Caiet de sarcini

pentru achiziția serviciilor de testare și audit de securitate a sistemelor/produselor Agenției de Guvernare Electronică

1. Prevederi generale

Prezentul caiet de sarcini stabilește cerințele tehnice și operaționale pentru achiziționarea serviciilor specializate de testare și audit a securității cibernetice pentru sistemele/resursele informaționale dezvoltate, implementate sau gestionate de Agenția de Guvernare Electronică (AGE).

Complexitatea sporită a peisajului de amenințări cibernetice, coroborată cu diversificarea tehnologiilor utilizate în serviciile publice, impune necesitatea contractării unei expertize terțe în vederea realizării testelor de securitate ale sistemelor/resurselor informaționale aferente.

În mod special, AGE se află într-o etapă de expansiune a portofoliului său de servicii digitale, prin dezvoltarea și lansarea unor soluții de nouă generație care vor redefini interacțiunea cetățeanului cu statul. Lansarea unor platforme critice precum Portofelul de identitate digitală (Wallet 2.0), Serviciul guvernamental de identitate și semnătură electronica mobilă (EVOSign), Serviciul guvernamental de identificare a persoanei la distanță (eKYC), introduce noi suprafețe de atac și fluxuri de date de o sensibilitate deosebită. Aceste sisteme, care gestionează identitatea digitală, autentificarea utilizatorului și date biometrice, impun un nivel superior de validare a securității, care depășește testarea tradițională și necesită o expertiză specializată în domeniile de referință.

2. Obiectul și scopul achiziției

Obiectul prezentei achiziții îl constituie încheierea unui contract pentru prestarea de servicii de evaluare a securității, care includ servicii de testare a securității (testare la vulnerabilități, teste de penetrare) și servicii de audit de securitate (verificarea conformității cu standardele aplicabile). Aceste servicii vor viza sistemele, platformele, infrastructurile și modulele aplicative dezvoltate, modernizate sau administrate de AGE, incluse în domeniul de aplicare. Serviciile vor fi prestate conform unui plan de implementare agreat, pentru perimetrul definit în prezentul document.

Scopul general al contractului este de a asigura și valida un nivel superior de securitate, confidențialitate, integritate și disponibilitate pentru portofoliul de servicii publice electronice, incluse în domeniul de aplicare. Atingerea acestui scop se va realiza prin îndeplinirea următoarelor obiective specifice:

a) **Identificarea, analiza și documentarea exhaustivă a vulnerabilităților** tehnice și logice la nivel de aplicație, infrastructură și cod sursă.
b) **Simularea controlată a atacurilor reale (teste de penetrare)** pentru a evalua eficiența măsurilor de protecție existente, nivelul de expunere și posibilitatea de escaladare a accesului, fără a produce întreruperi ale serviciilor.
c) **Furnizarea de recomandări tehnice detaliate** pentru remedierea tuturor deficiențelor, vulnerabilităților și neconformităților identificate, clasificate în funcție de prioritate și impact.
d) **Validarea eficienței măsurilor de remediere**, prin testare follow-up (unde este aplicabil), pentru a asigura eliminarea vulnerabilităților într-un mod controlat.
e) **Analiza conformității cu standardele de securitate aplicabile** serviciului/sistemului/aplicației.

3. Domeniul de aplicare a serviciilor

Domeniul de aplicare al serviciilor acoperă o gamă largă de active informatice și servicii de testare, reflectând diversitatea și complexitatea ecosistemului digital guvernamental.

3.1. Sisteme în domeniul de aplicare

Serviciile de testare a securității sunt solicitate pentru ecosistemul digital gestionat de AGE. Următoarele soluții guvernamentale de nouă generație reprezintă perimetrul principal al acestei achiziții:

- **Portofelul de identitate digitală (Wallet 2.0);**
- **Serviciul guvernamental de identitate și semnătură electronica mobilă (EVOSign);**
- **Serviciul guvernamental de identificare a persoanei la distanță (eKYC).**

3.2. Servicii de testare a securității

Prestatorul va oferi următoarele două categorii principale de servicii de testare:

3.2.1. Testare de securitate

Serviciile de testare a securității sunt de natură ofensivă și se concentrează pe identificarea și exploatarea practică a vulnerabilităților tehnice. Acestea vor include următoarele activități:

- **Testare de vulnerabilități:** Utilizarea de instrumente automate, completată de verificări manuale, pentru a scana și identifica vulnerabilități cunoscute, configurări eronate și lipsa actualizărilor de securitate.
- **Testare de penetrare:** O abordare practică, bazată pe scenarii de atac, care simulează acțiunile unui atacator real. Tipurile de testare de penetrare includ: Black Box (fără cunoștințe prealabile despre arhitectura internă), Gray Box (cu acces limitat, la nivel de utilizator autentificat), White Box (cu acces complet la codul sursă și documentația de arhitectură).
- **Revizuirea codului sursă (Security code review):** Analiza statică și manuală a codului sursă pentru identificarea defectelor de programare, a secvențelor de cod susceptibile la vulnerabilități și a erorilor în logica de business, în baza unei metodologii riguroase adaptate proiectului.

3.2.1. Audit de securitate (GAP Assessment)

Serviciile de audit de securitate este de natură defensivă și se concentrează pe verificarea conformității sistemului/serviciului cu standardul de referință și bune practici recunoscute, care vor include, dar nu se vor limita la (dependent de sistem, se va stabili la etapa de planificare):

- Cadrul de reglementare eIDAS, în special în ceea ce privește cerințele pentru serviciile de încredere și portofelele de identitate digitală europeană (EUDI Wallet).
- OWASP MASVS (Mobile Application Security Verification Standard) pentru aplicațiile mobile.
- ISO/IEC 30107 pentru mecanismele de detecție a atacurilor de prezentare din sistemele biometrice.

4. Metodologie și abordare tehnică

Prestatorul va trebui să demonstreze o abordare matură și structurată a procesului de testare și audit a securității, aliniată la cele mai bune practici și standarde internaționale.

4.1. Cadrul general de testare și audit de securitate

Prestatorul va demonstra și aplica în mod obligatoriu metodologii de testare și audit de securitate, fundamentate pe următoarele cadre de referință internaționale:

- **OWASP (Open Web Application Security Project):** dependent de sistemul/resursa scanată, se va solicita alinierea la Web Security Testing Guide (WSTG), Mobile Application Security Verification Standard (MASVS), Mobile Application Security Testing Guide (MASTG) și OWASP Top 10.
- **ISO/IEC:** cadrul general de management al securității informației conform ISO/IEC 27001/27002, de management al riscurilor conform ISO/IEC 27005, precum și alte standarde ISO aplicabile scopului. Pentru testarea specifică a sistemelor în care se prelucrează date biometrice, se va asigura conformitatea cu ISO/IEC 30107 (Biometric presentation attack detection).
- **NIST SP 800-115**: ghid tehnic pentru activități de testare a securității, inclusiv planificarea, executarea și documentarea testelor de securitate.
- **Cadrul european de reglementare eIDAS / EUDI Wallet:** acest cadru este esențial pentru auditarea conformității soluțiilor de identitate digitală și servicii de încredere (Wallet 2.0, EVOSign) în vederea asigurării interoperabilității la nivel european.
- Alte metodologii și ghiduri, precum MITRE ATT&CK, CIS Benchmarks, PTES (Penetration Testing Execution Standard), utilizate pentru activitățile de colectare de informații, modelare a amenințărilor, exploatare, post-exploatare și raportare.

4.2. Etapele proiectului

Pentru fiecare din sistemele/serviciile incluse în domeniul de aplicare, se va urma un proces structurat în trei etape principale, conform modelului stabilit în astfel de proiecte:

Etapa I: Planificare și pre-evaluare

Această etapă determină desfășurarea eficientă a activităților ulterioare.

- **Activități:** Organizarea unei ședințe de start (kick-off) cu toate părțile implicate; definirea clară a perimetrului (scoping) și a obiectivelor; stabilirea regulilor de angajament, inclusiv a perioadelor de timp pentru testare și a procedurilor de escaladare; definirea scenariilor de testare și/sau standardelor de audit care vor fi utilizate pentru fiecare din cele trei sisteme; identificarea persoanelor de contact tehnice și de business; obținerea autorizațiilor scrise necesare pentru desfășurarea testelor.
- **Livrabile:** Plan de proiect, Plan de testare și audit (Scope of Work – SoW), inclusiv scenarii, metodologii și instrumente), aprobate de AGE.

Etapa II: Evaluare și testare

Aceasta este faza de execuție practică, în care prestatorul va desfășura efectiv activitățile de testare și audit de securitate.

- **Activități:** Ariile minime de testare a securității trebuie să acopere, fără a se limita la, următoarele domenii, inspirate din cadrul general de testare și audit de securitate, în corespundere cu cerințele detaliate în documentele de referință:
  - Configurarea și gestionarea implementării securizate;
  - Managementul identificării și autentificării;
  - Controlul accesului;
  - Validarea datelor de intrare;
  - Managementul erorilor și log-urilor;
  - Securitate criptografică;

- Testarea logicii de business;
- Securitate la nivel client;
- Testare API;
- alte domenii, conform cadrului de testare stabilit.

În cazul auditului de securitate (GAP Assessment): activitatea va consta în verificarea sistematică a controalelor de securitate ale aplicației prin comparație cu standardul de referință, stabilit la etapa de planificare. Pentru fiecare cerință a standardului, se va analiza arhitectura, configurația și, unde este necesar, codul sursă, pentru a determina gradul de conformitate.

- **Livrabile:** Rapoarte intermediare de progres (la cerere), notificări în timp real (în maxim 24 de ore) pentru vulnerabilitățile cu severitate Critică.

Etapa III: Analiză, raportare și testare follow-up

Această etapă finalizează ciclul de testare și asigură transferul de cunoștințe către AGE.

- **Activități:** Analiza, corelarea și validarea tuturor rezultatelor obținute; clasificarea vulnerabilităților identificate utilizând un sistem standardizat (CVSS v4.0); elaborarea rapoartelor detaliate; prezentarea rezultatelor către echipele tehnice și managementul AGE; acordarea de suport și clarificări pentru înțelegerea deplină a riscurilor și a măsurilor de remediere.
- **Testare follow-up:** După ce echipa de dezvoltare a AGE sau a furnizorilor săi implementează măsurile de remediere, Prestatorul va efectua o testare follow-up pentru a valida corectitudinea și eficacitatea acestora și pentru a confirma închiderea vulnerabilităților.
- **Livrabile:** Rapoarte de test și de analiză cu recomandări detaliate, Rapoarte de follow-up.

4.3. Cerințe specifice pentru sisteme cu date biometrice (eKYC)

Prestatorul trebuie să demonstreze capacitatea și experiența de a efectua următoarele teste specifice:

a) **Testarea detectării atacurilor de prezentare (conform ISO/IEC 30107 Biometric presentation attack detection):** atacuri 2D (Utilizarea de fotografii printate de înaltă rezoluție, măști de hârtie, precum și prezentarea de imagini sau videoclipuri pe ecrane de înaltă definiție (telefon, tabletă); atacuri 3D **(**utilizarea de măști realiste sau modele 3D printate pentru a încerca să înșele sistemele de recunoaștere facială); atacuri video (utilizarea de înregistrări video ale utilizatorilor legitimi sau, mai avansat, de videoclipuri deepfake pentru a ocoli mecanismele de verificare); testarea mecanismelor de detecție a vivacității (liveness detection).
b) **Evaluarea securității ciclului de viață al datelor biometrice:** Se va evalua securitatea pentru următoarele etape: capturare date, procesare și stocare, transmisie și ștergere date biometrice.
c) **Testarea vulnerabilităților specifice eKYC:** Atacuri de replay (încercarea de a intercepta și re-utiliza pachete de date de la o sesiune de înrolare sau autentificare validă pentru a obține acces neautorizat sau a crea un cont duplicat); falsificarea documentelor (încercarea de a încărca documente de identitate modificate digital, de exemplu, schimbarea fotografiei, a numelui pentru a testa capacitatea sistemului de a detecta falsuri și a ocoli mecanismele de validare; ocolirea legăturii biometrice (testarea scenariilor în care un atacator încearcă să finalizeze un proces de înrolare folosind un document de identitate autentic al unei persoane, dar o probă biometrică/ selfie de la o altă persoană, pentru a verifica dacă sistemul validează corespondența dintre cele două.

5. Livrabile, raportare și monitorizare

Claritatea și calitatea livrabilelor sunt esențiale pentru a asigura valoarea serviciilor contractate.

Prestatorul va furniza următoarele documente, cu structura corespunzătoare. Toate documentele vor fi elaborate în limbile română și engleză.

5.1. Lista Livrabilelor

Pentru fiecare din sistemele/serviciile incluse în domeniul de aplicare, Prestatorul va furniza următoarele documente de proiect, structurate pe etape:

- **Etapa I (Planificare):**
  - **Plan de Proiect:** Include graficul de implementare, resursele alocate și managementul riscurilor proiectului.
  - **Plan de testare și audit** (SOW)**:** Document detaliat care descrie metodologia specifică, scenariile de testare și/sau standardele de audit care vor fi utilizate (pentru fiecare din cele trei sisteme.
- **Etapa II (Evaluare):**
  - Rapoarte intermediare de progres (la cerere).
  - Notificări în timp real (în maxim 24 de ore) pentru vulnerabilitățile cu severitate Critică.
- **Etapa III (Post-evaluare):**
  - Raport final de testare a securității (câte un raport pentru fiecare sistem/aplicație).
  - Raport de testare follow-up (care confirmă sau infirmă remedierea vulnerabilităților).
  - Raport de audit al conformității sistemului cu standardul specificat la etapa de planificare (câte un raport pentru fiecare sistem/aplicație).
- **După caz, la cerere:**
  - Rapoarte de progres a activității, care detaliază activitățile desfășurate, resursele consumate și stadiul general al contractului.

5.2. Structura rapoartelor finale

5.2.1. Raportul final de testare a securității (pentru fiecare sistem din domeniul de aplicare) va fi structurat în două părți distincte:

- Partea I - Sumar executiv (Executive Summary): Destinat personalului de decizie și managementului AGE. Acest sumar va fi concis, non-tehnic și va conține:
  - Descrierea clară a obiectivelor, perimetrului și perioadei de testare.
  - Evaluarea generală a posturii de securitate a sistemului, cu un scor de risc agregat.
  - Prezentarea grafică a distribuției vulnerabilităților pe categorii de risc.
  - Lista celor mai critice riscuri identificate și impactul potențial asupra business-ului.
- Partea II - Raport tehnic detaliat: Destinată echipelor tehnice, de dezvoltare și de securitate. Acest raport va fi exhaustiv și va include cel puțin următoarele capitole:
  - Metodologie: Descrierea detaliată a metodologiei, a standardelor urmate și a instrumentelor utilizate.
  - Perimetru: Lista exactă a componentelor (adrese IP, URL-uri, funcționalități) care au fost testate.
  - Descrierea vulnerabilităților: Pentru fiecare vulnerabilitate identificată, se vor furniza:
    - ✓ Denumirea succintă și identificator unic.
    - ✓ Descrierea detaliată a vulnerabilității și a contextului.
    - ✓ Pași exacți pentru reproducerea problemei (PoC - Proof of Concept).
    - ✓ Dovezi concrete (capturi de ecran, fragmente de cod, request/response HTTP).
    - ✓ Clasificarea severității (ex: Critic, Ridicat, Mediu, Scăzut) și scorul CVSS v4.0.

- ✓ Analiza impactului potențial (tehnic și de business).
- ✓ Recomandări de remediere clare, pragmatice și prioritizate.

- Anexă: Lista completă a tuturor testelor efectuate de testare la vulnerabilități, de penetrare, code review, inclusiv teste care nu au relevat vulnerabilități si descrierea rezultatelor obtinute la fiecare test.

5.2.2. Raportul de audit de securitate (GAP Assessment) va avea următoarea structură:

- Sumar executiv (Executive Summary), destinat personalului de decizie și managementului.
- Standardul de referință utilizat și nivelul de verificare solicitat.
- Un sumar grafic al nivelului de conformitate.
- O matrice de conformitate detaliată care, pentru fiecare cerință din standard, va prezenta:
  - ✓ ID-ul și descrierea cerinței.
  - ✓ Statusul conformității: Conform / Neconform / Parțial Conform / N/A.
  - ✓ Observații și dovezi tehnice care justifică statusul.
  - ✓ Recomandări specifice pentru atingerea conformității.

5.3. Integrare cu sistemul de bug-tracking al beneficiarului

Dependent de sistemul testat și nivelul de impact al vulnerabilităților identificate, AGE poate să solicite ca toate deficiențele și vulnerabilitățile identificate să fie înregistrate de către prestator direct în sistemul de management al proiectelor și de urmărire a erorilor (bug-tracking) utilizat de AGE. Astfel, prestatorul va avea responsabilitatea de a monitoriza stadiul remedierilor, inclusiv în sistemul de bug-tracking, și de a raporta progresul în rapoartele periodice, asigurând un ciclu complet de viață pentru fiecare problemă identificată, de la descoperire la validarea închiderii.

6. Cerințe de Calificare

6.1. Cerințe pentru compania ofertantă

- **Experiență profesională:** Experiență demonstrabilă de minim 3 ani în prestarea de servicii de testare a securității cibernetice și asigurare a calității.
- **Portofoliu de proiecte:** Prezentarea a cel puțin 3 proiecte relevante ca anvergură și complexitate (în sectorul public, financiar sau telecomunicații), finalizate cu succes în ultimii 3 ani. Cel puțin un proiect trebuie să fi inclus testarea unei aplicații mobile complexe și cel puțin un proiect trebuie să fi inclus testarea securității unei infrastructuri critice. Se vor prezenta dovezi (extrase de contract, scrisori de recomandare).
- **Certificări de management:** Deținerea unei certificări valabile ISO/IEC 27001 pentru sistemul de management al securității informației este obligatorie. Deținerea altor certificări, precum ISO 9001, ISO 20000 sau altele similare, constituie un avantaj.
- **Legalitatea instrumentelor:** Ofertantul trebuie să prezinte dovada utilizării legale pentru toate instrumentele software comerciale propuse a fi utilizate în cadrul contractului.
- Declarația de independența față de alte misiuni deja desfășurate în cadrul AGE aferente obiectului de achiziție – document original confirmat prin semnătura electronică. În cazul în care Ofertantul este reprezentat printr-o asociere și/sau nominalizează subcontractori, această declarație trebuie să fie depusă de fiecare membru asociat și/sau subcontractor.

6.2. Cerințe pentru personalul cheie

Echipa propusă de ofertant trebuie să includă personal cu expertiză dovedită în domeniile specifice ale contractului. Cerințele minime pentru posturile cheie sunt detaliate în tabelul de mai jos.

Rol	Experiență generală	Experiență specifică	Certificări
Lider de echipă	Minim 5 ani în IT sau managementul serviciilor IT	Minim 5 ani în Project management/Team leadership (proiecte securitate/ software)	CISSP sau CISM sau echivalentul Suplimentar: PMP, ITIL
Membru echipă testare securitate	Minim 5 ani în Securitate IT	Minim 3 ani în Penetration testing și Revizuire cod sursă	OSCP sau CEH Master sau echivalentul Suplimentar: GWAPT, GPEN, OSWE
Expert securitate biometrică	Minim 5 ani în Securitate IT	Minim 3 ani proiecte cu testare sisteme biometrice	OSCP sau CEH Master sau echivalentul Suplementar: Cunoaștere aprofundată a ISO/IEC 30107. Experiență demonstrabilă în planificarea și executarea testelor de tip PAD
Auditor securitate IT	Minim 5 ani în Securitate IT sau Guvernanță IT	Minim 3 ani în audit de securitate IT, evaluări de conformitate sau analize de risc	CISA (Certified Information Systems Auditor) sau ISO/IEC 27001 Lead Auditor sau echivalentul.

7. Cadrul contractual și condiții specifice

- **Durata și tipul contractului:** Se va încheia un singur contract de prestări servicii cu o durată fixă, corespunzătoare termenului de realizare propus de ofertant în oferta sa tehnică și financiară. Serviciile vor fi prestate în baza unui plan agreat, care va detalia perimetrul și obiectivele specifice.
- **Condiții de prestare:** Se acceptă efectuarea unor activități de proiect de la distanță (la sediul Prestatorului) cu condiția că acest lucru nu diminuează nivelul de calitate și securitate al testelor efectuate și livrabilelor care fac obiectul acestui Contract.
- **Confidențialitate:** Prestatorul (compania) și fiecare membru al echipei sale vor semna un Acord/angajament de confidențialitate.
- **Divulgarea coordonată a vulnerabilităților:** Înainte de începerea activităților, părțile vor semna un acord privind divulgarea coordonată a vulnerabilităților, care va stabili procedurile și termenele pentru notificarea, documentarea și remedierea vulnerabilităților identificate, asigurând un proces controlat și responsabil de comunicare a acestora.
- **Responsabilitate:** Prestatorul este pe deplin responsabil pentru orice daună sau întrerupere a serviciilor cauzată sistemelor aflate în testare, care rezultă din neglijența sa, din nerespectarea regulilor de angajament sau din depășirea perimetrului agreat.
- **Proprietate Intelectuală:** Toate livrabilele, rapoartele, scripturile personalizate și orice alt material produs în cadrul acestui contract vor deveni proprietatea intelectuală exclusivă a Agenției de Guvernare Electronică.