Anexa nr.1
la Caietul de sarcini

Specificații tehnice

[Acest tabel va fi completat de către ofertant în coloanele 2, 3, 4, 6, 7, iar de către BNM – în coloanele 1, 5,]

Numărul procedurii de achiziție nr. **ocds-b3wdp1-MD-1774278757998**
Obiectul achiziției: **Servicii cu privire la teste de securitate IT**

Denumirea serviciilor	Denumirea modelului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
1	2	3	4	5	6	7
Lotul: Servicii de evaluare şi de analiză a asigurării calităţii sistemelor (servicii de testare a securităţii sistemului informatic al BNM)						
Servicii de penetrare și evaluare a vulnerabilităților informatice în cadrul sistemului informatic al BNM prin teste specifice de penetrare din exteriorul și interiorul infrastructurii de rețea	Servicii de penetrare și evaluare a vulnerabilităților informatice în cadrul sistemului informatic al BNM prin teste specifice de penetrare din exteriorul și interiorul infrastructurii de rețea	Republica Moldova	SC CONOL-GRUP SRL	Specificația tehnică deplină este indicată în „Cerințele cu privire la serviciile de evaluare şi de analiză a asigurării calităţii sistemelor (servicii de testare a securităţii sistemului informatic al BNM)”	Se propune prestarea serviciilor de penetrare și evaluare a vulnerabilităților informatice în cadrul sistemului informatic al BNM prin teste specifice de penetrare din exteriorul și interiorul infrastructurii de rețea, conform cerințelor Caietului de sarcini (Anexa nr.3), după cum urmează: **1. PERIMETRUL ȘI ABORDAREA TESTĂRII** **1.1. Tipuri de testare propuse:** -teste de penetrare „Black Box”: infrastructura externă expusă în internet, inclusiv aplicațiile web, serviciile de rețea și perimetrele publice ale BNM, fără cunoștințe prealabile despre sisteme (cu excepția URL-urilor/IP-urilor furnizate); -teste de penetrare „Gray Box”: infrastructura interbancară, rețeaua internă BNM, aplicațiile interne, cu cont de utilizator la o stație de lucru cu roluri definite în etapa de pre-evaluare; -evaluarea vulnerabilităților (vulnerability assessment) a întregii infrastructuri de rețea, inclusiv infrastructura wireless; -teste de penetrare a „Sistemului Automatizat de Plăți Interbancare” (SAPI) și „Soluției de Plăți Instant” (IPS): la nivelul unui participant și a unui operator SAPI/IPS; -teste de penetrare a soluției „Active Directory”; -teste de penetrare prin prisma segmentelor de rețea; -teste de penetrare pentru „Sistemul informatic privind stocarea, consolidarea, analiza și monitorizarea datelor financiare ale sectorului de creditare nebancară” (SIREM); -teste de penetrare pentru „Sistemul Automatizat de Stat de evidență a asigurărilor obligatorii de răspundere civilă auto” (RCA Data). **1.2. Abordarea testării va include atât teste automate, cât și teste manuale:** -testele automate realizate cu instrumente profesionale de scanare a vulnerabilităților, aplicațiilor web, codului sursă și infrastructurii de rețea, pentru identificarea sistematică a erorilor de programare și a configurațiilor defectuoase;	-OWASP Testing Guide v4.2 (open web application security project) -OWASP Top 10:2021 -OWASP ASVS v4.0 (application security verification standard) -PTES (penetration testing execution standard) -NIST SP 800-115 (technical guide to information security testing and assessment) -OSSTMM v3 (open source security testing methodology manual) -ISSAF (information systems security assessment framework) -CVSS v3.1 (common vulnerability scoring system) -CWE (common weakness enumeration) -CVE (common vulnerabilities and exposures)

Denumirea serviciilor	Denumirea modelului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
1	2	3	4	5	6	7
					-testele manuale realizate de specialiști cu experiență, vizând aspecte ce necesită intuiția umană, inclusiv erori logice de programare, scenarii complexe de exploatare și validarea/infirmarea rezultatelor testelor automate. **2. ETAPELE PROCEDURII DE EVALUARE ȘI TESTARE** **2.1. Etapa de pre-evaluare (pre-assessment):** -elaborarea planului de testare și a planului de acțiuni (scope of work – SOW); -Definirea scenariilor de atac pentru fiecare componentă din perimetru; -obținerea autorizațiilor necesare de la Beneficiar; -stabilirea activităților, sistemelor incluse, termenelor de realizare și persoanelor responsabile din partea ambelor părți; -definirea regulilor de angajament (rules of engagement), inclusiv ferestrele de testare, procedurile de escaladare și persoanele de contact pentru urgențe; -verificarea conectivității și a accesului la sistemele din perimetru. **2.2. Etapa de evaluare (assessment):** a) recunoaștere și culegere de informații (reconnaissance): -Open Source Intelligence (OSINT): informații din domeniul public; -scanarea activă a sistemelor din SOW; -tehnici de enumerare a serviciilor, utilizatorilor, protocoalelor; -identificarea suprafețelor de atac. b) evaluarea vulnerabilităților și testare de penetrare: Ofertantul va analiza, fără a se limita la, următoarele categorii de vulnerabilități: -injectarea de cod malițios (SQL injection, command injection, LDAP injection, XML injection, OS command injection); -managementul defectuos al procesului de autentificare și al sesiunii de lucru; -cross-site scripting (XSS): reflected, stored și DOM-based; -referențierea directă a obiectelor în mod nesecurizat (IDOR); -erori privind configurația de securitate; -tratarea erorilor în mod nesecurizat și lipsa de protecție a informațiilor sensibile;	-MITRE ATT&CK framework -ISO/IEC 27001:2022 managementul securității informațiilor -ISO/IEC 27002:2022 controale de securitate a informațiilor -PCI DSS v4.0 (ca referință pentru testarea în sectorul financiar) -TIBER-EU (threat intelligence-based ethical red teaming cadru BCE)

Denumirea serviciilor	Denumirea modelului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
1	2	3	4	5	6	7
					-controale ineficiente privind managementul accesului; -cross-site request forgery (CSRF); -utilizarea de componente de sistem cu vulnerabilități cunoscute; -validarea parametrilor de intrare ai aplicațiilor; -comportamentul aplicațiilor/sistemelor la atacuri de tip Denial of Service (DoS, DDoS); -parole inițiale neschimbate pe echipamente; -configurații inițiale neschimbate; -corecții și actualizări de securitate neimplementate; -escaladarea privilegiilor; -woftware cu versiuni vechi ce prezintă vulnerabilități; -buffer overflow; -remote code execution; -directory traversal; -file and Path Disclosure; -configurarea defectuoasă a serverelor. c) în cadrul managementul sesiunii de lucru se vor verifica: -implementarea sesiunii printr-un framework de încredere testat din punct de vedere al securității; -generarea și protecția identificatorilor de sesiune împotriva abuzurilor; -generarea cookie-urilor cu atributele corespunzătoare (httpOnly, secure, sameSite); -procesul de creare și terminare a sesiunii (server/client); -intervalele de inactivitate și sesiunile active multiple; -confidențialitatea informațiilor de autentificare și sesiune; -măsuri adiționale de securitate pentru operațiile administrative sensibile. d) în cadrul configurării de securitate se vor verifica: -versiunile de software ale serverelor, platformelor și componentelor; -existența actualizărilor de securitate; -configurații prestabilite de la producător (utilizatori/parole implicite); -utilizatorii de aplicații și configurația acestora; -metodele și extensiile protocolului HTTP; -informații relevante din header-ul HTTP; -mecanismele de criptare pentru autentificare și transmisie.	

Denumirea serviciilor	Denumirea modelului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
1	2	3	4	5	6	7
					e) în cadrul tratării erorilor și protejarea informațiilor sensibile se vor verifica: -posibilitatea aplicațiilor de a divulga informații sensibile în mesaje de erori; -conținutul mesajelor de eroare din punct de vedere tehnic. f) în cadrul managementul accesului se vor verifica: -procesele de identificare, autentificare și autorizare; -credențialele hard-codate în sisteme; utilizatorii și credențialele stocate în fișiere de configurație în clar; -credențialele transmise în clar; -rolurile de acces, maparea pe drepturi și posibilitatea de ocolire; -metodele HTTP folosite în autentificare. g) în cadrul validării parametrilor de intrare se vor verifica: -filtrarea și validarea datelor din afara sistemelor; -metoda centralizată de validare a datelor; -seturi de caractere corespunzătoare pentru datele de intrare; -codificarea datelor înainte de validare; -validarea tuturor parametrilor, conținutului URL și HTTP; -tipuri de date așteptate, setul de date, lungimea; -măsuri de control pentru caractere cu potențial riscant (< > " ' % ( ) & + \ \' \"). h) testarea securității Wi-Fi: -descoperirea rețelelor Wi-Fi și a punctelor de acces (cunoscute/neautorizate); -identificarea dispozitivelor conectate; -colectarea informațiilor despre protocoale de securitate; -testarea rețelelor criptate cu WEP, WPA-PSK, WPA2-PSK; -impersonare SSID; -atacuri de tip man-in-the-middle (MITM); -monitorizare automată a traficului pentru fluxuri de date sensibile; -testarea sistemelor de backend din rețelele compromise. i) testarea la nivel de rețea: -obținerea informațiilor din domeniul public; -scanarea sistemelor din SOW; -tehnici de enumerare;	

Denumirea serviciilor	Denumirea modelului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
1	2	3	4	5	6	7
					-obținerea accesului neautorizat prin exploatarea vulnerabilităților; -consolidarea accesului; -ștergerea tuturor fișierelor utilizate în cadrul atacului. j) integrarea informațiilor de amenințare (threat intelligence): -soluția de testare va integra capabilitățile de descoperire și remediere a vulnerabilităților cu informații despre aplicațiile malware prezente în infrastructură și ușurința cu care vulnerabilitățile se pot exploata. **2.3. Etapa de post-evaluare (post-assessment):** -elaborarea rapoartelor de analiză cu cele mai bune măsuri și metode de remediere, în funcție de severitate și impact; -acordarea de suport Beneficiarului pentru înțelegerea deplină a problemelor identificate; -recomandarea măsurilor aplicabile pentru remedierea vulnerabilităților; -efectuarea testelor de penetrare repetate (re-testing) la resursele cu probleme identificate, pentru verificarea corectitudinii remedierii. **3. INSTRUMENTE ȘI MIJLOACE UTILIZATE** Se va utiliza un arsenal complex de instrumente profesionale licențiate și open-source, incluzând, dar fără a se limita la: -scanere de vulnerabilități: Nessus Professional / Tenable.io, OpenVAS, Nuclei; -testare aplicații web: Burp Suite Professional, OWASP ZAP, SQLMap, DalFox, Nikto; -testare rețea: Nmap, Masscan, Wireshark, Responder, CrackMapExec/NetExec, Impacket; -testare Active Directory: BloodHound, Rubeus, Mimikatz, Certify, ADRecon; -testare wireless: Aircrack-ng suite, Kismet, WiFite, Bettercap; -frameworks de exploatare: Metasploit Framework, Cobalt Strike; -testare SCADA/ICS (dacă aplicabil): Nmap NSE scripts specializate; -automatizare și raportare: Python, Bash, PowerShell, PlexTrac/Dradis; -reverse engineering și analiza malware: Ghidra, Radare2 (la necesitate). Toate instrumentele vor fi utilizate în mod legal, iar Ofertantul își asumă răspunderea legalității utilizării acestora, prezentând Beneficiarului dovada utilizării legale la solicitare.	

Denumirea serviciilor	Denumirea modelului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
1	2	3	4	5	6	7
					4. LIVRABILE Conform cerințelor Caietului de sarcini, se vor livra: -plan de proiect; -plan de testare; -planul de acțiuni (scope of work – SOW); -rapoarte de test: conținând toate vulnerabilitățile detectate, catalogate în funcție de gravitate; -rapoarte de analiză: cu recomandări de remediere detaliate; -rapoarte de test repetate (re-testing): confirmarea remedierii. Rapoartele vor fi structurate în: a) partea executivă: descrierea pe scurt a vulnerabilităților cu metode grafice; b) partea tehnică, incluzând cel puțin: sumar executiv, obiective și scop, metodologia utilizată, contextul testării, detalii despre rețea și sisteme (IP-uri, porturi, versiuni, SO), prezentarea individuală a fiecărei vulnerabilități (descriere, catalogare, descriere tehnică, analiza severității/probabilității, calcularea riscului, contramăsuri), alte detalii și recomandări, anexa cu lista testelor efectuate. **5. TERMENUL DE PRESTARE** Serviciile vor fi prestate în termen de maximum 100 de zile lucrătoare din data demarării contractului. Termenul pentru remedierea deficiențelor de către Beneficiar (cca 30 zile lucrătoare) nu este inclus în termenul de prestare. **6. ECHIPA DE PROIECT** Echipa de testare va fi compusă din specialiști cu certificări relevante în domeniul securității informatice (OSCP, OSWE, CEH, GPEN, GWAPT sau echivalent), cu experiență demonstrată în proiecte similare de testare a securității în sectorul financiar-bancar.	
Servicii de penetrare și evaluare a vulnerabilităților informatice prestate la solicitare	Servicii de penetrare și evaluare a vulnerabilităților informatice prestate la solicitare (on-demand)	Republica Moldova	SC CONOL-GRUP SRL	**Tip:** Servicii prestate la solicitare presupun servicii de penetrare și evaluare a vulnerabilităților informatice pentru aplicații accesibile din rețeaua internă a BNM cât și expuse în internet, care vor fi descrise detaliat într-o solicitare adresată de către Beneficiar către Prestator. **Cantitate:** Servicii de penetrare și evaluare a vulnerabilităților informatice prestate la solicitare se vor contoriza prin efort de lucru om/ore și nu vor depăși volumul de 200 om/ore pe parcursul a 12 luni din data demarării contractului, contabilizate ulterior pentru fiecare solicitare separat prin acte de prestare a serviciilor detaliate și semnate de ambele părți. Cantitatea specificată este	Se propune următorul model de prestare a serviciilor de penetrare și evaluare a vulnerabilităților informatice la solicitarea Beneficiarului: **1. MODEL DE PRESTARE A SERVICIILOR LA SOLICITARE**	-OWASP Testing Guide v4.2 (open web application security project) -OWASP Top 10:2021 -OWASP ASVS v4.0 (application security verification standard)

Denumirea serviciilor	Denumirea modelului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
1	2	3	4	5	6	7
				indicată orientativ pentru evaluarea financiară, iar executarea contractului va avea loc în funcție de volumul de servicii prestate efectiv conform solicitării Beneficiarului. **<u>Cerințe față de servicii</u>** - În baza solicitării adresate de către Beneficiar, Prestatorul în decurs de 10 zile de la recepționarea solicitării va veni cu o estimare de efort pentru realizarea serviciilor de penetrare și evaluare a vulnerabilităților informatice pentru soluția informatică indicată în solicitare de către Beneficiar inclusiv Planul de testare și acțiuni (SOW – Scope of Work); - Urmare acceptării de către Beneficiar a efortului estimat, Prestatorul în decurs de 30 de zile lucrătoare va presta serviciile de penetrare și evaluare a vulnerabilităților informatice; - Cerințele față de metodologiile, tehnicile și standardele utilizate în evaluarea vulnerabilităților inclusiv etapele procedurii de evaluare și testare vor fi similare celor indicate la pct.2.3-2.4 din ”Cerinţele cu privire la serviciile de evaluare şi de analiză a asigurării calităţii sistemelor (servicii de testare a securitatii sistemului informatic al BNM)” - Prestatorul va prezenta raportul de testare și raportul de analiză conform cerințelor față de livrabile specificate la pct. 2.5. din ”Cerinţele cu privire la serviciile de evaluare şi de analiză a asigurării calităţii sistemelor (servicii de testare a securitatii sistemului informatic al BNM)”. **<u>Notă:</u>** Ofertantul va descrie în oferta sa modelul propus pentru prestarea serviciilor de penetrare și evaluare a vulnerabilităților informatice prestate la solicitare precum și metodele aplicate pentru estimarea prețurilor pentru Beneficiar. Informația inclusă în ofertă trebuie să fie suficientă pentru a aprecia că relația dintre BNM și Ofertantul selectat în procesul de prestare a serviciilor de penetrare și evaluare a vulnerabilităților informatice prestate la solicitare va fi una transparentă și corectă.	**1.1. Procesul de prestare:** -la recepționarea solicitării din partea Beneficiarului, se va analiza cerințele și complexitatea testării solicitate; -în decurs de maximum 10 zile de la recepționare, Beneficiarului i se va prezenta estimarea de efort (în om/ore), planul de testare și planul de acțiuni (scope of work – SOW); -urmare acceptării de către Beneficiar a efortului estimat, Ofertantul va presta serviciile în decurs de maximum 30 de zile lucrătoare; -conform cerințelor din caietul de sarcini, rezultatele vor fi documentate prin raport de testare și raport de analiză. **1.2. Tipul serviciilor:** -servicii de penetrare și evaluare a vulnerabilităților informatice pentru aplicații accesibile din rețeaua internă a BNM și/sau expuse în internet; -testarea poate include orice combinație de: Black Box, Gray Box, testare automată și manuală; -fiecare solicitare va fi descrisă detaliat de către Beneficiar cu indicarea aplicațiilor/sistemelor țintă. **1.2. Volumul serviciilor:** -maximum 200 om/ore pe parcursul a 12 luni din data demarării contractului; -contorizarea se face pentru fiecare solicitare separat, prin acte de prestare a serviciilor detaliate, semnate de ambele părți; -cantitatea este orientativă, executarea contractului fiind în funcție de volumul de servicii prestate efectiv. **2. METODOLOGII, TEHNICI ȘI STANDARDE** Cerințele față de metodologiile, tehnicile și standardele utilizate vor fi similare celor indicate în caietul de sarcini, și anume: -abordare conform OWASP Testing Guide v4.2, PTES, NIST SP 800-115, OSSTMM v3; -testare automată și manuală cu instrumente profesionale licențiate; -analiza vulnerabilităților conform clasificării CVSS v3.1 și CWE; -scenarii de atac adaptate specificului aplicației/sistemului testat. **3. LIVRABILE PER SOLICITARE** Pentru fiecare solicitare, se va prezenta:	-PTES (penetration testing execution standard) -NIST SP 800-115 (technical guide to information security testing and assessment) -OSSTMM v3 (open source security testing methodology manual) -ISSAF (information systems security assessment framework) -CVSS v3.1 (common vulnerability scoring system) -CWE (common weakness enumeration) -CVE (common vulnerabilities and exposures) -MITRE ATT&CK framework -ISO/IEC 27001:2022 managementul securității informațiilor -ISO/IEC 27002:2022 controale de securitate a informațiilor -PCI DSS v4.0 (ca referință pentru testarea în sectorul financiar) -TIBER-EU (threat intelligence-based

Denumirea serviciilor	Denumirea modelului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
1	2	3	4	5	6	7
					-planul de testare și SOW (înainte de începerea testării); -raportul de testare cu toate vulnerabilitățile detectate, catalogate în funcție de gravitate; -raportul de analiză cu recomandări de remediere detaliate; -actul de prestare a serviciilor cu detaliere om/ore. **4. METODA DE ESTIMARE A PREȚURILOR** Estimarea efortului se va face pe baza următorilor factori: -complexitatea și dimensiunea aplicației/sistemului testat (număr de funcționalități, endpoint-uri, pagini); -tipul testării solicitate (Black Box / Gray Box); -cerințe speciale de conformitate sau reglementare; -necesitatea testării repetate (re-testing) post-remediere; -prețul per om/oră este fix, conform ofertei financiare, asigurând transparența și corectitudinea relației contractuale; -detaliere transparentă a efortului estimat pe activități/categorii de teste, permițând Beneficiarului o evaluare clară a costurilor. **5. ASIGURAREA CALITĂȚII** -fiecare livrabil va trece printr-un proces intern de review de calitate; -rapoartele vor respecta aceeași structură și cerințe ca pentru serviciul de bază (parte executivă + parte tehnică); -se va acorda suport post-livrare pentru clarificări și înțelegerea deplină a constatărilor.	ethical red teaming cadru BCE)

Semnat: Digitally signed by Țepilovan Dumitru
Date: 2026.04.10 15:01:42 EEST
Reason: MoldSign Signature
Location: Moldova
MOLDOVA EUROPEANĂ

în calitate de: **Administrator**

Ofertantul: **SC „CONOL-GRUP” SRL,** adresa: **str. Lev Tolstoi nr. 74, of. 190, MD-2012, mun. Chișinău**