CONSILIUL JUDEȚEAN CONSTANȚA
DIRECȚIA GENERALĂ ECONOMICO – FINANCIARĂ
BIROUL INFORMATICĂ
• Bd. Tomis nr. 51, Constanța – 900725 • Tel. : 0241-488446 / Fax : 0241-488438 • e-mail : consjud@cjc.ro

Anexă la referat nr.11973 din 11.04.2024

Se aprobă,
PREȘEDINTE C.J.C
LUPU Mihai

CAIET DE SARCINI

Achiziție " Servicii de audit calificat de securitate cibernetică în conformitate cu Directiva NIS nr.1148/2016 transpusă în legislația națională prin Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice "

Cuprins

Terminologie

Terminologie	Definiţii
U.A.T.	Unitatea Administrativ Teritorială
CJC	Consiliul Judeţean Constanţa
SII	Sistem Informatic Integrat
TIC	Tehnologia Informaţiei si Comunicaţiilor
CISM	CISM Certified Information Security Manager (CISM) este o certificare de management si guvernanta, care a fost obţinută de către mai mult de 40.000 de profesionişti de la introducerea sa în 2003. Spre deosebire de alte certificări de securitate, CISM este dedicată persoanelor care gestionează, realizează designul, supraveghează şi evaluează cadrul de Securitate a informaţiei din cadrul unei organizaţii.
CISA	CISA (Certified Information Systems Auditor) este certificarea cea mai populară a ISACA. Din 1978, examenul CISA măsoară excelenţa în domeniul auditului de sisteme informatice, control şi securitate. CISA a crescut până la nivel unei recunoaşteri globale şi a fost adoptată la nivel mondial ca un simbol al performanţei. La nivel mondial există în acest moment peste 150000 de certificări CISA în peste 170 de ţări, iar certificarea CISA este în acest moment certificarea preferată de indivizi şi companii pentru demonstrarea profesionalismului în domeniul auditului de sisteme informatice.
IAPP	Certificările IAPP sunt respectate şi aclamate de angajatori şi concepute special pentru profesioniştii care gestionează, analizează, manipulează şi accesează date sensibile ca parte a aşteptărilor rolului lor
GDPR	Regulamentul General privind Protecţia Datelor (în engleză: General Data Protection Regulation). Este un regulament al Uniunii Europene (UE) care reglementează modul în care datele personale ale cetăţenilor UE sunt colectate, utilizate şi protejate
NIS2	Network and Information Security Directive (Directiva privind securitatea reţelelor şi a informaţiilor)
Hacking	procesul de a accesa sau manipula sistemele informatice, reţele sau dispozitive electronice fără autorizare sau permisiune
Phishing	tehnică de fraudă online prin care atacatorii încearcă să obţină informaţii personale şi confidenţiale, cum ar fi numele de utilizator, parola, informaţiile de cont bancar sau de card de credit, prin intermediul unor mesaje sau site-uri web falsificate
Malware	„software rău intenţionat", care include viruşi, viermi, troieni, spyware şi ransomware
DNSC	Directoratul Naţional de Securitate Cibernetică
RASNIS	RASNIS - raport de audit de securitate a reţelelor şi sistemelor informatice

1. Introducere

Această secțiune a Documentației de Atribuire include ansamblul cerințelor pe baza cărora fiecare Ofertant va elabora Oferta (Propunerea Tehnică și Propunerea Financiară) pentru realizarea serviciilor care fac obiectul Contractului ce rezultă din această procedură.

În cadrul acestei proceduri, U.A.T. Județul Constanța - Consiliul Județean Constanța îndeplinește rolul de Autoritate Contractantă, respectiv Achizitor în cadrul Contractului.

Pentru scopul prezentei secțiuni a Documentației de Atribuire, orice activitate descrisă într-un anumit capitol din Caietul de Sarcini și nespecificată explicit în alt capitol, trebuie interpretată ca fiind menționată în toate capitolele unde se consideră de către Ofertant că aceasta trebuia menționată pentru asigurarea îndeplinirii obiectului Contractului.

2. Contextul realizării acestei achiziții de servicii

U.A.T. Județul Constanța în calitate de Autoritate Contractantă achiziționează servicii de evaluare a infrastucturii hardware și a tuturor politicilor, procedurilor și măsurilor de protecţie implementate la nivelul reţelei şi sistemelor informatice, în vederea identificării disfuncţionalităţilor şi vulnerabilităţilor.

Având în vedere faptul că un sistem informatic integrat (SII) reprezintă totalitatea echipamentelor, aplicaţiilor, fluxurilor şi a activităţilor necesare pentru managementul complet al unei instituţii, prestatorul serviciilor va realiza o analiză tehnică de evaluare a sistemului informatic integrat existent şi a tuturor elementelor informatice care nu fac parte dintr-un sistem integrat aşa cum se înţelege definiţia acestuia în literatura de specialitate dar fac parte din activităţile existente de exploatare a SII al instituţiei.

Astfel, în urma analizei, prestatorul va elabora Raport de Audit de Securitate a Rețelelor și Sistemelor Informatice care va cuprinde recomandări cu privire la activităţile necesare optimizării funcţiilor de utilizare şi management ale SII existent precum şi elaborarea unei strategii de dezvoltare ale SII în vederea optimizării fluxurilor de lucru şi a creşterii securităţii fizice și cibernetice.

2.1. Informații despre Autoritatea Contractantă

U.A.T. Județul Constanța prin Consiliul Județean Constanța cu sediul în Bulevardul Tomis nr.51, este autoritatea administrației publice locale, constituită la nivel județean pentru coordonarea activităţii consiliilor comunale, orăşeneşti şi municipale, în vederea realizării serviciilor publice de interes judeţean.

Instituţia îndeplineşte atribuţii privind: organizarea şi funcţionarea aparatului de specialitate al consiliului judeţean, ale instituţiilor şi serviciilor publice de interes judeţean şi ale societăţilor comerciale şi regiilor autonome de interes județean; dezvoltarea economico-socială a județului; gestionarea patrimoniului județului; gestionarea serviciilor publice din subordine; cooperarea interinstituțională.

Autoritatea Contractantă	Consiliul Judeţean Constanţa	Constanţa, Bulevardul Tomis nr.51, cod poştal 900725 Program de lucru: luni - joi 8:00-16:30 vineri 8:00-14:00

2.2. Informații despre contextul care a determinat achiziționarea serviciilor

- Eficacitate, eficiență, confidențialitate, integritate, disponibilitate, conformitate și încredere.
- Dezvoltarea unei strategii eficiente de integrare a sistemelor informatice la nivelul institutiei.
- Problemele tehnice datorate eterogenității soluţiilor hardware şi software şi diversităţii tehnologiilor utilizate de diversele sisteme informatice din cadrul institutiei.
- Avertismentele constante despre hackeri și securitatea cibernetică, astfel încât instituția să nu rămână vulnerabilă în fața unor amenințări reale.
- Identificarea vulnerabilitatilor sistemului informatic și găsirea unor soluții viabile pentru înlăturarea urmărilor acestora.
- Evoluțiile legislative determinate de necesitatea alinierii la legislația europeană (de ex. Regulamentul General de Protecție a Datelor cu Caracter Personal – GDPR, Directiva NIS2, Legea 58/2023, etc);
- Directiva NIS2 este legislația la nivelul UE privind securitatea cibernetică. Acesta prevede măsuri juridice pentru a stimula nivelul general de securitate cibernetică în UE;
- Obligativitatea respectării cerințelor Legii 58/2023 privind securitatea și apărarea cibernetică a Romaniei prin care administrațiile publice trebuie să adopte și să implementeze politici și măsuri în scopul cunoașterii, prevenirii, comunicării, contracarării vulnerabilităților , riscurilor și amenințărilor în spațiul cibernetic, deoarece legea este aplicabilă rețelelor și sistemelor informatice deținute, organizate, administrate sau utilizate de autorități și instituții ale administrației publice centrale si locale.

2.3. Informații despre beneficiile anticipate de către Autoritatea Contractantă

Achiziţionarea serviciilor de audit calificat a infrastructurii hardware și software pentru U.A.T. Judeţul Constanţa - Consiliul Judeţean Constanţa urmărește îmbunătățirea actului desfășurarii activității în condiții optime, de calitate și securitate fizică și cibernetica care implică:

- Identificarea deficiențelor infrastructurii IT;
- Analiza licențelor software existente;
- Strategie de legalizare a licențelor software;
- Evaluarea riscul IT la nivelul institutiei;
- Identificarea celor mai bune practici de investiție în IT așa încât să beneficiem de întregul potențial al sistemului;
- Dezvoltarea unui plan strategic de dezvoltare al infrastructurii IT;
- Dezvoltarea unui plan de upgrade și troubleshooting al rețelei;
- Alegerea celei mai eficiente metode de protejare a informațiilor existente în cadrul institutiei;
- Realizarea unui proces decizional cu date de intrare colectate și procesate în mod profesionist;
- Conformitatea cu prevederile normativelor/reglementărilor.

2.4. Factori interesați și rolul acestora

Factorii interesaţi sunt persoanele care utilizează echipamentele IT - respectiv salariații U.A.T. Judeţul Constanţa - Consiliul Judeţean Constanţa. Echipamentele IT ce sunt analizate/auditate sunt necesare desfășurării activităţilor specifice intregului colectiv, astfel încât să se asigure în bune și sigure condiţii desfăşurarea în condiţii normale a tuturor activităţilor asigurându-se astfel un grad superior de creștere a eficienței activităților din cadrul CJC cu respectarea legislatiei, regulamentelor și standardelor în vigoare.

Factorii interesați care intră în relație directă cu Contractantul pe perioada derularii Contractului sau ale căror decizii ar putea influența activitatea Contractantului în furnizarea serviciilor sunt specialiștii IT din cadrul Biroului Informatică și reprezentanții Structurii de securitate al Autorității contractante.

3. Descrierea serviciilor solicitate

Servicii de audit hardware si software:

- verificarea configurațiilor la fața locului;
- verificarea procedurilor și politicilor legate de exploatarea echipamentelor IT;
- centralizarea informatiilor despre erorile aparute în serviciile cheie, analiza deficiențelor în sistemul informatic și a limitărilor infrastructurii;
- evaluarea eficienței întregii infrastructuri IT a instituției;
- identificarea deficiențelor în designul infrastructurii;
- indentificarea software-urilor existente și recomandarea de upgrade-uri necesare bunei funcționări;
- identificarea criterilor de securitate și propunerea de noi metode pentru a proteja rețeaua de date de viruși și accese neautorizate ;
- recomandari pentru corectarea erorilor din rețea;
- metode de optimizare a componentelor sistemului și a inventarului IT;
- propuneri de planuri pe termen scurt și lung pentru a moderniza structura rețelei, serverele și echipamentele de rețea, sistemul de printing astfel încât aceasta analiză să ducă la stabilitate și dezvoltare în procesul de transformare digitală.

În cazul constatării unor neconformități, auditorul formulează recomandari pentru remedierea acestora și perfecționarea activității entității .
Constatările vor evidenția punctele tari și punctele slabe ale sistemului informatic și vor menționa aspectele care trebuie remediate.

Toate cerințele din prezentul caiet de sarcini sunt minimale şi obligatorii.

3.1. Descrierea situației actuale la nivelul Autorității Contractante

Eterogenitătatea soluţiilor hardware şi software şi a diversităţii tehnologiilor utilizate de diversele sisteme informatice din cadrul institutiei precum și avertismentele constante despre hackeri și securitatea cibernetică conduc la necesitatea auditării atât din punct de vedere hardware cât și software în contextul digitalizării și securității fizice și cibernetice.

3.2. Obiectivul general la care contribuie realizarea serviciilor

U.A.T. Județul Constanța prin Consiliul Județean Constanța a avut întotdeauna ca obiectiv general crearea unui sistem modern de dotare atât pentru sediul central cât și pentru unitățile aflate în subordine/finanțate, ce oferă posibilitatea desfășurării activităților în bune condiții cu respectarea legislației în vigoare.

3.3. Obiective specifice care contribuie realizarea serviciilor

Obținerea unei asigurari rezonabile asupra implementării și funcționării sistemului în conformitate cu prevederile legislației în vigoare cu reglementarile în domeniu, cu standardele internaționale și ghidurile de bune practici, precum și evaluarea sistemului din punctul de vedere al furnizării unor

servicii informatice de calitate sau prin prisma performanței privind modernizarea administrației și asigurarea încrederii în utilizarea mijloacelor elecronice.

Obținearea unor beneficii în urma analizei tehnice: identificarea oportunităților; găsirea soluțiilor potrivite; evitarea cheltuielilor inutile.

Analiza infrastructurii si a sistemului informatic inclus in domeniul caietului de sarcini este unul de importanță critică pentru desfășurarea în condiții optime și sigure a activităților CJC. Confidențialitatea, integratitatea informatiei și disponibilitatea sistemului informatic al CJC sunt elemente foarte importante. Deasemenea, intrarea posibila a CJC in domeniul de aplicabilitate al legii organice care va implementa Directiva Europeana NIS2 în Romania face ca sistemul de management și tehnologiile adecvate să rezulte în urma unei unei analize tehnice temenice, făcute profesional, dupa standarde si practici internaționale.

3.4. Serviciile solicitate: activitățile ce vor fi realizate

Serviciile de audit calificat de securitate cibernetică solicitate (AS1, AS2, AS4, AS5) în conformitate cu cerințele Legii 362/2018 sunt:

3.4.1 Auditul arhitecturii AS1

- verificarea conformităţii măsurilor de securitate legate de alegerea, poziţionarea şi implementarea dispozitivelor hardware/ software în reţelele şi sistemele informatice a cerinţelor minime de securitate şi a politicilor interne ale institutiei.

3.4.2 Auditul de configurare AS2

- verificarea implementării măsurilor de securitate în conformitate cu stadiul tehnicii, cerinţele minime de securitate şi politicile de securitate în ceea ce priveşte configuraţia dispozitivelor hardware/ software componente ale reţelelor şi sistemelor informatice. Aceste dispozitive pot fi în special echipamente de reţea, sisteme de operare (server sau staţie de lucru), aplicaţii sau produse de securitate.

3.4.3 Auditul de penetrare AS4

- efectuarea de teste specifice în conformitate cu standardele de securitate relevante, adică activități realizate pentru testele de penetrare la nivelul rețelei in vederea identificarii și evaluării vulnerabilităților.

3.4.4 Auditul securitatii organizatiei AS5

- auditul organizaţiei cu privire la securitatea logică şi fizică şi urmărirea asigurării că politicile şi procedurile de securitate definite de operatorul de servicii esenţiale: sunt conforme cu nevoile de securitate ale organizaţiei, nivelul tehnologic şi standardele în vigoare.

În realizarea serviciilor solicitate, activitatea Contractantului va fi condusă de următoarele principii:

a. Contractantul acționează în interesul Autorității Contractante pe durata prestării serviciilor, în condițiile și cu limitele descrise în documentația aferentă prezentei proceduri de atribuire;
b. Contractantul acționează în sensul realizării obiectivelor prezentate pentru Contract în ceea ce privește optimizarea folosirii resurselor necesare îndeplinirii obiectivelor Contractului precum și în ceea ce privește asigurarea profesionalismului resurselor implicate.

3.5. Rezultatele care trebuie obținute în urma prestării serviciilor

Implementarea Contractului în conformitate cu prevederile prezentului Caiet de Sarcini trebuie să conducă cel puțin la atingerea următoarelor rezultate finale măsurabile:

- evaluare a eficienței întregii infrastructuri IT a instituției;
- identificarea deficiențelor în designul infrastructurii;
- indentificarea software-urilor existente și recomandarea de upgrade-uri necesare bunei funcționări;
- identificarea criterilor de securitate și propunerea de noi metode pentru a proteja rețeaua de date de viruși și accese neautorizate;
- recomandari pentru corectarea erorilor din retea;
- metode de optimizare a componentelor sistemului și a inventarului IT;
- dezvoltarea unui plan strategic de dezvoltare al infrastructurii IT;
- dezvoltarea unui plan de upgrade și troubleshooting al rețelei;
- strategie de legalizare a licențelor software;
- raport cu recomandări de acţiuni necesare optimizării funcţiilor de asigurare a utilizării, managementului şi securităţii componentelor sistemului;
- obținerea unei strategii de dezvoltare şi digitalizare la nivelul instituţiei;
- obținerea ghid de guvernanţă şi securitate în domeniul TIC la nivelul instituţiei;
- obținerea unui ghid practic de măsuri minime de asigurare a securităţii sistemului informatic, care sa conțină minim urmatoarele:
  - ✓ Scop si obiective;
  - ✓ Vulnerabilitati, riscuri si amenintari;
  - ✓ Direcții de acțiune;
  - ✓ Implementarea cerințelor minime de securitate conform legislatiei, regulamentelor si standardelor internaționale;
  - ✓ Indicatori de evaluare a conformității.

Alegerea celei mai eficiente metode de modernizare si optimizare a infrastructurii IT și de protejare a informațiilor existente în cadrul institutiei;

3.6. Atribuţiile şi responsabilităţile Părţilor

Contractantul este pe deplin responsabil pentru:

a) realizarea activităţilor conform calendarului activităţilor agreat de ambele părţi în termenele specificate şi se consideră că a luat în considerare toate dificultăţile pe care le-ar putea întâmpina în acest sens şi nu va invoca nici un motiv de întârziere sau costuri suplimentare;
b) în cazul respingerii de către beneficiar a raportului final, prestatorul va comunica cu beneficiarul în vederea modificării raportului prezentat, perioada de comunicare a observaţiilor între părţi şi de elaborare a raportului final fiind de maxim 10 zile lucrătoare de la data notificării privind respingerea raportului de către beneficiar;
c) să informeze beneficiarul în cazul imposibilităţii îndeplinirii prevederilor contractuale şi să justifice cauzele care conduc la această situaţie;

d) răspunde de eventualele încălcări ale obligaţiilor contractuale din vină proprie sau din vina propriilor angajaţi;
e) prestarea serviciilor în conformitate cu cerinţele Caietului de Sarcini.
f) respectarea pe parcursul îndeplinirii obligaţiilor asumate, Normele de protecţie a muncii, Normele de prevenire şi stingere a incendiilor şi protecţia mediului.
g) asigurarea valabilităţii tuturor autorizaţiilor şi certificatelor (atât pentru organizaţia sa, cât şi pentru personalul/echipamentul propus pentru realizarea serviciilor), care sunt necesare (conform legislaţiei în vigoare) pentru prestarea serviciilor;

Pe durata desfăşurării procedurii de auditare, auditorul va răspunde pentru:
h) asigurarea de echipamente IT&C şi licenţe pentru aplicaţiile software utilizate de către echipa de experţi;
i) asigurarea cheltuielilor aferente comunicării;
j) asigurarea de servicii de secretariat şi traducere în limba română, acestea din urmă dacă sunt considerate necesare conform celor menţionate anterior;
k) asigurarea costurilor aferente multiplicării şi imprimării documentelor;
l) auditorul va fi în întregime răspunzător pentru acoperirea cheltuielilor de transport, diurnă şi cazare pentru experţi.

Toate costurile legate de realizarea cerinţelor din caietul de sarcini (costuri materiale, costuri pentru deplasări, costuri pentru plata unor activităţi auxiliare, etc.) vor fi suportate de auditor. Beneficiarul va plăti doar preţul prevăzut în contract.

Autoritatea Contractantă, respectiv beneficiarul este responsabilă pentru:

a) dacă e cazul, va comunica în termenele specificate prestatorului observaţiile sale cu privire la:
   - derularea activităţilor propuse în ofertă în vederea stabilirii calendarul final al activităţii de analiză (maxim 3 zile lucrătoare de la comunicarea ordinului de începere);
   - respingerea raportului RASNIS (maxim 5 zile lucrătoare de la prezentarea de către prestator a raportului). În acest caz, beneficiarul va comunica cu prestatorul în vederea modificării raportului prezentat, perioada de comunicare a observaţiilor între părţi şi de elaborare a raportul final fiind de maxim 1O zile lucrătoare de la data notificării de respingere a raportului de către beneficiar;
b) punerea la dispoziţia prestatorului a datelor şi informaţiilor necesare pentru asigurarea prestării serviciilor ce fac obiectul contractului;
c) va asigura accesul (fizic şi logic) la echipamentele şi aplicaţiile software parte a componentelor SII ce urmează a fi analizat - accesul fizic la echipamentele achizitorului se va efectua numai în prezenţa unui angajat al achizitorului, special desemnat pentru această activitate;
d) va desemna persoanele cu drept de control şi recepţie asupra modului de îndeplinire a contractului de către furnizor;
e) punerea la dispozitia Contractantului, daca este cazul, a unui spatiu de lucru mobilat;
f) va efectua plata conform prevederilor contractului.

4. Ipoteze și riscuri

În pregătirea Ofertei, Ofertanții trebuie să aibă în vedere cel puțin riscurile și ipotezele descrise în continuare. În acest sens, la întocmirea ofertei, Ofertantul trebuie să ia în considerare resursele necesare (de timp, financiare și de orice altă natură), pentru implementarea strategiilor de risc propuse.

a. conținutul serviciilor solicitate este descris în mod explicit în Caietul de Sarcini;
b. nu se prevăd schimbări ale cadrului instituțional și legal care să afecteze major implementarea și desfășurarea în bune condiții a Contractului;
c. toate informațiile relevante și disponibile la nivelul Autorității Contractante pentru realizarea serviciilor vor fi puse la dispoziția Contractantului;
d. Contractantul va semna un acord de confidențialitate la momentul semnării Contractului și va respecta toate instrucțiunile privind utilizarea informațiilor confidențiale (după cum este aplicabil).

Riscuri care pot fi identificate la momentul elaborării Caietului de Sarcini și riscuri care pot apărea în derularea contractului sunt următoarele:

a. nerespectarea calendarului de prestare a serviciilor
b. datele și informațiile transmise de autoritatea contractantă către prestator nu sunt suficiente pentru realizarea obiectului
c. dificultăți de comunicare și colaborare între părțile semnatare ale contractului
d. adăugarea de activități/ solicitări de informații noi, în funcție de progresul activităților.

Riscurile vor fi evaluate din punctul de vedere al impactului și probabilității de apariție.

Nr. Crt.	Riscul identificat	Responsabil	Măsuri de gestionare la nivelul autorității contractante
1	Nerespectarea calendarului de prestare a serviciilor	Prestator Autoritatea contractantă	- stabilirea, după semnarea contractului, a unui calendar ferm de lucru; - desemnarea de responsabili cu urmărirea respectării calendarului de lucru; - desemnarea de persoane de legătură prestator-autoritate contractantă.
2	Datele și informațiile transmise de autoritatea contractantă către prestator nu sunt suficiente pentru realizarea obiectului contractului	Autoritatea contractantă	- solicitarea către prestator a informațiilor și seturilor de date necesare pentru realizarea activitatilor; - identificarea împreună cu prestatorul a unor soluții alternative în cazul în care datele solicitate nu există la nivelul autorității contractante.

3	Dificultăți de comunicare și colaborare între părțile semnatare ale contractului	Prestator Autoritatea contractantă	- facilitarea si intermedierea comunicării cu proprietarii aplicațiilor în cazul în care este nevoie de date și informații suplimentare. - asigurarea suportului, de la departamentele vizate, din cadrul autorității contractante pentru furnizarea de informații.
4	Adăugarea de activități/ solicitări de informații noi, în funcție de progresul activităților.	Autoritatea contractantă	- modalitatea de realizare se va stabili împreună cu prestatorul, cu asigurarea încadrării în prevederile ofertei.

După identificarea vulnerabilităților, este important să se evalueze riscurile asociate cu fiecare vulnerabilitate.

Auditul tehnic trebuie să evalueze minim riscurile asociate cu aplicațiile informatice utilizate, cum ar fi pierderea sau coruperea datelor, testarea securității aplicațiilor în diverse scenarii (de exemplu teste de penetrare) pentru a determina dacă aceastea pot fi compromise prin atacuri de tipul hacking, phishing, malware sau alte metode, posibilitatea sustragerii / înlocuirii ilegale a unor acte sau a istoricului operațiunilor efectuate în aplicații, ș.a.m.d.;

5. Modul de întocmire al ofertei

În vederea îndeplinirii contractului, oferta tehnică va conţine descrierea de ansamblu a abordării propuse de ofertant şi va include prezentarea planului cu etapele de desfăşurare a activităţilor de analiză tehnică, luând în calcul termenele de realizare a activităţilor specificate în caietul de sarcini.

Ofertanţii vor prezenta toate aspectele considerate necesare pentru îndeplinirea contractului şi atingerea obiectivelor, care trebuie sa includa minimal prezentarea metodologiei de lucru, a standardelor de securitate informațională sau alte standarde internaționale aplicabile serviciilor, la care aceștia se raportează.

În cazul în care achizitorul are observaţii cu privire la planul de activităţi prezentat în ofertă de către ofertantul declarat câştigător, acesta va formula şi transmite prestatorului observaţiile sale, în termen de maxim 3 zile lucrătoare de la comunicarea ordinului de începere, în vederea stabilirii de către ambele părţi a calendarului final al activităţii de analiză.

Oferta financiară va fi exprimată în lei fără TVA şi va include toate costurile privind prestarea serviciilor de analiză tehnică conform specificaţiilor.
Nu se va permite modificarea valorii ofertei sau a conţinutului acesteia pe toată perioada derulării contractului.

Oferta tehnică va include asumarea tuturor cerinţelor, cu respectarea specificaţiilor tehnice descrise.

6. Locul și durata desfășurării activităților

6.1. Locul desfășurării activităților

Activitățile incluse în Caietul de sarcini se vor desfășura la sediul Autorității Contractante - Consiliul Judeţean Constanţa în localitatea Constanţa, Bulevardul Tomis nr.51, cod poștal 900725

Pentru activitățile ce trebuie realizate la sediul Autorității Contractante, prestatorul va respecta regulamentul de organizare și funcționare interioară al beneficiarului.

Prestatorul este obligat să ia toate măsurile organizatorice şi tehnice pentru respectarea prevederilor Caietului de sarcini.

6.2. Data de început și data de încheiere a prestării serviciilor sau durata prestării serviciilor

Contractul de achiziţie publică intră în vigoare de la data semnării şi înregistrării acestuia de către ambele părţi şi se finalizează la data îndeplinirii tuturor obligaţiilor contractuale, dar nu mai tarziu de 31.12.2024.

Activitatea de audit calificat (hardware și software) se va realiza pe o perioadă de maxim 2 luni (zile calendaristice) de la data comunicării de către beneficiar a ordinului de începere - achizitorul va transmite prestatorului ordinul de începere în care va specifica data de la care se calculează perioada de prestare a serviciilor şi va preciza termenul maxim de finalizare a prestării serviciilor.

Perioada de 2 luni include toate etapele prestării serviciilor de analiză tehnică detataliată, respectiv:

- stabilirea de către părti a planului cu etapele de desfăşurare a activităţilor de analiză tehnică (în cazul în care beneficiarul are observaţii cu privire la planul propus de către prestator în ofertă);
- auditarea şi evaluarea nivelului de securitate cibernetică a SII existent;
- elaborarea de către prestator a raportului final şi transmiterea acestuia către beneficiar;
- analiza de către beneficiar a raportului comunicat;
- întocmirea planurilor de măsuri şi a ghidurilor ce fac parte din contract;
- perioada alocată comunicării observaţiilor între părţi.

7. Resursele necesare/expertiza necesară pentru realizarea activităților în Contract și obținerea rezultatelor

Activitățile solicitate trebuie executate de către specialiști cu certificari, experiență dovedită, practica dar și de recomandări din partea clienților.

Pentru realizarea activităților în cadrul Contractului, Autoritatea Contractantă anticipează că sunt necesare anumite domenii de expertiză sau următoarele categorii de profesii *:*

Ca urmare, ofertantii trebuie să furnizeze odată cu oferta urmatoarele:

Echipa alocată proiectului trebuie sa aiba cel puțin

a) 1 auditor atestat DNSC pentru activitati comune de audit NIS (se va prezenta atestatul) cu certificarea ISACA Certified Information Manager (CISM) sau similar, sau cu certificarea ISACA Certified Information Systems Auditor (CISA), sau similar.
b) 1 expert de securitate care sa aiba una din urmatoarele certificari
   - GIAC Security Leadership (GSLC) sau similar

- ISC2 Certified Information Systems Security Professional (CISSP) sau similar
- ISC2 Systems Security Certified Practitioner (SSCP) sau similar
- IAPP – Fellow of Information Privacy (FIP) sau similar

c) Lista de referințe/recomandari pentru activități similare celor incluse în acest caiet de sarcini.
   - referințe pentru pre audit sau audit NIS, sau audit de securitate sau consultanță de securitate cibernetica pentru minim 3 clienti;

d) Scrisoare de recomandare și permisiunea de verificare a referinței la clientul pentru care s-a prezentat referința/recomandarea.

Autoritatea contractantă poate solicita înlocuirea unui expert pe perioada de derulare a contractului pe baza unei cereri scrise și justificate dacă se consideră că acesta este ineficient sau nu își îndeplinește sarcinile conform cerințelor din Caietul de Sarcini și ofertei transmise de prestator.

Prestatorul poate înlocui, doar din motive obiective, expertul propus, doar cu acordul entității contractante și doar cu experți care demonstrează un nivel minim similar de expertiză cu al expertului acceptat inițial.

7.1. Infrastructura Contractantului necesară pentru desfășurarea activităților Contractului

Ofertantul devenit Contractant trebuie să se asigure că personalul care își desfășoară activitatea în cadrul Contractului, dispune de sprijinul material și de logistica necesară pentru a permite acestuia să se concentreze asupra realizării activităților din cadrul Contractului.

7.2. Infrastructura și resursele disponibile la nivel de Autoritate Contractantă pentru îndeplinirea Contractului

Sistemele informatice supuse auditării tehnice:

- ✓ server web=1
- ✓ server aplicatii=15
- ✓ routere: 1 acces net
- ✓ 1 pt. proiect
- ✓ 1 cu functii de routare folosit de serverul web
- ✓ 10 AP-uri Wifi
- ✓ switch-uri=39 (21 cu management si 18 fara management)
- ✓ laptop-uri=75
- ✓ desktop-uri=267
- ✓ MFP=65
- ✓ Printer=20

8. Cadrul legal care guvernează relația dintre Autoritatea Contractantă și Contractant (inclusiv în domeniile mediului, social și al relațiilor de muncă)

Contractantul trebuie să respecte toate prevederile legale, aplicabile la nivel național, dar și regulamentele aplicabile la nivelul Uniunii Europene .

Pe perioada realizării tuturor activităților din cadrul Contractului, Contractantul este responsabil pentru implementarea celor mai bune practici, în conformitate cu legislația și regulamentele existente la nivel național și la nivelul Uniunii Europene. Contractantul va fi ținut deplin responsabil pentru subcontractanții săi în prestarea serviciilor prevăzute în Caietul de Sarcini, urmând să răspundă față de Autoritatea Contractantă, pentru orice nerespectare sau omisiune a respectării oricăror prevederi legale și normative aplicabile. Autoritatea Contractantă nu va fi ținută responsabilă pentru nerespectarea sau omisiunea respectării de către Contractant sau de către subcontractanții acestuia a oricărei prevederi legale sau a oricărui act normativ aplicabil precum și atât pentru prestarea serviciilor cât și pentru rezultatele generate de prestarea serviciilor.

În cazul în care intervin schimbări legislative, Contractantul are obligația de a informa Autoritatea Contractantă cu privire la consecințele asupra activităților care fac obiectul Contractului și de a-și adapta activitatea în funcție de decizia Autorității Contractante în legătură cu schimbările legislative. În cazul în care o astfel de situație este aplicabilă trebuie precizat în Contract mecanismul de soluționare a unor astfel de situații.

Ofertantul devenit Contractant are obligația de a respecta în executarea Contractului, obligațiile aplicabile în domeniul mediului, social și al muncii instituite prin dreptul Uniunii, prin dreptul național, prin acorduri colective sau prin dispozițiile internaționale de drept în domeniul mediului, social și al muncii enumerate în anexa X la Directiva 2014/24, respectiv:

a. *Convenția nr. 87 a OIM privind libertatea de asociere și protecția dreptului de organizare;*
b. *Convenția nr. 98 a OIM privind dreptul de organizare și negociere colectivă;*
c. *Convenția nr. 29 a OIM privind munca forțată;*
d. *Convenția nr. 105 a OIM privind abolirea muncii forțate;*
e. *Convenția nr. 138 a OIM privind vârsta minimă de încadrare în muncă;*
f. *Convenția nr. 111 a OIM privind discriminarea (ocuparea forței de muncă și profesie);*
g. *Convenția nr. 100 a OIM privind egalitatea remunerației;*
h. *Convenția nr. 182 a OIM privind cele mai grave forme ale muncii copiilor;*

Actele normative și standardele indicate mai jos sunt considerate indicative și nelimitative; enumerarea actelor normative din acest capitol este oferită ca referință și nu trebuie considerată limitativă:

- Legea 98/2016 privind achizițiile publice, cu modificările și completările ulterioare;
- H.G. nr.395/2016 pentru aprobarea Normelor metodologice de aplicare a prevederilor referitoare la atribuirea contractului de achiziție publică/ acordului cadru din Legea nr. 98/2016 privind achizițiile publice, cu modificările și completările ulterioare;
- Instrucțiune ANAP nr.1/2021 privind modificarea contractului de achiziție publică/ contractului de achiziție sectorială/ acordului-cadru;
- Ordinul nr. 1.554/2023 privind aprobarea structurii şi conţinutului Documentaţiei standard de atribuire a contractului de achiziţie publică/sectorială de produse;
- Regulamentul (UE) nr. 241/2021 al Parlamentului European şi al Consiliului din 12 februarie 2021 de instituire a Mecanismului de redresare şi reziliență;
- Regulamentul Delegat (UE) 2021/2106 al Comisiei din 28 septembrie 2021 de completare a Regulamentului (UE) 2021/241 al Parlamentului European și al Consiliului de instituire a Mecanismului de redresare și reziliență prin stabilirea indicatorilor comuni și a elementelor detaliate ale tabloului de bord privind redresarea și reziliența;

- Decizia de punere în aplicare a Consiliului de aprobare a evaluarii planului de redresare şi rezilienţă al României din 29 octombrie 2021;
- În vederea aplicării prevederile art. 5 alin. (1) din Legea nr. 354/2022 privind protecţia sistemelor informatice ale autorităţilor şi instituţiilor publice în contextul invaziei declanşate de Federaţia Rusă împotriva Ucrainei, publicat în Monitorul Oficial, Partea I nr. 1200 din 14 decembrie 2022;
- În temeiul art. 12 alin. (3) din Hotărârea Guvernului nr. 371/2021 privind organizarea şi funcţionarea Ministerului Cercetării, Inovării şi Digitalizării, cu modificările şi completările ulterioare;
- Hotărârea nr. 1321/2021 privind aprobarea Strategiei de securitate cibernetică a României, pentru perioada 2022-2027, precum şi a Planului de acţiune pentru implementarea Strategiei de securitate cibernetică a României, pentru perioada 2022-2027
- Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice, denumită în continuare Legea NIS, transpune în legislația națională Directiva (UE) 2016/1148 (NIS) a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune. Implementarea Legii NIS la nivelul României intră în atributul Directoratului Național de Securitate Cibernetică, DNSC, autoritate competentă la nivel național pentru securitatea rețelelor și sistemelor informatice.
- Legea nr. 182/2002 privind protecția informațiilor clasificate;
- Prevederile art.33. art.88-90 și Anexei nr.10E din Standardele naționale de protecție a informațiilor clasificate în România aprobate prin Hotărârea Guvernului nr.;
- Legea 58/2023 privind securitatea şi apărarea cibernetică a României, precum şi pentru modificarea şi completarea unor acte normative
- GHID PRACTIC PENTRU OSE Implementarea măsurilor minime de asigurare a securității rețelelor și sistemelor informatice, ISACA Romania Chapter (Information Systems Audit and Control Association – organizația din România)

8.1. Managementul/Gestionarea Contractului și activități de raportare în cadrul Contractului

Autoritatea Contractuală va asigura managementul si gestionarea contractului pe toata perioada derularii acestuia, respectiv coordonarea, monitorizarea și controlul tuturor activităților și rezultatelor realizate de Contractant

8.2. Elaborarea raportului de Audit de Securitate Cibernetică (RASNIS)

În baza analizei tuturor aspectelor menţionate, precum şi a celor pe care prestatorul le consideră necesare, dar nu au fost specificate, prestatorul va elabora Raportul de Audit de Securitate în conformitate cu Legea NIS (RASNIS) în care va stabili nivelul de securitate cibernetică a sistemului informatic din cadrul Consiliului Județean Constanța, conformitatea acestuia cu cerințele minime de securitate cerute de Legea NIS. Va prezenta recomandările cu privire la acţiunile corective (dacă e cazul) şi ghidurile cu măsurile necesare pentru optimizarea şi asigurarea funcţionalităţii, a managementului şi a securităţii componentelor sistemului informatic.

În elaborarea măsurilor se va avea în vedere configuraţia SII existent, iar pentru fiecare soluţie propusă se va preciza prioritatea de îndeplinire a măsurii, respectiv importanţa şi iminenţa implementării soluţiei (termen scurt, mediu, lung).

În termen de maxim 5 zile lucrătoare de la prezentarea de către prestator a raportului, beneficiarul va notifica prestatorul cu privire la aprobarea/respingerea raportului, cu prezentarea motivelor în cazul al doilea.

În cazul în care beneficiarul va respinge raportul:

- prestatorul va analiza observaţiile şi va comunica cu beneficiarul în vederea clarificării acestora şi unde e cazul, va modifica raportul prezentat;
- modificarea raportului final se va realiza de către prestator fără modificarea preţului contractului;
- perioada de comunicare a observaţiilor între părţi este de maxim 1O zile lucrătoare de la data notificării cu privire la respingerea raportului, urmând ca până la finalul acestei perioade, prestatorul să elaboreze raportul final în vederea aprobării/acceptării de către beneficiar.

Raportul de Audit (RASNIS) şi documentele relevante rezultate în urma prestării serviciilor vor deveni proprietatea beneficiarului.

9. Metodologia de evaluare a Ofertelor prezentate

Atribuirea Contractului se va face aplicând criteriul de atribuire „preţul cel mai scăzut".

Autoritatea contractantă îşi rezervă dreptul de a respinge oferta care nu se încadrează în specificaţiile solicitate prin Caietul de sarcini, chiar dacă acesta are preţul cel mai scăzut.

10. Cerințe de asigurare a calitații

Prestatorul se va asigura că raportul de audit (RASNIS) va fi realizat conform cerințelor stabilite de către Directoratul National de Securitate Cibernetică prin actele normative emise în acest sens.

11. Cerințe de recepție

Acceptarea raportului final se va realiza pe bază de proces verbal de acceptanță, dupa analizarea acestora de către beneficiar.

Recepția raportului final se va face în termen de 10 zile lucrătoare de la primirea confirmării de către beneficiar .

12. Limba documentației de atribuire , a ofertei, a contractului și a documentelor aferente

Limba română.

13. Efectuarea plăților în cadrul Contractului

Plata integrală a serviciilor se va efectua de către achizitor, prin ordin de plată, în termen de 30 de zile de la data la care factura electronică este disponibilă pentru descărcare din sistemul RO e-factura.

Factura va fi însoţită de procesul-verbal de recepţie precizat în capitolul 11.

14. Clauze de confidențialitate

Între părțile implicate se va semna un Acord de confidențialitate care are drept scop protejarea datelor și informațiilor neclasificate, proprietate CJC.

Autoritatea Contractantă va dobândi în baza contractului încheiat în urma derulării achiziției, după momentul recepționarii serviciului și achitarea prețului contractului, dreptul de utilizare exclusivă, nerestricționată teritorial, nelimitată în timp a documentațiilor livrate, precum și (în aceleași condiții) următoarele drepturi patrimoniale asupra documentațiilor: dreptul de reproducere, dreptul de distribuire, dreptul de închiriere, dreptul de împrumut, dreptul de comunicare publică prin orice mijloace și dreptul de realizare de alte documentații, informări/prezentări /materiale derivate, indiferent de suportul pe care se vor găsi acestea.

Diseminarea către un terț a informațiilor nepublicate aferente acestui contract de servicii, care sunt proprietatea CJC de către Contractant în vederea accesului la informații nepublicate aferente acestui contract de servicii, se face numai cu acordul scris al deținătorului acestora, respectiv CJC.

15. Alte cerințe

În cazul în care activitățile contractului necesită utilizarea unor date cu caracter personal, prestatorul va prelua toate obligațiile prevăzute de prevederile în domeniu, în conformitate cu Regulamentul nr. (UE) 679/2016 al Parlamentului European și al Consiliului privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE, coroborate cu cele ale Legii nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679.

16. SEMNĂTURI/ AVIZE:

	NUME	FUNCŢIA	SEMNĂTURA	DATA
ELABORAT	Minerva DANCU	Inspector de specialitate, Biroul IT		25.04.2024
VERIFICAT	Daniel PITU	Inspector, Serviciul Monitorizare Investitii Proiecte, Avizare		26.04.2024
AVIZAT	Emilia Georgeta ȚUȚUI	Director General, D.G.E.F		25.04.2024
APROBAT	Stelian GIMA	Vicepreședinte, Șef Structură Securitate		29.04.2024