, din orice cauză ar fi aceasta, să:
- exercite cel puțin același grad de diligență cu privire la Datele cu Caracter Personal ale Părții co-contractante pe care îl exercită pentru a-și proteja propriile Date cu Caracter Personal de natură similară; și
- la nivel minim, vor adopta, menține și urma practici și proceduri de securitate scrise și cuprinzătoare care sunt suficiente pentru a proteja Datele cu Caracter Personal împotriva oricărei (i) divulgări, acces, utilizări sau modificări neautorizate; (ii) utilizări abuzive, furt, distrugeri sau pierderi; sau (iii) incapacități de a justifica deținerea respectivelor Date cu Caracter Personal.
9.4 Fără a limita caracterul general al prevederilor de mai sus, Părțile vor folosi sau reproduce Datele cu Caracter Personal doar în măsura în care este necesar să-și îndeplinească obligațiile în conformitate cu Contractul sau orice comandă de lucrări sau dispoziție similară în conformitate cu Contractul. În plus, Părțile vor divulga Datele cu Caracter Personal doar personalului (angajaților) care justifică o nevoie a cunoașterii respectivelor Date cu Caracter Personal (și doar în măsura în care este necesar) pentru îndeplinirea scopurilor prevăzute în Contract.
9.5. Părțile se vor asigura că:
(a) fiecare angajat al lor care va intra în contact cu Datele cu Caracter Personal va fi obligat să își respecte obligațiile de confidențialitate stabilite în prezentul document; și
(b) mențin și urmează practici și proceduri de securitate care sunt suficiente pentru a detecta tipare, practici sau forme specifice de activitate care indică existența posibilă a unui furt sau a unei utilizări abuzive a Datelor cu Caracter Personal. Părțile vor raporta în mod prompt toate aceste incidente sau activități suspicioase. Părțile declară că vor realiza evaluări regulate ale riscurilor pentru a identifica și evalua în mod rezonabil riscurile interne și externe anticipabile asupra securității, confidențialității și integrității evidențelor electronice, imprimate pe hârtie și de altă natură care conțin Date cu Caracter Personal și vor evalua și îmbunătăți, după caz, eficacitatea mecanismelor de protecție pentru limitarea unor asemenea riscuri.
9.6. Părțile nu vor transmite Datele cu Caracter Personal fără a obține aprobarea prealabilă a celeilalte părți. Dacă orice Date cu Caracter Personal sunt transmise (prin corespondență, bandă magnetică, transmisie prin email sau orice alte suporturi de comunicare) respectiva Parte va folosi și se va asigura că angajații săi vor folosi cel mai înalt nivel de diligență pentru a proteja respectivele informații împotriva intruziunii, intervențiilor neautorizate, furtului, pierderii și încălcărilor de confidențialitate.
9.7. Părțile vor înștiința reciproc în mod prompt (și în orice caz în maxim 24 de ore din momentul în care iau cunoștință) în scris, cu privire la orice daună accidentală sau intenționată, alterare, distrugere, divulgare neautorizată, pierdere, utilizare abuzivă sau furt al sau asupra Datelor cu Caracter Personal (inclusiv accesul neautorizat la sau utilizarea Datelor cu Caracter Personal prelucrate in cursul sau in legatura cu prezentul Contract, manevrarea sau ștergerea inadecvată a datelor, furt al unor informații și/sau divulgarea neautorizată accidentală sau intenționată a Datelor cu Caracter Personal) prelucrate în cursul sau in legătură cu Contractul. Părțile își vor oferi reciproc întreaga cooperare pentru a investiga, remedia și reduce impactul efectelor incidentului
9.8. Fiecare Parte are obligația de a realiza informarea persoanelor vizate cu privire la Datele cu Caracter Personal prelucrate în cursul derulării prezentului Contract sau derivând din aceasta. La cerere, fiecare Parte va pune la dispoziția celeilalte Părți informarea întocmită în acest sens.
9.9. Fiecare Parte va raspunde cererilor Persoanelor vizate formulate în legătură cu Datele cu Caracter Personal prelucrate în baza sau în conexiune cu prezentul Contract. În cazul în care pentru soluționarea unei cereri provenind de la o Persoana Vizata sunt necesare informatii suplimentare provenind de la cealalta Parte contractanta, aceasta se angajeaza sa le puna la dispozitie in cel mai scurt timp posibil.
9.10. Obligațiile instituite prin prezenta clauză nu se vor aplica în măsura în care Părțile sunt obligate să divulge Datele cu Caracter Personal în conformitate cu prevederile legii sau cu o dispoziție a unei instanțe, agenție de reglementare sau altă autoritate guvernamentală cu jurisdicție;
9.11 Continutul raportului de audit este confidențial. Părțile care vor accesa raportul de audit din partea Furnizorului sunt: auditorii Furnizorului implicați în prestarea Serviciilor, personalul care gestionează

sistemul informațional al Furnizorului și cel responsabil de relația cu Autoritatea Națională pentru Securitatea Rețelelor și Sistemelor Informatice (ANSRSI. Conținutul raportului de audit se va stoca, în mod securizat la nivelul Furnizorului, în sistemul informațional al acestuia, timp de 5 ani de la data finalizării raportului. Cu toate acestea nu se consideră încălcare a clauzelor de confidențialitate și Furnizorul va putea pune la dispoziția autorităților (ex: ANSRSI) conținutul raportului de audit, parțial sau integral, conform cerințelor legale. Prin semnarea acestui contract Achizitorul se consideră informat asupra acestei clauze si nu se va putea indrepta impotriva Furnizorului pentru incalcarea clauzelor de confidentialitate din acest motiv.

9.12. Nu se consideră încălcarea prezentei clauze de confidențialitate situația în care auditorul este chemat să depună mărturie într-o cauză civilă sau penală sau cazul în care i se solicită detalii sau lămuriri referitoare la obiectul auditului din partea unei autorități competente.

**10. Răspundere si garanții**

10.1 Furnizorul garantează că efectuarea testelor se va realiza într-o manieră responsabilă și profesionistă în conformitate cu bunele practici din domeniu. Prestatorul nu va colecta informații din infrastructura Achizitorului la care i se va permite accesul, care nu sunt relevante pentru verificarea/stabilirea conformității acestuia cu cerințele legale (ex: Legea NIS), conform scopului acestui contract. Prestatorul nu va utiliza datele de conectare la infrastructura Achizitorului după finalizarea prestării Serviciilor. Achizitorul se angajează ca la finalizarea prestării Serviciilor **să schimbe** toate credențialele de acces care au fost puse la dispoziția auditorilor Furnizorului pentru realizarea Serviciilor.

10.2. Achizitorul garantează că are dreptul de detinere legală (este proprietarul) a întregii infrastructurii, sistemelor si aplicatiilor care constituie obiectul prestarii Serviciilor (domeniul auditului) de către Furnizor. În cazul in care Achizitorul nu este detinatorul legal al acestor bunuri, parțial sau integral, el garantează că a obținut toate permisiunile, acordurile necesare si drepturile de acces din partea proprietarului legal al sistemelor supuse prestarii Serviciilor din acest contract, înainte de a permite accesul Prestatorului la acestea.

10.3 Achizitorul acceptă faptul că este imposibil ca Prestatorul să testeze/verifice rețelele, sistemele și personalul clientului pentru fiecare vulnerabilitate sau atac cibernetic existent sau posibil. Serviciile prestate nu garantează că sistemele/aplicatiile/reteaua Achizitorului sunt securizate complet împotriva tuturor formelor de atac posibile, intrucat securitatea cibernetică este intr-o dinamica permanenta. Testele și verificările întreprinse ca urmare a derularii prezentului contract, precum si rezultatele acestora reprezintă abordarea proprie a Prestatorului.

10.4 Terții afectați trebuie să fie anunțați de către Achizitor cu privire la intervalul de timp si modalitatea în care se vor efectua Serviciile din prezentul contract.

10.5 Achizitorul poate opri testarea oricând printr-o notificare adresată Prestatorului prin telefon și prin email. Achizitorul si Prestatorul declară că sunt conștienți de riscurile reprezentate de efectuarea unor teste asupra infrastructurii informatice (ex: refuzul serviciului, indisponibilitatea/defectarea unor echipamente/rețele/sisteme/aplicații, alterarea/stergerea datelor). Prestatorul declară că va acționa cu responsabilitate și profesionalism în cazul efectuări testelor asupra infrastructurii Achizitorului, astfel încât să limiteze pe cât posibil apariția acestor riscuri specifice. Achizitorul declară că își va implementa toate măsurile de prevenire ale apariției acestor riscuri specifice (ex*: disponibilitatea unor medii de test*) cât și că va implementa toate măsurile necesare revenirii imediate la nivelul de funcționare normal al infrastructurii posibil a fi afectate de realizarea testelor, dacă este cazul (ex*: realizarea unor copii de siguranță, disponibilitatea unor echipamente redundante*).

10.6 Prestatorul nu poate fi ținut responsabil pentru eventualele daune aduse de terți asupra datelor/informatiilor/infrastructurii informatice sau fizice ale Achizitorului, ca urmare a exploatării unor vulnerabilități ale acestora.

10.7 Prestatorul nu va fi tinut responsabil pentru prejudicii directe sau indirecte (incluzand dar fara a se limita la: pierderea businessului, veniturilor, profiturilor, datelor, informatiilor, defectarea echipamentelor, intreruperea furnizarii serviciilor Achizitorului) indiferent cand ar putea aparea acestea.

10.8 Achizitorul este singurul responsabil de asigurarea masurilor de protectie adecvata, efectuarea copiilor de siguranta ale datelor si/sau echipamentelor utilizate in legatura cu prestarea Serviciilor Prestaorului si nu va efectua nicio actiune impotriva Prestatorului din cauza unor eventuale pierderi de date, repuneri în funcțiune a serviciilor/aplicațiilor/echipamentelor/infrastructurii, întârzieri în prestarea serviciilor Achizitorului, indisponibilitatea resurselor acestuia, ca urmare a efectuării serviciilor.

10.9 Achizitorul va răspunde în mod normal, conform procedurilor sale interne, atunci când va detecta, în jurnalele echipamentelor sale de alertare, testele efectuate ca urmare a prestarii serviciilor ca și când

sistemele sale ar fi supuse unui atac real, pentru a nu distorsiona rezultatele testelor. Totusi, Achizitorul nu va alerta autoritățile cu privire la aceste teste si nu va intreprinde actiuni legale impotriva Prestatorului ca urmare a prestarii Serviciilor.

10.10 Personalul prestatorului cat si Prestatorul nu pot fi tinuți responsabili pentru și nu își asumă eventualele discordante între concluziile Raportului de audit și unele aspecte concrete din teren, identificate sau identificabile de către terți sau Beneficiar, inclusiv de către reprezentanții autorităților, din următoarele cauze dar fără a se limita la acestea:

- eroarea introdusă de realizarea auditului/testarilor prin prelevarea unor eșantioane;
- acuratețea și/sau completitudinea datelor și informațiilor furnizate de către reprezentanții Beneficiarului;
- erori inerente de comunicare între echipa Prestatorului și reprezentanții Achizitorului, cauzate de înțelegerea diferită a unor termeni sau conditii;
- efectuarea de modificări ale documentației si/sau proceselor/echipamentelor/infrastructurii analizate la momentul efectuarii Serviciilor de catre Prestator sau după finalizarea acestora;
- erori umane;
- consecinte ale unor incidente de securitate produse
- modificari ale sistemelor produse dupa finalizarea auditului
- nefunctionarea unor sisteme care erau operationale la data efectuarii auditului.

10.11 Raportul de audit cu toate anexele sale, metodele și instrumentele de audit sunt și rămân în proprietatea Prestatorului. Achizitorul va primi o copie a raportului de audit și va accepta concluziile raportului de audit, oricare ar fi acestea. Achizitorul convine că nu va face niciun fel de presiuni (ex: financiare, de imagine, operaționale) asupra Prestatorului/auditorilor săi și nu va întreprinde nicio acțiune împotriva acestuia astfel încât concluziile din raportul de audit să fie modificate conform indicațiilor și/sau dorinței Achizitorului. Prestatorul se angajează ca la finalul auditului cât și pe parcusul acestuia să păstreze legătura cu Achizitorul și să explice acțiunile sale ori de câte ori îi va fi solicitat acest lucru de către Achizitor. Prestatorul se angajează să prezinte și să explice concluziile auditului la finalul acestuia.

10.12.Achizitorul va asigura, după caz:

- interfețele privind colaborarea membrilor echipei de audit a Prestatorului cu prestatorii Achizitorului de servicii terți care lucrează în numele său (ex: reprezentanții firmei de IT căreia Achizitorul i-a externalizat serviciile IT);
- desemnarea în mod specific de a responsabilităților acestor prestatori de servicii terți în cadrul auditului efectuat de Prestator;
- disponibilitatea responsabililor săi de detectarea incidentelor de securitate care să colaboreze cu auditorii Prestatorului privind realizarea obiectului acestui contract.

10.13. Prestatorul garantează Achizitorul că nu implică în realizarea Serviciilor alți auditori care nu au nicio relație contractuală cu acesta, care nu au semnat Codul etic al auditorului de securitate cibernetică, care nu au un atestat de auditor de securitate cibernetică valabil eliberat de ANSRSI sau care sunt sub efectul unor sancțiuni, respectiv suspendare sau retragere atestat;

10.14 Părțile convin și garantează că îndeplinesc toate obligațiile legale și de reglementare necesare desfășurării Serviciilor;

10.15 Prestatorul nu va răspunde pentru modalitatea în care Achizitorul implementează recomandările efectuate ca urmare a prestării Serviciilor ce fac obiectul prezentului contract.

10.16 Prestatorul răspunde pentru neexecutarea sau executarea defectuoasă culpabilă a obligațiilor asumate prin prezentul contract. În toate cazurile și din orice motiv, suma totală a despăgubirilor ce pot fi solicitate de Achizitor nu va putea depăși 50 % din valoarea totală a prezentului contract.

10.17 Prestatorul poatesă păstreze anumite tipuri de informații legate de audit odată ce acesta a fost finalizat. Aceste informații pot fi:

- datele de contact ale Achizitorului și reprezentanților săi;
- raportul de audit și anexele sale;
- documentația evaluată de auditorii Prestatorului în cadrul contractului;
- corespondența electronică/fizică avută cu Achizitorul și cu reprezentanții săi.

10.18 Cu exceptia situatiei cand exista o obligatie legala in acest sens care sa impuna pastrarea datelor in forma in care au fost colectate, Achizitorul va anonimiza/sterge/decontextualiza/cripta, după caz, toate informațiile pe care Achizitorul le va indica în scris.

10.19 Toate recomandările auditorilor Prestatorului vor fi efectuate personalului desemnat de Achizitor, pe canalele de comunicare convenite, și vor fi incluse în raportul de audit.

**11. Sancțiuni pentru neîndeplinirea culpabila a obligațiilor**

11.1. Termenul legal/contractual de plată respecta prevederile art. 6, respectiv art. 7 din Legea nr. 72/2013. Modul de determinare si dobânda legală penalizatoare se circumscriu prevederilor art. 8 din Legea nr. 72/2013.Daunele interese minimale vor fi stabilite în conformitate cu art. 10 din Legea nr. 72/2013.
11.2. În cazul in care, din vina sa exclusivă prestatorul nu reuşeşte să-şi execute obligaţiile asumate prin contract, atunci achizitorul are dreptul de a deduce, ca penalităţi, o suma echivalenta cu dobanda legala/zi de intarziere, din valoarea serviciilor neprestate, (cf. art. 176, alin. (2) Cod proc. fiscală).
11.3. In cazul in care achizitorul nu onoreaza facturile in termen de 30 de zile de la expirarea perioadei convenite, atunci acesta are obligatia de a plati, ca penalitati, o suma echivalenta cu dobanda legala/zi de intarziere, din plata neefectuata (cf. art. 176, alin. (2) Cod proc. fiscală).
11.4. Penalitatile datorate curg de drept din data scadentei obligatiilor asumate cf. prezentului contract.
11.5. Pentru prejudiciul provocat prin neexecutarea sau executarea necorespunzatoare a obligatiilor asumate, care depasesc valoarea penalitatilor ce pot fi percepute in conditiile art. 12.2. si 12.3., in completare partile datoreaza daune-interese in conditiile dreptului comun, care pot fi solicitate in baza unei actiuni in justitie, pe cale separata.
11.6. Nerespectarea obligatiilor asumate prin prezentul contract de catre una dintre parti, in mod culpabil si repetat, da dreptul partii lezate de a considera contractul de drept reziliat si de a pretinde plata de daune-interese.
11.7. Achizitorul isi rezerva dreptul de a renunta oricand la contract, printr-o notificare scrisa adresata prestatorului, fara nici o compensatie, daca acesta din urma da faliment, cu conditia ca aceasta anulare sa nu prejudicieze sau sa afecteze dreptul la actiune sau despagubire pentru prestator. In acest caz, prestatorul are dreptul de a pretinde numai plata corespunzatoare pentru partea din contract indeplinita pana la data denuntarii unilaterale a contractului.

**12. Garantia de buna executie a contractului**

În temeiul prevederilor **art. 164, alin. (3)** din **Legea nr. 99/2016** privind achiziţiile sectoriale, achizitorul **nu solicită** constituirea garanţiei de bună execuţie

**13. Recepţie şi verificări**

11.1. Achizitorul are dreptul de a verifica modul de prestare a serviciilor pentru a stabili conformitatea lor cu prevederile legale in domeniu si cu conditiile cuprinse in prezentul contract.
11.2. Verificarile vor fi efectuate in conformitate cu prevederile prezentului contract.
11.3. Achizitorul are obligatia de a notifica, in scris, prestatorului, identitatea reprezentantilor sai imputerniciti pentru acest scop.

**12. Amendamente**

Părţile contractante au dreptul, pe durata îndeplinirii contractului, de a conveni modificarea clauzelor contractului, prin act adiţional, numai în cazul apariţiei unor circumstanţe care lezează interesele comerciale legitime ale acestora şi care nu au putut fi prevăzute la data încheierii contractului

**13. Incepere, finalizare, intarzieri, sistare**

13.1. Prestatorul va începe executarea contractului in cel mai scurt timp posibil de la semnarea acestuia, pana cel tarziu la data de 13..12.2024.
13.2. In cazul in care exista motive de intarziere, care nu se datoreaza prestatorului, sau alte circumstante neobisnuite susceptibile de a surveni, altfel decat prin incalcarea contractului de catre prestator, il indreptatesc pe acesta de a solicita prelungirea perioadei de prestare a serviciilor sau a oricărei faze a acestora, atunci partile vor revizui, de comun acord, perioada de prestare si vor semna un act aditional.
13.3. In afara cazului în care achizitorul este de acord cu o prelungire a termenului de prestare, orice intarziere in indeplinirea contractului da dreptul achizitorului de a solicita penalitati prestatorului în conformitate cu **pct. 9.1.** din prezentul contract.

**14. Modalitati de plată**

Achizitorul are obligatia de a efectua plata contractului in conformitate cu **art. 5** din acesta.

**15. Ajustarea pretului contractului**

15.1. Pentru serviciile prestate, platile datorate de achizitor prestatorului sunt cele convenite prin prezentul contract.
15.2. Achizitorul **nu acceptă ajustarea preţului.**

**16. Cesiunea**

Cesiunea obligațiilor născute din contract este permisă în condițiile reglementate de **art. 237, alin. (2), lit. a) si lit. b) din Legea nr. 99/2016,** actualizată.

**17. Forța majoră și cazul fortuit**

17.1. Forța majoră este constatată de o autoritate competentă.

17.2. Forța majoră exonerează părțile contractante de îndeplinirea obligațiilor asumate prin prezentul contract, pe toată perioada în care aceasta acționează.

17.3. Îndeplinirea contractului va fi suspendată în perioada de acțiune a forței majore, dar fara a prejudicia drepturile ce li se cuveneau părților până la apariția acesteia.

17.4. Partea contractantă care invocă forța majoră are obligația de a notifica celeilalte părți, imediat și în mod complet, producerea acesteia și să ia orice măsuri care îi stau la dispoziție în vederea limitării consecințelor.

17.5. Dacă forța majoră acționează sau se estimează că va acționa o *perioadă* mai mare de 3 luni, fiecare parte va avea dreptul să notifice celeilalte părți încetarea de plin drept a prezentului contract, fără ca vreuna din părți să poată pretinde celeilalte daune-interese.

**18. Soluționarea litigiilor**

18.1. Achizitorul și prestatorul vor face toate eforturile pentru a rezolva pe cale amiabilă, prin tratative directe, orice neînțelegere sau dispută care se poate ivi între ei în cadrul sau în legătură cu îndeplinirea contractului.

18.2. Dacă Achizitorul și prestatorul nu reușesc să rezolve în mod amiabil o divergență contractuală, disputa se va soluționa de către instanța judecatorească de la sediul Achizitorului.

**19. Comunicări**

19.1. Orice comunicare între părți, referitoare la îndeplinirea prezentului contract, trebuie să fie transmisă în scris.

19.2. Orice document scris trebuie înregistrat atât în momentul transmiterii, cât și în momentul primirii.

19.3. Comunicările între părți se pot face și prin telefon, fax sau e-mail cu condiția confirmării în scris a primirii comunicării.

**20. Limba care guverneaza contractul**

Limba care guverneaza contractul este **limba română.**

Părțile au înțeles să încheie azi, **07.11.2024,** prezentul contract în 2 (două) exemplare, câte unul pentru fiecare parte.

Achizitor,
**S.C. AEROPORTUL ARAD S.A.**
**Director General**
**Vasile Ovidiu Moșneag**

Prestator,
**S.C. CERTINSPECT REGISTER S.R.L.**
**Administrator,**
**Răzvan Cristian Ionescu**

Sef Contabil,
**Cosmina Anisia Toma**

**Viza CFP,**

**Viza Juridică,**

**Anexa 1**

| Tip document: | Ofertă tehnică nr. 5650 / 04.11.2024. |
|---|---|
| **Client: Aeroport Arad S.A.** | |
| **Realizarea serviciilor de audit de securitate cibernetică în scopul îndeplinirii nivelului de conformare al organizației cu prevederile legii nr. 362/2018 („legea NIS") privind asigurarea unui nivel ridicat de securitate a rețelelor și a sistemelor informatice** | |

## Introducere

Securitatea cibernetică este noua preocupare majoră a mediului de afaceri. Pregătirea pentru riscul cibernetic are un impact semnificativ asupra cadrului de control intern al organizației și necesită un interes special din toate punctele de vedere: resurse umane, tehnice și organizatorice.

**Uniunea Europeană obligă organizațiile care prestează servicii esențiale pentru populație să își asigure securitatea informatică și să colaboreze cu autoritățile statului pentru a garanta un răspuns coordonat, în cazul apariției unor atacuri informatice.**

Directiva UE 2016/1148 privind securitatea rețelelor și a sistemelor informatice **(directiva NIS), implementată în România prin Legea nr.362/2018 (legea NIS), prevede noi cerințe de securitate cibernetică care trebuie implementate. Aceasta directivă are un impact puternic asupra organizațiilor care nu se conformează întrucât amenzile pot ajunge până la 5% din cifra de afaceri,** conform Legii nr.362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice, care transpune prevederile NIS.

**NIS (Network and Information Security)** vizează protejarea infrastructurilor critice și digitale pentru asigurarea funcționării sistemelor care sunt fundamentale pentru societate și stabilirea măsurilor în vederea obținerii unui nivel comun ridicat de securitate, luând în calcul riscurile asociate. Nu în ultimul rând, prin măsurile impuse, ca orice directivă europeană, NIS vizează protejarea cetățenilor UE împotriva riscurilor cibernetice care ar putea să îi afecteze prin livrarea cu întârziere sau defectuoasă a serviciilor esențiale.

Spre deosebire de GDPR, NIS se adresează unui public determinat:

- **Operatorilor de Servicii Esențiale (OSE)**: entități publice/private din următoarele sectoare de activitate: energie, transport, sector bancar, infrastructuri ale pieței financiare, sănătate, furnizarea și distribuirea de apă potabilă) și
- **Furnizorilor de servicii digitale (DSP-Digital Service Providers)**: piețe online, motoare de căutare online și servicii de cloud computing.

**Certinspect Register este printre primele companii atestate** să efectueze audituri de securitate cibernetică în baza legii NIS (atestat seria CLE nr. 7024/25.08.2021). In timpul auditurilor sunt verificate aspecte precum managementul securității cibernetice, protecția rețelelor și sistemelor informatice, apărarea cibernetică si reziliența serviciilor esențiale oferite populației.

## I. Descrierea generala a serviciului oferit

### I.1. Analiza inițială de securitate cibernetică

Activitățile din această etapă vor consta în:
a) Identificarea serviciilor esențiale (scopului auditului) la fața locului, în sensul legii NIS, în urma analizei serviciilor furnizate de beneficiar către terți;

b) Analiza măsurilor tehnice și organizatorice adecvate și proporționale pentru îndeplinirea următoarelor cerințe minime de securitate de către operator:

- managementul drepturilor de acces;

- conștientizarea și instruirea utilizatorilor;
- jurnalizarea și asigurarea trasabilității activităților în cadrul rețelelor și sistemelor informatice;
- testarea și evaluarea securității rețelelor și sistemelor informatice;
- managementul configurațiilor rețelelor și sistemelor informatice;
- asigurarea disponibilității serviciului esențial și a funcționării rețelelor și sistemelor informatice;
- managementul continuității funcționării serviciului esențial;
- managementul identificării și autentificării utilizatorilor;
- răspunsul la incidente;
- mentenanța rețelelor și sistemelor informatice;
- managementul suporturilor de memorie externa;
- asigurarea protecției fizice a rețelelor și sistemelor informatice;
- realizarea planurilor de securitate;
- asigurarea securității personalului;
- analizarea și evaluarea riscurilor de securitate;
- asigurarea protecției produselor și serviciilor aferente rețelelor și sistemelor informatice;
- managementul vulnerabilităților și alertelor de securitate.

c) Identificarea procesului de comunicare cu DNSC necesar punerii la dispoziția acestei autorități a informațiilor referitoare la incidentele de securitate informatică, a impactului acestora, precum și a oricăror informații ce ar putea fi solicitate;

d) Gestionarea schimbărilor la nivelul serviciilor esențiale furnizate.

Analiza infrastructurii IT este o etapă obligatorie în care se colectează informații despre sistemul ce urmează a fi testat, astfel:

- identificarea infrastructurii IT – în cadrul acestei sub-etape se identifica numărul de IP-uri interne si externe, VPN-uri, numărul de rețele si subretele din cadrul infrastructurii IT a Beneficiarului;
- identificarea echipamentelor și aplicațiilor software care vor fi supuse testelor de vulnerabilitate;
- analiza infrastructurii IT – în cadrul acestei sub-etape se studiază documentația infrastructurii și se strâng informații de la personalul tehnic pentru a avea o imagine detaliată a arhitecturii IT și modului de funcționare al acesteia.

Analiza infrastructurii IT va lua in calcul următoarele elemente:

- topologii de interconectare;
- versiunile programelor de baza (sistem de operare, programe utilitare și servicii ale sistemului de operare);
- aplicațiile utilizate;
- mecanisme de securitate în uz (politicile de securitate din cadrul entității, instrucțiuni sau regulamente de utilizare a echipamentelor, patch-uri si update-uri de securitate, mecanisme de autentificare a utilizatorilor, etc.).

In urma finalizării analizei, se vor colecta informațiile necesare derulării procesului de scanare a vulnerabilităților.

## I.2. Scanare vulnerabilități - Network Enumeration and Scanning

Acest proces are ca scop verificarea vulnerabilităților cunoscute și dacă pot fi exploatate, având în vedere criticalitatea și severitatea lor.

**Metode:**

- Scanarea vulnerabilităților (ex: Nessus, OpenVAS);
- Testarea activă a exploatării vulnerabilităților identificate;
- Verificarea sistemelor de autentificare și acțiuni limitate de brute-force;
- Exploatarea vulnerabilității (ex: Metasploit, Exploituri publice);
- Tehnici post-exploition (accesarea datelor și a sistemelor private).

Procesul de identificare al vulnerabilităților implică scanarea infrastructurii IT a Beneficiarului în scopul identificării vulnerabilităților acesteia și a identificării unor soluții de remediere ulterioare.

Obiectivele vizate in cadrul procesului de identificare a vulnerabilităților sunt următoarele:

**a. Descoperire infrastructura** – identificare servere și alte dispozitive din rețea, folosind soluții standard in industrie.

**b. Detectare servicii** – identificarea porturilor deschise si serviciilor disponibile pe fiecare sistem descoperit, cum ar fi: servicii de email, aplicații Web, servicii de partajare fișiere.

**c. Identificare vulnerabilități** – efectuarea analizei bazate pe sistemul de operare, servicii, configurări și informații culese in fazele anterioare.

**d. Clasificare vulnerabilități** – clasificarea vulnerabilităților descoperite și folosirea standardelor existente (CVE) pentru calcularea impactului riscurilor în funcție de vulnerabilitate.

**e. Raportare** – centralizarea concluziilor, prioritizarea și organizarea în funcție de cerințele Beneficiarului.

**f. Managementul vulnerabilităților** – sortarea și prioritizarea vulnerabilităților se va realiza în funcție de gradul de risc și numărul de echipamente afectate. Soluțiile se vor oferi pentru vulnerabilitățile "Critice" si "Înalte" descoperite.

Scanările de vulnerabilități sunt de doua tipuri:

- **scanări interne** – acestea se efectuează din rețelele controlate de Beneficiar și în cadrul acestora vor fi utilizate conturi de utilizator cu privilegii care permit verificări extinse al versiunilor de servicii si biblioteci ale sistemelor de operare si aplicațiilor, precum și setările acestora;

- **scanări externe** – acestea vor fi efectuate după ce protecțiile firewall de prevenire și detectare a intruziunilor vor fi setate pentru permiterea conectării. Se recomandă folosirea mai multor soluții utilizând teste de penetrare specifice atacatorilor, pentru a se asigura detectarea a cât mai multor vulnerabilități și verificarea rezistenței echipamentelor la vulnerabilități, precum și rezistența hardware la un atac prelungit și constant.

Având in vedere multitudinea de instrumente și tehnici de testare a securității se pot identifica mai multe categorii de astfel de teste:

- teste de verificare a arhitecturii infrastructurii IT;
- scanarea sistemelor în vederea identificării serviciilor de rețea;
- scanarea de vulnerabilități a echipamentelor din rețea;
- scanarea de viruși (malware si ransomware) a echipamentelor din rețea;
- analiza serviciilor de rețea (DNS, DHCP, etc.)
- scanarea serviciilor care rulează pe servere;
- analiza configurațiilor echipamentelor de rețea;
- testarea accesului la echipamentele de tip wireless;
- evaluarea conexiunii la internet si redundanța acesteia.

Scanarea interna pentru vulnerabilități va fi efectuata utilizând un echipament (laptop, miniPC) furnizat de Prestator, instalat în rețeaua locală, cu acces VPN, nerestricționat de firewall sau soluția internă de prevenire și detectare a intruziunilor.

Condiții de efectuare a scanării interne:

- Firewall: soluția de prevenire si detectare a intruziunilor trebuie să permită accesul de la IP-ul intern alocat echipamentului folosit pentru scanări;
- Trebuie create/alocate conturi cu privilegii administrative pentru echipamentele de rețea și serverele testate;

Rezultatele scanărilor de securitate vor fi centralizate într-un raport scris, prezentat sub forma unui rezumat, însoțit de o analiza tehnică detaliată. Raportul va cuprinde, de asemenea, recomandări tehnice cu privire la măsurile necesare a fi implementate pentru asigurarea protecției informatice.
Notă: Scanările pentru detectarea vulnerabilităților tehnice ar trebui reluate periodic, iar vulnerabilitățile identificate în urma raportului, care sunt clasificate "Critice" sau "Înalte", vor trebui remediate în cel mai scurt timp de către personalul care are atribuțiile și drepturile de acces necesare. Pentru vulnerabilitățile identificate ca "Medii" se poate crea un plan de remediere. Pentru o eficiență și siguranță sporită a Beneficiarului punem la dispoziție și un serviciu opțional de consultanță, sub forma unui abonament lunar (ofertă separată).

### I.3. Testele de penetrare

Evaluarea securității infrastructurii IT va fi completată, în această ultimă etapă, prin efectuarea de teste de penetrare, doar pentru aplicațiile critice expuse la internet, care se bazează pe încercarea unor scheme cunoscute de penetrare a sistemelor de calcul prin intermediul exploatării vulnerabilităților de securitate identificate. Anumite testări, ce vor fi agreate cu Beneficiarul, se vor realiza în afara programului de lucru, pentru prevenirea întreruperilor activităților.

Un audit de penetrare cibernetică sau, mai scurt, pentest, reprezintă o activitate de testare a sistemelor de securitate prezente în infrastructura clientului în scopul reducerii riscului de securitate IT.
Testele de penetrare evaluează sistemele de control procedurale și operaționale, precum și cele tehnologice, imită comportamentul malițios al unui atacator extern și nu este necesară cunoașterea detaliilor de acces ale echipamentelor (parole).

Aceste teste de penetrare oferă următoarele beneficii:

- prevenirea unor atacuri informatice ce au la baza vulnerabilități ale sistemului informatic;
- testarea rețelei utilizând o metodologie și instrumente similare cu cele ale atacatorilor;
- verificarea și expunerea vulnerabilităților existente din cadrul infrastructurii IT;
- având o imagine completă și în profunzime a problematicii vulnerabilităților descoperite se poate arăta cum pot fi acestea exploatate pentru atacarea sistemelor;
- testele demonstrează faptul că vulnerabilitățile nu există numai la nivel teoretic, cât și practic;
- oferă o abordare realistă a problemelor de securitate identificate;
- permit testarea procedurilor și a riscului reprezentat de factorul uman (prin tehnici de inginerie socială).

## I.4 Tarife

Următorul tabel prezintă tarifele corespunzătoare serviciilor solicitate și se bazează pe informațiile furnizate de dvs. în documentul „*Chestionar în vederea ofertării serviciului de audit pentru verificarea respectării cerinţelor minime de asigurare a securităţii reţelelor şi sistemelor informatice, conform Ordinului nr. 1323/2020 și prevederilor Legii nr. 362/2018 ("Legea NIS")*" care este parte din prezenta ofertă.

| Nr. crt. | Tipul auditului ofertat | Tarife (LEI fara TVA) |
|---|---|---|
| 1. | *Servicii de audit pentru verificarea respectării cerinţelor minime de asigurare a securităţii reţelelor şi sistemelor informatice, conform Ordinului nr. 1323/2020 și prevederilor Legii nr. 362/2018 ("Legea NIS")* | 29.500 |
| | **TARIF TOTAL:** | **29.500** |

Note: * La prețurile menționate în prezenta ofertă se adaugă TVA.
Pentru alte detalii sau informații suplimentare cu privire la o ofertă de preț, nu ezitați să ne contactați.

**FURNIZOR,**

**CERTINSPECT REGISTER SRL**
**Reprezentant legal:**

**Administrator**

**Răzvan Cristian Ionescu**

**BENEFICIAR,**

**S.C. AEROPORTUL ARAD S.A.**
**Reprezentant legal:**

**Director General**

**Vasile Ovidiu Mosneag**

Vizā juridică

UNIUNEA NAȚIONALĂ A BAROURILOR DIN ROMÂNIA
HOSSZU, IONIȚĂ GEREA, DOBOȘ ȘI ASOCIAȚII S.P.A.R.L.
BARUL ARAD