OFERTA TEHNICA

<u>**Cuprins**</u>

Numele Ofertantului:

Deloitte Consultanta SRL

1. Rezumat

Acest exercitiu de testare de penetrare bazata pe principiile framework-ului TIBER-EU, va permite BNM sa isi maturizeze rezilienta cibernetica impotriva atacatorilor malitiosi, sa isi evalueze capacitatea infrastructurii IT, capacitatea personalului BNM de a raspunde la un atac cibernetic si va scadea nivelul de risk rezultat din exploatarea resurselor IT.

Astfel, BNM isi va putea executa sarcinile sale importante ca Banca Centrala, cum ar fi elaborarea si aplicarea politicii monetare si de schimb valutar, autorizarea, reglementarea si supravegherea institutiilor de credit, promovarea si monitorizarea bunei functionari a sistemelor de plati, contribuind in general la asigurarea stabilitatii financiare a Moldovei.

Suntem recunoscători pentru oportunitatea de a vă oferi serviciile noastre și suntem mândri să arătăm de ce suntem cei mai potriviți pentru solicitarea dvs.

Aducem clienților experiența și expertiza vastă in executarea a numeroase exerciții de teste de penetrare, in special in aria financiar-bancara. Credem cu tarie ca un astfel de exercitiu, precum cel solicitat, care urmeaza metodologia TIBER-EU, necesita un grad detaliat de intelegere a muncii ce urmeaza a fi prestata, reguli clare de comunicare, de management al riscului si de management de proiect. Echipa Deloitte are experienta in executarea testelor de pentrare pentru Banca Nationala a Romaniei, avand experienta relevanta in domeniul in care activati.

In cele ce urmeaza veti observa impartirea proiectului in doua etape majore: „Etapa I - Threat Intelligence” si „Etapa II – Testare infrastructuri”, etape care vor permite BNM să experimenteze un atac cibernetic sofisticat, controlat.

„Etapa I – Threat Intelligence” este prima si cea mai importanta etapa deoarece seteaza tonul intregului proiect si al etapelor urmatoare si realizarea scenariilor de testare intruziva.

Scenariile de testare bazate pe Threat intelligence care imita adversari cibernetici din viata reala sunt esentiale pentru succesul activittilor de testare de tip TIBER-EU. Componenta de Threat Intelligence ofera o imagine detaliata a suprafetei de atac a entitatii vizate si ajuta la realizarea de scenarii de atac realiste si actionabile. Astfel de scenarii de testare doresc sa imite tacticile, tehnicile si procedurile atacatorilor potentiali si vor ajuta la licrarea unei simulari realiste.

Raportul ce rezulta din Etapa I – Threat Intelligence” va fi folosit in finalul acestei etape si in cadrul „Etapei II – Testare infrastructuri” de catre echipa de experti pentru a crea scenarii realiste de atac si pentru a executa atacurile respective, ajutand echipa de experti sa furnizeze o evaluare practica a capacitatii de protectie, detectie si raspuns a lui BNM.

Legat de managementul riscului, exista elemente de risc inerente asociate cu un test TIBER-EU pentru toate părțile, datorită criticității sistemelor de productie, a oamenilor și a proceselor implicate în teste. Posibilitatea de a provoca un incident evidențiază necesitatea unui management activ și robust al riscurilor. În conformitate cu riscul potențial al testului, acordam o prioritate ridicată stabilirii unor controale solide de gestionare a riscurilor pe întregul proces al testului, pentru a se asigura că acesta este realizat în mod controlat.

Pentru a asigura un test controlat și sigur, rolurile și responsabilitățile tuturor părților interesate trebuie să fie clar stabilite și înțelese. Cu toate acestea, este la fel de critic că testul este realizat fără cunoștința prealabilă a entității (cu excepția unui număr mic de membri ai personalului) pentru a obține o imagine reală a capacității de protecție, detecție și răspuns a entității.

În plus, pentru a ne asigura că testul este realizat la cele mai înalte standarde, echipa pe care o punem la dispozitia acestui proiect este una cu o vasta experienta si care detine certificari relevante multiple, inluzand cele solicitate in cadrul Caietului de Sarcini.

Anticipand eventuale modificari in cadrul activitatilor din acest proiect, neputand cunoaste la acest moment modificarile, abordarea noastra generala pentru acest proiect pentru a veni in intampinarea BNM si pentru a putea livra beneficiile asteptate si solicitate va fi una de tip „Agile” in care vom fi flexibili in structura managementului de proiect, tinand cont de nevoile imediate ale proiectului, evaluarea activitatilor de proiect si eventual adaugarea de noi activitati, in functie de necesitati. De asemenea, avand in vedere echipa exinsa pe care o includem in cadrul acestui proiect ne va permite sa desfasuram anumite activitati in paralel, cum ar fi testarea celor doua infrastructuri BNM cat si cea interbancara.

In fiecare saptamana se va organiza o intalnire interna Deloitte in care participa toti membrii echipei. In cadrul acestei intalniri se prezinta rezultatele parcurgerii activitatilor anterioare, activitatile ce urmeaza a fi parcurse in urmatoarea saptamana dar si eventualele limitari.
La fiecare 2 saptamani se va organiza cate o sedinta comuna de lucru la care participa reprezentantii Deloitte si persoanele desemnate din partea BNM. Aceste intalniri au rolul de a armoniza eforturile comune de livrare a proiectului in cauza.
In cazul in care informatii noi apar in timpul derularii activitatilor proiectului, informatii de natura care sa afecteze semnificativ parametrii si timpii de livrare a proiectului, acestea vor fi prezentate cu celeritate de catre expertii tehnici atat managerului de proiect Deloitte, urmand ca mai apoi managerul de proiect Deloitte sa aplice eventuale corectii si, eventual, anuntarea persoanelor responsabile din partea BNM.

Intreg proiectul va fi supravegheat de catre un Partener responsabil cu coordonarea si asigurarea calitatii a acestui proiect (back-stopping) care face parte din echipa de management al companiei. Partenerul de proiect revizuiește toate livrabilele și este ultimul responsabil pentru conformitatea livrabilelor cu cerințele contractuale

2. Abordarea și metodologia propuse pentru prestarea serviciilor, datele de intrare și datele de ieșire pentru activitățile din cadrul Contractului

2.1. Abordarea propusă

Intreg proiectul va fi gestionat folosind o abordare bazata pe Management de Proiect. Desi in general ciclul de viata al acestui proiect va fi unul liniar (traditionalul model „waterfall”), exista etape unde abordarea de tip „agile” va fi adoptata pentru a face fata cerintelor Caietului de Sarcini si pentru a optimiza timpul de desfasurare al acestui proiect (de exemplu, anumiti pasi din cadrul Etapei II, Testare infrastructura BNM si interbancara). De asemenea, pe masura ce avanseaza proiectul, conform abordarii de tip „agile” vom acorda o atentie sporita obiectivelor imediate si constrangerilor ale proiectului.

2.2. Metodologia propusă

i. Metodologia pentru realizarea activitatilor în contextul responsabilităților și atribuțiilor stabilite în Caietul de Sarcini, prin prezentarea activităților și a modalității efective de realizare a acestora și a rezultatului fiecărei activități desfășurate pentru a demonstra atingerea, în cadrul duratei de realizare a serviciilor, a obiectivelor asociate Contractului, utilizând formatul următor:

Activitate	Modalitatea efectivă de realizare a activității (metoda, procedura, tehnica, procedeul, după caz)	Date de intrare utilizate pentru realizarea activității (resurse folosite; ex. software, resurse umane, informații etc.)	Date de ieșire - Rezultate obținute la finalul activității (rezultate intermediare și/sau finale)	Durata activității	Informații suplimentare relevante în legătură cu activitatea, acolo unde este aplicabil
Etapa I - Threat Intelligence (TI)					
Kick-Off (Definire si aprobare Document de Autorizare)	○ Definire detaliata a obiectivelor de testare; ○ Stabilire impreuna cu clientul a datelor de livrare si a recurentei intalnirilor de status-update (propunem 1 intalnire la un interval de 2 saptamani) ○ Identificarea sistemelor tinta si a resurselor (inclusiv datele confidentiale); ○ Identificarea actiunilor permise (citire, modificare, stergere, executare cod de exploatare vulnerabilitati); ○ Identificarea si selectarea resurselor (tehnice si personal);	**Resurse umane** ○ Manager Proiect – expert cheie 1 ○ Expert cheie 2 ○ Expert cheie 3 ○ Reprezentantii BNM alocati pentru acest proiect	Documentul de autorizare	2 zile lucratoare - Sapt 1 a proiectului	

	○ Revizuire draft a planului de testare; ○ Colectarea informatiilor (ex: documentatie sistem, politici specifice de securitate IT&C); ○ Analiza riscurilor aferente desfasurarii proiectului si includerea acestora in Documentul de Autorizare ○ Realizare document aplicabilitate si planul de testare (Documentul de autorizare) Aprobare client a Documentului de Autorizare	○ Personal backstopping – Partenerul responsabil cu Asigurarea Calitatii **Informatii** ○ BNM va trebui sa furnizeze documentatie sistem, politici specifice de securitate IT&C si alte documente relevante			
Etapa tehnica TI (OSINT - Open Source Intelligence)	○ Realizarea a DNS lookups si incercarea de a face zonetransfer de la domeniul client initial folosind Subbrute si DNSEnum ○ Efectuarea de cautari manuale WHOIS/DNS folosind Dig, NSLookup si WHOIS ○ Plasarea tuturor domeniilor descoperite in excelul corespunsator (Domenii). Pentru fiecare domeniu vom valida sub-domeniul, IP-ul si proprietarul respectiv ○ Verificarea oricaror intervale legate de clienti sau numere ASN in registrii de Internet (Afrinic, Apnic, Ari, Lacnic si Ripe) ○ Documentarea tuturor intervalelor in excelul "Domenii" ○ Documentarea de capturi de ecran si a altor dovezi relevante in tab-ul Regional Internet Registry ○ Rularea a Discover (Extern, Pasiv) si a theHarvester pentru a gasi sub-domenii aditionale, angajati, adrese de e-mail si documente ○ Utilizarea Censys si Shodan pentru a descoperi IP-uri aditionale, informatii legate de scanarea porturilor si ASN-uri (Autonomous System Number) ○ Utilizarea DNSDumpster pentru a descoperi subdomenii aditionale si ASN-uri ○ Documentarea tuturor IP-urilor, intervalelor si a ASN-urilor gasite in excelul "Domenii" ○ Documentarea de capturi de ecran si a altor dovezi relevante in tab-ul Shodan si Censys ○ Efectuarea activitatii de "liveness" si initial NMAP pentru descoperirea de hast-uri active	**Resurse umane** ○ Manager Proiect – expert cheie ○ Expert cheie 2 ○ Expert cheie 3 **Resurse tehnice / tool-uri** ○ DNS Lookup ○ Subbrute ○ DNSEnum ○ Dig ○ NSLookup ○ WHOIS ○ Excel ○ Afinic ○ Apnic ○ Ari ○ Lacnic ○ Ripe ○ Discover ○ theHarvester ○ Censys ○ Shodan ○ DNSDumpster	Obtinerea de informatii necesare etapei the colectare informatii Threat Intelligence	5 zile lucratoare - Sapt 1, 2 ale proiectului	

	○ Documentarea tuturor hoast-urilor in excelul "Domenii" pentru a obtine o lista interesanta de IP-uri active de clienti pentru a fi testate ○ Utilizarea motoarelor de cautare si alte unelte pentru a cauta pagini oficiale/neoficiale ale clientului (blog-uri, site-uri de stiri sau marketing), informatii scurse (credentiale, liste de spam, etc) sau pagini de login (VPN, remote desktop, mail, forumuri) ○ Verificarea "robots.txt" a fiecarui domeniu identificat pentru directoare interesante ○ Documentarea website-urilor gasite in excelul "Domenii" ○ Crearea si popularea unei noi pagini in sectiunea "Informatii scurse" cu orice tip de informatie relevanta scursa (leak-uita) ○ Crearea si popularea unei noi pagini sectiunea "Pagini de login" cu capturi de ecran si pagini de login ○ Asigurarea ca am analizat toate output-urile uneltelor utilizate si ca am adaugat un strat de "intelligence" pentru a avea un output cat mai coerent, complet si util pentru toata echipa	○ NMAP ○ Robots.txt			
Scanare de vulnerabilitati	○ Scanare de vulnerabilitati a aplicatiilor si a serviciilor conexe de vulnerabilitati, in modul neautentificat.	**Resurse umane** ○ Manager Proiect – expert cheie ○ Expert cheie 3 ○ Expert cheie 4 **Resurse tehnice / tool-uri** ○ Nessus ○ OpenVAS ○ NeXpose	Obtinerea de informatii necesare etapei the colectare informatii Threat Intelligence.	3 zile lucratoare - Sapt 2 a proiectului	
Raportare Threat Intelligence (TI)	○ Agregare informatii obtinute in cadrul Etapei I - TI ○ Validare constatari, eliminare alarme false (false positives) ○ Interpretare informatii disponibile despre BNM ○ Imbogatirea informatiilor obtinute cu detalii din alte surse externe (ex: Shodan, Censys.io, DNSSpy.io, etc) ○ Analiza vectorilor de atac si modul de exploatare a acestora	**Resurse umane** ○ Manager Proiect – expert cheie ○ Expert cheie 2 ○ Expert cheie 3	○ Agregarea informatiilor obtinute in cadrul etapei de Threat	1 zile lucratoare - Sapt 3 a proiectului	

	○ Creare lista aplicatii web expuse in internet conform info din Etapa I - TI ○ Confirmare lista aplicatii web expuse in internet impreuna cu reprezentantii BNM ○ Dezvoltare scenarii de atac pentru testele de Red Teaming (inclusiv Social Engineering) ○ Validare impreuna cu BNM a scenariilor de Red Teaming si includerea acestora in raport TI ○ Livrare raport Threat Intelligence	**Resurse tehnice / tool-uri** ○ Nessus ○ OpenVAS ○ NeXpose	Intelligence si interpretarea lor ○ Realizarea de scenarii de atac ○ Raport Threat Intelligence		
Etapa II – Testare Infrastructura					
Testare infrastructura BNM (extern si intern)					
Exploatarea tactica a retelei (Tactical Network Exploitation-TNE)	○ Parcurgerea motodologiei proprii a TNE si conectarea la reteaua clientului ○ Identificarea celor mai interesante / exploatabile / usoare cai de atac al mediului tinta bazandu-ne pe rezultatul NMAP (ex: interfete de management/sensibile cum ar fi Apache, Tomcat, IIS, JBOSS, NETBIOS, RDP) ○ Documentarea ariilor de interes in locurile corespunzatoare ○ Interpretarea rezultatelor oferite de diverte tool-uri pentru a capata acces sporit in retea ○ Daca rezultatul oferit de responder este un hash NetNTLM, atunci prima data este executat un atac de spargere a parolei ○ Imbunatatirea rezultatelor cu observatii privind grupurile din care utilizatorii capturati fac parte ○ Pe baza rezultatelor oferite de responder identificarea celor mai interesante conturi (acei useri ce fac parte din anumite grupuri privilegiate) ○ Documentarea tuturor conturilor identificate. Din cauza datelor sensibile (date cu caracter personal - nume de utilizator, parole, etc) acestea nu se vor documenta in sistemele Deloitte ○ Pe baza informatiilor obtinute in prima etapa de recunoastere, vom accesa sistemele de interes accesand direct serviciile sau vom efectua logare utilizand credentialele capturate sau primite. Exemple: servere FTP, wiki, Sharepoint, etc	**Resurse umane** ○ Expert cheie 2 ○ Expert cheie 3 ○ Expert cheie 4 ○ Expert cheie 5 **Resurse tehnice / tool-uri** ○ NMAP ○ Cobalt Strike ○ Responder ○ Bettercap ○ CEWL ○ Impact ○ NTLMrelayx ○ Proxychains ○ Hashcat ○ Socat ○ Powershell ○ Metasploit ○ SMBmap	Obtinere acces in infrastructura clientului	3 zile lucratoare - Sapt 3 a proiectului	

	○ Acolo unde este necesar, se vor folosi exploit-uri SIGURE (se va confirma cu expertul asignat si cu clientul inainte) pentru a obtine acces in sistemele de interes ○ Descoperirea informatiilor relevante, cum ar fi mai multe detalii despre tinta sau informatii ce pot fi folosite in viitoare atacuri. ○ Actualizarea corespunzatoare a listelor de conturi si Info Gathering si documentarea informatiilor care necesita analiza aditionala	○ Eyewithness ○ Various internally developed scripts			
Miscare laterala	○ Obtinerea drepturilor de administrator local si/sau descoperirea unor metode de obtinere a drepturilor de administrator ○ Indentificarea posibilelor servicii interesante, procese active, căi către fișiere, executabile ○ Actualizarea corespunzatoare a listelor de conturi si Info Gathering si documentarea informatiilor care necesita analiza aditionala ○ Avand in vedere noile privilegii obtinute, se va realiza o reluare a pasilor aferenti recunoasterii (scanare noua a sistemului cu privilegiile noi) ○ Obtinerea accesului intr-un nou sistem, folosind deja sistemul compromis ○ Folosirea de tool-uri sau tehnici manuale pentru a identifica alte sisteme, conturi de utilizatori, parole, capata acces in alte sisteme, si/sau escalarea privilegiilor ○ Actualizarea corespunzatoare a listelor de conturi si Info Gathering si documentarea informatiilor care necesita analiza aditionala	**Resurse umane** ○ Expert chee 2 ○ Expert cheie 3 ○ Expert cheie 4 ○ Expert cheie 5 **Resurse tehnice / tool-uri** ○ NMAP ○ Cobalt Strike ○ Responder ○ Bettercap ○ CEWL ○ Impact ○ NTLMrelayx ○ Proxychains ○ Hashcat ○ Socat ○ Powershell ○ Metasploit ○ SMBmap ○ Eyewithness ○ Various internally developed scripts	Extinderea accesului in infrastructura clientului	3 zile lucratoare - Sapt 3, 4 ale proiectului	

Actiuni finale de testare	○ Utilizarea unei abordari non-stealth (ex: Nessus), se vor identifica sisteme interesante si se va face "galagie" pentru a verifica masurile de monitorizare a securitatii utilizate de catre Client ○ Documentarea activitatilor in sectiunea "Indicatori de compromis" ○ Documentarea rezultatelor si finding-urilor si propunerea de recomandari ○ Asigurarea ca nu exista informatii confidentiale sau sensibile care sa fie notate in evidente si observatii	**Resurse umane** ○ Expert cheie 3 ○ Expert cheie 4 **Resurse tehnice / tool-uri** ○ Nessus	Corelare cu activitatea de Blue Team, testarea masurilor de detectie a clientului	1 zile lucratoare - Sapt 4 a proiectului	
Wrap-up	○ Incarcarea evidentelor in sistemele corespunzatoare ○ Incarcarea playbook-ului in sistemele corespunzzatoare ○ Incarcarea programului de lucru in sistemele corespunzatoare ○ Crearea unei liste de utilizatori (conturi FARA parole) si hostnames (hoast-uri si log-uri de Cobalt Strike) care au fost compromise in timpul testarii ○ Trimiterea fisierelor catre Client intr-un mod securizat	**Resurse umane** ○ Expert cheie 2	Documentarea evidentelor si informatiilor rezultate din cadrul acestei activitati	1 zi lucratoare - Sapt 4 a proiectului	
Testare infrastructura interbancara					
Exploatarea tactica a retelei (Tactical Network Exploitation-TNE)	○ Parcurgerea motodologiei proprii a TNE si conectarea la reteaua clientului ○ Identificarea celor mai interesante / exploatabile / usoare cai de atac al mediului tinta bazandu-ne pe rezultatul NMAP (ex: interfete de management/sensibile cum ar fi Apache, Tomcat, IIS, JBOSS, NETBIOS, RDP) ○ Documentarea ariilor de interes in locurile corespunzatoare ○ Interpretarea rezultatelor oferite de diverte tool-uri pentru a capata acces sporit in retea ○ Daca rezultatul oferit de responder este un hash NetNTLM, atunci prima data este executat un atac de spargere a parolei ○ Imbunatatirea rezultatelor cu observatii privind grupurile din care utilizatorii capturati fac parte ○ Pe baza rezultatelor oferite de responder identificarea celor mai interesante conturi (acei useri ce fac parte din anumite grupuri privilegiate) ○ Documentarea tuturor conturilor identificate. Din cauza datelor sensibile (date cu caracter personal - nume de utilizator, parole, etc) acestea nu se vor documenta in sistemele Deloitte ○ Pe baza informatiilor obtinute in prima etapa de recunoastere, vom accesa sistemele de interes accesand direct serviciile sau vom efectua logare	**Resurse umane** ○ Expert cheie 2 ○ Expert cheie 3 ○ Expert cheie 4 ○ Expert cheie 5 **Resurse tehnice / tool-uri** ○ NMAP ○ Cobalt Strike ○ Responder ○ Bettercap ○ CEWL ○ Impact ○ NTLMrelayx ○ Proxychains ○ Hashcat	Obtinere acces in infrastructura clientului	3 zile lucratoare - Sapt 4 ale proiectului	

	utilizand credentialele capturate sau primite. Exemple: servere FTP, wiki, Sharepoint, etc ○ Acolo unde este necesar, se vor folosi exploit-uri SIGURE (se va confirma cu expertul asignat si cu clientul inainte) pentru a obtine acces in sistemele de interes ○ Descoperirea informatiilor relevante, cum ar fi mai multe detalii despre tinta sau informatii ce pot fi folosite in viitoare atacuri. ○ Actualizarea corespunzatoare a listelor de conturi si Info Gathering si documentarea informatiilor care necesita analiza aditionala	○ Socat ○ Powershell ○ Metasploit ○ SMBmap ○ Eyewithness ○ Various internally developed scripts			
Miscare laterala	○ Obtinerea drepturilor de administrator local si/sau descoperirea unor metode de obtinere a drepturilor de administrator ○ Indentificarea posibilelor servicii interesante, procese active, căi către fișiere, executabile ○ Actualizarea corespunzatoare a listelor de conturi si Info Gathering si documentarea informatiilor care necesita analiza aditionala ○ Avand in vedere noile privilegii obtinute, se va realiza o reluare a pasilor aferenti recunoasterii (scanare noua a sistemului cu privilegiile noi) ○ Obtinerea accesului intr-un nou sistem, folosind deja sistemul compromis ○ Folosirea de tool-uri sau tehnici manuale pentru a identifica alte sisteme, conturi de utilizatori, parole, capata acces in alte sisteme, si/sau escalarea privilegiilor ○ Actualizarea corespunzatoare a listelor de conturi si Info Gathering si documentarea informatiilor care necesita analiza aditionala	**Resurse umane** ○ Expert cheie 2 ○ Expert cheie 3 ○ Expert cheie 4 ○ Expert cheie 5 **Resurse tehnice / tool-uri** ○ NMAP ○ Cobalt Strike ○ Responder ○ Bettercap ○ CEWL ○ Impact ○ NTLMrelayx ○ Proxychains ○ Hashcat ○ Socat ○ Powershell ○ Metasploit ○ SMBmap	Extinderea accesului in infrastructura clientului	3 zile lucratoare - Sapt 5 a proiectului	

		○ Eyewithness ○ Various internally developed scripts			
Actiuni finale de testare	○ Utilizarea unei abordari non-stealth (ex: Nessus), se vor identifica sisteme interesante si se va face "galagie" pentru a verifica masurile de monitorizare a securitatii utilizate de catre Client ○ Documentarea activitatilor in sectiunea "Indicatori de compromis" ○ Documentarea rezultatelor si finding-urilor si propunerea de recomandari ○ Asigurarea ca nu exista informatii confidentiale sau sensibile care sa fie notate in evidente si observatii	**Resurse umane** ○ Expert cheie 3 ○ Expert cheie 4 **Resurse tehnice / tool-uri** ○ Nessus	Corelare cu activitatea de Blue Team, testarea masurilor de detectie a clientului	1 zile lucratoare - Sapt 5 a proiectului	
Wrap-up	○ Incarcarea evidentelor in sistemele corespunzatoare ○ Incarcarea playbook-ului in sistemele corespunzzatoare ○ Incarcarea programului de lucru in sistemele corespunzatoare ○ Crearea unei liste de utilizatori (conturi FARA parole) si hostnames (hoast-uri si log-uri de Cobalt Strike) care au fost compromise in timpul testarii ○ Trimiterea fisierelor catre Client intr-un mod securizat	**Resurse umane** ○ Expert cheie 2	Documentarea evidentelor si informatiilor rezultate din cadrul acestei activitati	1 zi lucratoare - Sapt 5 a proiectului	
Activitati Blue Team					
Activitati de sprijin Blue Team	○ Anuntarea personalului desemnat din partea Clientului, parte din echipa de securitate, despe teste le penetrare efectuate ○ Declararea posibilelor incidente de securitate catre echipa desemnata din partea Clientului ○ Sprijinirea locala a echipei de securitate a Clientului pentru a raspunde la incidente ○ Prezentarea atacului catre echipa de securitate desemnata din partea clientului ○ Punerea la dispozitia echipei de securitate desemnata din partea Clientului a Indicatorilor de compromis ale atacurilor ○ Comunicare si suport privind raspunsul la incidente pe intreaga perioada de desfasurare a testeleor de penetrare	**Resurse umane** ○ Manager Proiect – expert cheie ○ Expert cheie 2 ○ Expert cheie 4	Sprijinirea echipei de Blue Team a clinetului in imbunatatirea capacitatilor de detectie si raspuns.	20 zile lucratoare - Sapt 3 - 5, ale proiectului	Pe intreaga perioada a testarii efective.
Inginerie sociala (Social Engineering)					

Campanie ROGUE WIFI	○ Creare scenariu rogue wi-fi aplicabil si construire echipamentelor hardware ○ Crearea unei configuratii software specifice pentru executarea scenariului ○ Verificarea cu clientul a detaliilor scenariului propus ○ Lansare campanie rogue wi-fi si mentinerea centrului de comanda si control pe o perioada de timp agreata cu clientul ○ Dupa expirarea perioadei de timp agreata, se vor exporta rezultatele si se vor dezactiva dispozitiv rogue wi-fi si centru de comanda si control ○ Anonimizarea rezultatelor ○ Emiterea observatiilor echipei implicate si adaugarea acestora in raport	**Resurse umane** ○ Expert cheie 2 ○ Expert cheie 3 **Resurse tehnice / tool-uri** ○ Proprietary scripts	○ Scenariu rogue wi-fi ○ Rezultate scenariu Rogue wi-fi	2 zile lucratoare - Sapt 5 a proiectului	
Wrap-up	○ Incarcarea evidentelor in sistemele corespunzatoare ○ Incarcarea playbook-ului in sistemele corespunzatoare ○ Incarcarea programului de lucru in sistemele corespunzatoare	**Resurse umane** ○ Manager Proiect – expert cheie	Documentarea evidentelor si informatiilor rezultate din cadrul acestei activitati	1 zi lucratoare - Sapt 5 a proiectului	
Raport intermediar					
Raport intermediar	○ Agregarea constatarilor din cadrul etapei II intr-un raport intermediar care include IOCs, findings and propunere recomandari de remediere pentru eventualele vulnerabilitati cu grad mare de criticitate. ○ Livrarea si prezentarea raportului intermediar, inclusiv finding-uri complete, catre echipa clientului	**Resurse umane** ○ Manager Proiect – expert cheie ○ Expert cheie 2 ○ Expert cheie 3 ○ Expert cheie 4 ○ Expert cheie 5 ○ Personal backstopping – Partenerul responsabil cu Asigurarea Calitatii ○ Reprezentantii BNM alocati pentru acest proiect	○ Raport de testare intermediar ○ Lista vulnerabilitati critice ○ Recomandari remediere vulnerabilitati critice	2 zile lucratoare - Sapt 6 a proiectului	
Remediere vulnerabilitati critice de catre Client	○ Reconfigurarea controalelor afectate de vulnerabilitati critice de catre Client	**Resurse umane** ○ Reprezentantii BNM alocati pentru acest proiect		Pana la 4 zile lucratoare -	Va depinde in functie de numarul de vulnerabilitati critice

				Sapt 6 a proiectului	descoperite si de timpul care ii este necesar clientului pentru remedierea acestora. Aceasta fereastra de remediere va fi stabilita de comun acord cu clientul.
Re-testare					
Re-testare infrastructura BNM	○ Dupa reconfigurarea controalelor afectate de vulnerabilitatile critice, echipa Deloitte va efectua retestarea vulnerabilitatilor critice identificate anterior in cadrul infrastructurii BNM.	**Resurse umane** ○ Manager Proiect – expert cheie ○ Expert cheie 2 ○ Expert cheie 3	○	2 zile lucratoare - Sapt 7 a proiectului	
Re-testare infrastructura interbancara	○ Dupa reconfigurarea controalelor afectate de vulnerabilitatile critice, echipa Deloitte va efectua retestarea vulnerabilitatilor critice identificate anterior in cadrul infrastructurii interbancare.	**Resurse umane** ○ Manager Proiect – expert cheie ○ Expert chee 2 ○ Expert cheie 3 ○ Expert cheie 4 ○ Expert cheie 5	○	2 zile lucratoare - Sapt 7 a proiectului	
Raport final					
Raport final	○ Agregarea constatarilor din cadrul etapei II intr-un raport final care include IOCs, findings and propunere recomandari de remediere pentru eventualele vulnerabilitati cu grad mare de criticitate. ○ Livrarea si prezentarea raportului intermediar, inclusiv finding-uri complete, catre echipa clientului	**Resurse umane** ○ Manager Proiect – expert cheie ○ Expert cheie 2 ○ Expert cheie 3 ○ Expert cheie 4	○ Raport de testare final	2 zile lucratoare - Sapt 7 a proiectului	

		○ Expert cheie 5 ○ Personal backstopping – Partenerul responsabil cu Asigurarea Calitatii			
Update proiect (intalniri de coordonare, monitorizare si control)					
Update proiect (Deloitte Intern)	*De coordonare:* a. Organizarea întâlnirii de demarare a activităților în Contract, pentru obținerea asigurării că toate partile implicate au aceeași perspectivă asupra activităților și rezultatelor din Contract b. Coordonarea activitatilor din Contract. *De monitorizare:* *a.* Măsurarea progresului activităților din Contract prin raportare la Contract. *De control:* a. Identificarea acțiunilor corective pentru abordarea abaterilor de la Contract constatate și care se referă la dimensiuni precum abordarea și metodologia utilizată în realizarea serviciilor, nivelul calitativ, cost, timp etc.	**Resurse umane** ○ Manager Proiect – expert cheie ○ Expert cheie 2 ○ Expert cheie 3 ○ Expert cheie 4 ○ Expert cheie 5	○ Minute sedinte	6 zile lucratoare - Sapt 1, 2, 3, 4, 5, 6, ale proiectului	Pe intreaga perioada de desfasurare efectiva a proiectului, o data pe saptamana.
Update proiect (Deloitte + BNM)	*De coordonare:* a. Organizarea întâlnirii de demarare a activităților în Contract, pentru obținerea asigurării că Autoritatea Contractantă și Contractantul au aceeași perspectivă asupra activităților și rezultatelor din Contract b. Coordonarea activitatilor din Contract *De monitorizare:* *a.* Măsurarea progresului activităților din Contract prin raportare la Contract. *De control:* a. Identificarea acțiunilor corective pentru abordarea abaterilor de la Contract constatate de comun acord în cadrul întâlnirilor dintre Deloitte și Client, și care se referă la dimensiuni precum abordarea și metodologia utilizată în realizarea serviciilor, nivelul calitativ, cost, timp etc.	**Resurse umane** ○ Manager Proiect – expert cheie ○ Reprezentantii BNM alocati pentru acest proiect	○ Minute sedinte	6 zile lucratoare - Sapt 1, 2,3,4,5,6 ale proiectului	Pe intreaga perioada de desfasurare efectiva a proiectului, o data la doua saptamani.

Tool-uri folosite

Nume	Descriere	Versiune
Kali Linux	Various tools from Kali Linux distribution	Rolling release 2020.2
Nessus Vulnerability Scanner	Network and Vulnerability Scanner	Version 6.2.7
Burp Suite Professional	Intercepting Proxy for Web Vulnerability Assessment	Version 1.7
Nmap Port Scanner	Network port scanner	Version 7
Nikto	Open Source web server vulnerability scanner	Version 2.1.6
Foxy-proxy	Firefox proxy manager	Version 6.2
DirBuster	Tool to brute force directories and files names	1.0-RC1

Deloitte detine licentele si drepturile de utilizare pentru instrumentele de lucru mentionate mai sus.

ii. Metodologia utilizată pentru obținerea asigurării că activitățile ce urmează a fi realizate și rezultatele ce urmează a fi obținute îndeplinesc cerințele din Caietul de Sarcini, respectiv depășesc cerințele privind nivelul calitativ solicitat și ating nivelul descris de Ofertant în Propunerea Tehnica (Planul de management/gestionare a calității în cadrul Contractului)

Activitatea ce urmează a fi realizată pentru obținerea asigurării realizării nivelului de calitate	**Nominalizați activitatea, rezultatul – după caz- incluse la capitolul anterior în legătură cu care se realizează obținerea asigurării**	**Metoda, procedura tehnica, instrumentul**	**Resurse folosite (ex.: software, resurse umane, informații, laboratoare etc.)**	**Structura organizațional ă/ unitatea funcțională implicată**	**Documente și înregistrări privind calitatea**	**Perioada de remediere a Defectelor/ Neconformităților**	**Informații suplimentare, acolo unde este aplicabil**
Intalnirea de inceput a proiectului (Kick-Off meeting)	Pct 1.1 din Planul de lucru	La demararea proiectului se va organiza o intalnire de kick-off care are rol de aliniere a perspectivelor, informatiilor si abordarilor comune Deloitte si BNM.	○ Partener responsabil Asigurarea Calitatii QA ○ Manager Proiect – expert cheie	○ Personal Backstopping ○ Manager Proiect	Minuta intalnirilor	Conform contract.	

			○ Reprezentantii BNM alocati pentru acest proiect	○ Personal BNM desemnat			
Stabilirea de SLA-uri in cadrul Documentul de aplicabilitate	Pct 1.1.9 si 1.1.10 din Planul de lucru						
Organizarea întâlnirilor de lucru, de monitorizare a progresului activităților și de analiză a rezultatelor intermediare, corespunzătoare fiecărei etape din Contract	Pct 1.7 si 2.21 din Planul de lucru	In fiecare saptamana se va organiza o intalnire interna Deloitte in care participa toti membrii echipei. In cadrul acestei intalniri se prezinta rezultatele parcurgerii activitatilor anterioare, activitatile ce urmeaza a fi parcurse in urmatoarea saptamana dar si eventualele limitari. La fiecare 2 saptamani se va organiza cate o sedinta comuna de lucru la care participa reprezentantii Deloitte si persoanele desemnate din partea clientului. Aceste intalniri au rolul de a armoniza eforturile comune de livrare a proiectului in cauza. In cazul in care informatii noi apar in timpul derularii activitatilor proiectului, informatii de natura care sa afecteze semnificativ parametrii si timpi de livrare a proiectului, acestea vor fi prezentate cu celeritate de catre expertii tehnici atat managerului de proiect Deloitte, urmand ca mai apoi managerul de proiect Deloitte sa aplice eventuale corectii si, eventual, anuntarea persoanelor responsabile din partea BNM.	○ Manager Proiect – expert cheie ○ Expert cheie 2, 3, 4 si 5 ○ Personal backstopping – Partenerul responsabil cu Asigurarea Calitatii QA ○ Reprezentantii BNM alocati pentru acest proiect	○ Personal Backstopping ○ Manager Proiect ○ Experti cheie ○ Personal BNM desemnat	Minuta intalnirilor	Conform contract.	
Alocarea unui personal competent, calificat si experimentat pentru desfasurarea proiectului		Datorită riscurilor inerente asociate testării de tip Red Team, un element care ajuta in procesul de management al riscurilor si de asigurare a calitatii este utilizarea celor mai competenti si calificati specialisti cu experienta practica.	○ Manager Proiect – expert cheie ○ Expert chee 2, 3, 4 si 5 ○	○ Manager Proiect ○ Experti cheie			

		Echipa Deloitte desemnata acestui proiect depaseste asteptarile setate de catre BNM in cadru documentatie de atribuire atat prin alocarea unui numar mai mare de specialisti pe care Deloitte ii are la dispozitie, cat si prin certificarile aditionale pe care acestia le detin, dar si numarul de proiecte semnificativ la care persoanalul desemnat a participat in trecut.					
Desfasurarea proiectului in tr-o maniera „Agile”		Desfasurarea proiectului in tr-o maniera „Agile” care este indreptata spre nevoile imediate ale proiectului si de asemenea permite desfasurarea in paralel a anumitor activitati.		○ Personal Backstopping ○ Manager Proiect ○ Experti cheie			
Asigurarea calitatii (QA) pentru toate livrabilele		Managerul de Proiect are experiența şi capacitatea de a urmări şi de a se implica activ în managementul contractului, precum şi de a verifica în mod constant aspectele ce țin de calitate. Implicarea partenerului responsabil cu asigurarea calităţii în toate fazele proiectului. Avand in vedere vasta experienta profesionala a expertilor, certificarile variate si specializate pe subiectul in cauza, acestia sunt factori care contribuie la intarirea faptului ca depunem toate eforturile necesare indeplinirii tuturor conditiilor de calitate asteptate de catre Autoritatea Contractanta.	○ Partener responsabil Asigurarea Calitatii QA ○ Manager Proiect – expert cheie	○ Personal Backstopping ○ Manager Proiect			

3. Planul de lucru pentru implementarea/realizarea serviciilor/obținerea rezultatelor în cadrul Contractului

A se vedea graficul de timp atasat la oferta unde este prezentata in detaliu planificarea detaliata a planului de activitati , a timeline-ului si a necesarului de personal.

4. Personalul propus și managementul realizării serviciilor

a. Structura echipei propuse pentru realizarea serviciilor, cu prezentarea organigramei echipei și a *informațiilor* relevante pentru experții cheie și documente suport pentru demonstrarea calificărilor educaționale și profesionale, a abilităților, a experienței solicitate.

Nume și Prenume	**Poziția de expert cheie pentru care este propus**	**Activitățile din cadrul contractului la realizarea cărora participă**	**Numărul de zile lucrătoare alocate expertului**	**Operatorul economic participant la procedură, ce asigură accesul la expertul ce va presta activități în contract**
Ifrim Adrian	Expert cheie 1 Project Manager	Management Proiect si activitati de teste de penetrare	12	Deloitte Consultanta SRL
Ionescu Andrei	Expert 2 expert Sef securitate sisteme informatice Personal Backstopping / Quality Assurance (Asigurarea calitatii)	Activitati de teste de penetrare	17 3	Deloitte Consultanta SRL
Ionica Dragos	Expert 3 expert testare securitate infrastructura retea	Activitati de teste de penetrare	15	Deloitte Consultanta SRL
Mocanu Cristian	Expert 4 expert testare securitate sisteme informatice	Activitati de teste de penetrare	12	Deloitte Consultanta SRL
Marin Dan	Expert 5 expert testare securitate sisteme informatice si infrastructurii de tip WI-FI	Activitati de teste de penetrare	8	Deloitte Consultanta SRL

b. O descriere a modului de asigurarea a suportului (back-stopping) pe perioada derulării Contractului la nivelul Ofertantului

Backstopping-ul este activitatea de bază desfășurată de către anumiti membri ai echipei Deloitte în sprijinul lor direct al echipei care presteaza munca efectiva din teren. Această caracteristică distinctivă in cadrul abordării unui proiect de testare Intelligence-led Red Team este ceea ce ne deosebește fata de alți furnizori care, de obicei, nu au un cadru instituțional care să ofere backstopping-ul sistematic întreprins de un astfel de proiect. Prin acest proces de backstopping Deloitte se diferentiaza fata de alte institutii si permite clientilor sa utilizeze acest cadru de sprijin institutional pentru maximizarea rezultatelor.

Personal managerial relevant pentru planificarea, organizarea, conducerea și controlul activităților în cadrul Contractului	Adrian Ifrim, Manager de proiect, acesta are rolul de a asigura planul de activitati si managementul tutoror activitatilor si persoanalului pentru a atinge obiectivele proiectului de timp, calitate si buget. Andrei Ionescu, Partener responsabil cu coordonarea si asigurarea calitatii a acestui proiect. Acesta este desemnat in Planul de Activitati ca si QA Partner, Personal Backstopping / Quality Assurance
Metode și instrumente utilizate pentru capitalizarea și valorificarea cunoștințelor necesare în operarea proceselor și pentru realizarea conformității serviciilor și rezultatelor solicitate prin Contract în cadrul organizației operatorului economic, Ofertant	• Identificarea si alocarea personalului cel mai potrivit pentru proiectul de fata. • Organizarea de sedinte periodice de update a proiectului. • Pregatirea documentatiei proiectului. • Pregatirea detaliata a planului de lucru (activitati, resurse, timeline) • Managementul si supravegherea activitatilor expertilor (mentinere contact permanent cu expertii, monitorizare progres, evaluare performante experti). • Revizuirea si editarea livrabilelor pregatite de experti.
Surse interne și surse externe pe care se bazează cunoștințele organizaționale pentru derularea activităților solicitate prin Contract	Sursa externa: Framework-ul TIBER-EU Sursa interna: Cunostintele si experienta expertilor propusi

c. Abordarea și metodologia propusa pentru gestionarea relației cu Autoritatea Contractanta, prin raportare la informațiile furnizate și cerințele cuprinse în Caietul de Sarcini la Secțiunea Managementul Contractului, respectiv:
   i. Prezentarea metodelor și a planurilor de management utilizate pentru planificarea și monitorizarea derulării activităților din Contract, pentru planificarea și monitorizarea obținerii rezultatelor în cadrul Contractului, pentru planificarea și monitorizarea costurilor în cadrul Contractului, pentru planificarea și monitorizarea relațiilor cu factorii interesați identificați ca fiind relevanți în cadrul Caietului de Sarcini;
   ii. Descrierea modului de realizare a comunicării cu Autoritatea Contractantă pe durata derulării Contractului.

Acest aspect a fost prezentat in multiple sectiuni pe parcursul prezentei Propuneri Tehnice.

- Din cadrul BNM si Deloitte se vor nominaliza persoanele responsabile (managerii de proiect) care să asigure o comunicare intre echipele de lucru.
- Se va stabili metoda de escaladare către comitetul de conducere al contractului a tuturor aspectelor care ar putea impacta derularea cu succes a contractului.
- Asigurarea unor multiple mijloace de comunicare intre persoanele direct implicate care să nu permită întârzieri sau neclarităţi.
- Realizarea comunicării în cadrul contractului se va face prin doua metode:
    - comunicarea prin discuții directe folosita drept instrument de întărire a relațiilor intre membrii echipei (discutii telefonice, intalniri fizice periodice)

  - comunicarea bazata pe tehnologia informației (e-mail, fax) - folosita în cazul transmiterii unor informații esențiale contractului.
- Delimitarea clara a informațiilor ce pot fi transmise prin discuții directe şi a celor ce pot fi transmise prin mijloace scrise.
- Facilitarea accesului la informații în vederea realizării Obiectivelor contractului reprezintă un aspect fundamental care va fi subliniat de echipa de proiect încă de la întâlnirea iniţială de demarare a proiectului.
- In cadrul intalnirilor periodice de aliniere si progres a celor doua echipe de lucru, Deloitte si BNM, vom avea ca baza de discutii documentele ce au stat la baza atribuirii contractului catre Deloitte (Oferta Tehnica, planul de lucru cu Activitati si Timeline, etc). In cadrul intalnirilor respective se va inregistra minuta intalnirilor pentru a ramane ca dovada a celor discutate si agreate in timpul intalnirilor de progres.
- In cazul in care informatii noi apar in timpul derularii activitatilor proiectului, informatii de natura care sa afecteze semnificativ parametrii si timpii de livrare a proiectului, acestea vor fi prezentate cu celeritate de catre expertii tehnici atat managerului de proiect Deloitte, urmand ca mai apoi managerul de proiect Deloitte sa aplice eventuale corectii si, eventual, anuntarea persoanelor responsabile din partea BNM.
- Rapoartele intermediare si finale si orice informatii de matura sensibila se vor prezenta intr-o maniera securizata persoanelor desemnate si autorizate din partea ambelor parti.

d. Modalitatea de îndeplinire a cerințelor privind raportarea solicitate în cadrul Contractului, inclusiv documentele finale în raport cu prevederile cerințelor minime din Caietul de Sarcini.

A. RAPOARTELE/DOCUMENTELE CE PRIVESC REZULTATUL ACTIVITĂȚILOR

Cerința minimă din Caietul de Sarcini	**Modalitatea de îndeplinire a cerinței**
Etapa de documentare a testului de penetrare constă în generarea unui raport consolidat care trebuie să cuprindă toate rezultatele detaliate obținute în timpul testelor, cu analiza corespunzătoare a acestor informații, în scopul de a fi interpretate în mod corect de către BNM și de a înțelege implicațiile de securitate asupra infrastructurii analizate.	Dupa faza de testare, Deloitte va pregăti un raport final de testare consolidat cu rezultatele testului de securitate, în limba română. Raportul de testare final este precedat de un raport intermediar (pre re-testare) si de raportul de Threat Intelligence ce a stat la baza dezvoltării scenariilor de testare.
Raportul consolidat va cuprinde si descrierea vulnerabilităţilor identificate, cu un rating de risc pe fiecare vulnerabilitate și va propune măsuri de rezolvare adecvate.	Raportul va include vulnerabilitățile și amenințările identificate ca riscuri potențiale (conform metodologiei CVSS), precum și recomandările pentru eliminarea acestora. Constatările și riscurile (tehnice) vor fi discutate în detaliu cu administratorii de sistem desemnaţi de BNM.
Raportul rezultat în urma testării va include minimum următoarele aspecte: • Perioada efectuarii testului de penetrare; • Înregistrarea tuturor activităţilor; • Menţionarea tuturor constatărilor; • Autorizaţii şi validări;	Raportul final, rezultat in urma testarii va include urmatoarele: • Perioada de desfasurare a proiectului cu fazele/activitatile aferente. • Echipa care a participat in cadrul proiectului. • Un sumar executiv ce va sublinia constatările tehnice și de proces, vulnerabilitățile identificate si validate, și recomandările noastre. • Descriere detaliată a scopului, abordării și a procedurilor efectuate. • Un rezumat al metodologiei de testare. • Detaliere a observațiilor tehnice, enumerând elementele afectate și cele mai importante evoluții posibile. • Semnificația sau implicațiile observațiilor detaliate, din punct de vedere tehnic, dar si de impact de business evaluat.
Constatările vor trebui detaliate şi prezentate astfel încât să permită elaborarea rapidă a unui plan de remediere, după cum urmează: • Descrierea vulnerabilităţilor identificate şi recomandări de remediere; • Sistemul gazdă, sistemele de reţea sau aplicaţiile web afectate de vulnerabilităţile identificate;	

<table>
<tr>
<td>• Riscurile tehnice si de business inerente acestor vulnerabilităţi.</td>
<td rowspan="2">• Descrierea potențialei cauze a vulnerabilității, și dovezi pentru a ilustra modul în care se poate reproduce problema.
• Evaluarea riscului finding-urilor, bazată pe criticalitate, probabilitatea de apariție, posibilitățile de exploatare și natura consecințelor tehnice și funcționale.
• Referințe către CVE sau BID sau bazele de date cu vulnerabilități ale furnizorilor (dacă sunt disponibile)

În baza solicitării dumneavoastră, Deloitte va oferi o prezentare orientată către conducerea institutiei si factorilor de decizie și / sau a grupurilor de lucru ale BNM pentru a rezuma observațiile cheie și să evalueze riscurile expuse.
Deloitte determină nivelul de risc al fiecărei observații pe baza probabilității și potențialul de a crea daune al problemei (impact), luând în considerare criticalitatea sistemelor afectate.

Constatarile vor fi clasificate conform matricei de risc de mai jos:
<table>
<tr><th>Probabilitate/Risc (clasificare constatare)</th><th>Improbabil</th><th>Posibil</th><th>Probabil</th></tr>
<tr><td>Mare</td><td>Important</td><td>Semnificativ</td><td>Critic</td></tr>
<tr><td>Mediu</td><td>Important</td><td>Important</td><td>Semnificativ</td></tr>
<tr><td>Scazut</td><td>Minor</td><td>Minor</td><td>Minor</td></tr>
</table>
</td>
</tr>
<tr>
<td>Structura raportului final va fi urmatoarea:

Introducere
Această secţiune descrie scopul şi rezultatul proiectului precum si paşii ce au fost realizaţi pe parcursul testului de penetrare de securitate.
Rezumat
Cuprinde situația generală de risc, problemele de securitate identificate și măsurile de atenuare recomandate. De asemenea, vor fi prezentate pe scurt cele mai importante probleme identificate, inclusiv o evaluare a riscurilor și a posibilelor consecințe a lacunelor de securitate identificate, precum și recomandările pentru a le atenua.
Documentație detaliată
Această secțiune a raportului trebuie să conțină lista completă a tuturor constatărilor. Documentul va include toate informațiile necesare care să permită repetarea testelor, dacă este necesar. Constatările trebuie să fie clasificate în funcţie de nivelul de risc ca „mare” , ”mediu” sau ”scăzut”. De asemenea, documentul trebuie să includă explicația detaliată și evaluarea riscurilor, precum și posibilele consecințe pentru BNM. Cauzele vulnerabilităților tehnice trebuie să fie examinate în contextul constatărilor specifice.</td>
</tr>
</table>

B. RAPOARTELE CE PRIVESC PROGRESUL ACTIVITĂȚILOR, ADMINISTRAREA ȘI MANAGEMENTUL CONTRACTULUI

Cerința minimă din Caietul de Sarcini	**Modalitatea de îndeplinire a cerinței**
Activitati de coordonare	
Organizarea întâlnirii de demarare a activităților în Contract, pentru obținerea asigurării că Autoritatea Contractantă și Contractantul au aceeași perspectivă asupra activităților și rezultatelor din Contract	La demararea proiectului se va organiza o intalnire de kick-off care are rol de aliniere a perspectivelor, informatiilor si abordarilor comune Deloitte si BNM.
Organizarea întâlnirilor de lucru, de monitorizare a progresului activităților și de analiză a rezultatelor intermediare, corespunzătoare fiecărei etape din Contract	In fiecare saptamana se va organiza o intalnire interna Deloitte in care participa toti membrii echipei. In cadrul acestei intalniri se prezinta rezultatele parcurgerii activitatilor anterioare, activitatile ce urmeaza a fi parcurse in urmatoarea saptamana dar si eventualele limitari. La fiecare 2 saptamani se va organiza cate o sedinta comuna de lucru la care participa reprezentantii Deloitte si persoanele desemnate din partea clientului. Aceste intalniri au rolul de a armoniza eforturile comune de livrare a proiectului in cauza. In cazul in care informatii noi apar in timpul derularii activitatilor proiectului, informatii de natura care sa afecteze semnificativ parametrii si timpi de livrare a proiectului, acestea

	vor fi prezentate cu celeritate de catre expertii tehnici atat managerului de proiect Deloitte, urmand ca mai apoi managerul de proiect Deloitte sa aplice eventuale corectii si, eventual, anuntarea persoanelor responsabile din partea BNM.
Coordonarea resurselor și activităților de către fiecare parte contractantă separat și împreună	Aceasta coordonare se va realiza in timpul intalnirilor periodice de status-update si de sincronizare. Din partea Deloitte, Managerul de proiect detine viziunea de ansamblu asupra intregului proiect si va gestiona resursele si activitatile.
Distribuirea informațiilor privind rezultatele/documentele intermediare și finale factorilor interesați relevanți identificați în Caietul de Sarcini și în Propunerea Tehnică	Rapoartele intermediare si finale se vor prezenta intr-o maniera securizata persoanelor desemnate si autorizate din partea clientului la datele agreate de comun acord in planul de lucru.
Activitati de monitorizare	
Măsurarea progresului activităților din Contract prin raportare la Contract si alte documente agreate intre parti.	Progresul activitatilor va fi monitorizat in cadrul intalnirilor periodice de aliniere intre partile implicate, luand in calcul planurile de management si de activitati furnizate anterior.
Activitati de control	
Controlul implică identificarea acțiunilor corective pentru abordarea abaterilor de la Contract constatate de comun acord în cadrul întâlnirilor dintre Contractant și Autoritatea Contractantă, și care se referă la dimensiuni precum abordarea și metodologia utilizată în realizarea serviciilor, nivelul calitativ, cost, timp etc.	Prin activitatile periodice pe care le desfasoara atat echipa de experti, managerul de proiect dar si Partenerul responsabil cu asigurarea calitatii din partea Deloitte, controlul, propunerea si aplicarea masurilor corective se intampla cu foarte mica intarziere, pe masura ce se desfasoara activitatile din cadrul proiectului.

e. Abordarea propusă pentru managementul riscurilor, cu luarea în considerare a cerințelor incluse în Caietul de Sarcini

Riscurile prezentate în Caietul de Sarcini sau riscurile identificate de către Ofertant, după cum este aplicabil în funcție de conținutul Caietului de Sarcini	Măsurile propuse de către Ofertant ca parte a strategiei de risc (prevenirea/atenuarea/eliminarea riscurilor identificate)	Activitatea din planul de lucru și metodologia de prestare a serviciilor unde este reflectată măsura propusă
Dificultăți de colaborare și comunicare între factorii interesați implicați	• Stabilirea unei persoane din cadrul fiecărei entitati care să asigure o comunicare echipele de lucru • Escaladarea către comitetul de conducere al contractului a tuturor aspectelor care ar putea impacta derularea cu succes a contractului • Asigurarea unor mijloace de comunicare intre persoanele direct implicate care să nu permită intârzieri sau neclarităţi • Realizarea comunicării în cadrul contractului se va face prin doua metode: o comunicarea prin discuții directe folosita drept instrument de întărire a relațiilor intre membrii echipei	Activitatile si intalnirile de Kick-off si cele periodice de update proiect.

	○ comunicarea bazata pe tehnologia informației (e-mail, fax) - folosita în cazul transmiterii unor informații esențiale contractului. • Delimitarea clara a informațiilor ce pot fi transmise prin discuții directe şi a celor ce pot fi transmise prin mijloace scrise.	
Datele și informațiile necesare desfășurării serviciilor comunicate de către Autoritatea Contractantă nu sunt suficiente pentru îndeplinirea cerințelor solicitate prin Caietul de Sarcini	• Facilitarea accesului la informaţii în vederea realizării Obiectivelor contractului reprezintă un aspect fundamental care va fi subliniat de echipa de proiect încă de la întâlnirea iniţială de demarare a proiectului. • Printr-un proces participativ, de implicare a tuturor factorilor interesați, prin susţinerea din partea Autoritatii Contractante, printr-un bun management şi o bună coordonare a procesului de colectare a datelor din partea echipei de proiect, aceasta supoziție va fi îndeplinită. În plus, trebuie subliniat faptul că membrii ai echipei de proiect posedă excelente abilitați de comunicare cu grupul ţintă al acestui proiect, fiind familiarizaţi cu cadrul socio-economic din România, prin implicarea în ultimii ani în activităţi de management de program.	Activitatile si intalnirile de Kick-off si cele periodice de update proiect.
Adăugarea de activități/ solicitări de informații noi, în funcție de progresul activităților	• Deloitte va fi flexibil la eventualele solicitări suplimentare cu condiţia ca acestea să fie definite în faza de planificare pentru a se putea realiza o alocare adecvata a resurselor ce urmează a fi mobilizate în această direcţie. • Avand in vedere numarul aditional de experti implicati in proiect, pentru ca gradul lor de incarcare sa nu fie maxim, acestia vor putea prelua activitati / solicitari aditionale in cazul in care astfel de situatii se vor materializa, avand in vedere atingerea tuturor cerintelor din cadrul contractului si incadrandu-ne in termenele stricte de livrare. • Să se stabilească o limită superioară de cerinţe noi pe care	Activitatile si intalnirile de Kick-off si cele periodice de update proiect.

	le poate formula clientul în cursul implementării contractului	
Incadrarea strictă în timpul alocat derulării contractului	• Managerul de proiect va urmări în mod riguros stadiul de implementare a contractului., solicitând membrilor echipei statusuri săptămânale ale activităţilor realizate. • Stabilirea de termene de livrare ferme pentru fiecare dintre activităţile contractului. • Clientul va fi implicat încă din fazele incipiente ale contractului şi va fi la curent cu eventualele situaţii care ar putea determina întârzieri ale activităţilor înainte de a se produce. • Includerea in proiect a mai multor resurse umane / experti pentest decat minimul solicitat pentru ne asigura de faptul ca gradul de incarcare pe fiecare expert nu este maxim	Activitatile si intalnirile de Kick-off si cele periodice de update proiect. De asemenea, faptul ca am alocat mai multe resurse pentru efectuarea activitatilor.
Indeplinirea cerințelor contractuale în condiții de calitate așteptate de către Autoritatea Contractantă.	• In cadrul acestei oferte prezentam metodologia de respectare şi aplicare a managementului calitatii de către toata echipa de proiect. • Punerea la dispoziția tuturor experților cheie, dar şi a personalului de backstopping încă de la începutul contractului a procedurii de management al calitatii pentru a fi însușita şi respectata. • Managerul de Proiect are experiența şi capacitatea de a urmări şi de a se implica activ în managementul contractului, precum şi de a verifica în mod constant aspectele ce țin de calitate. • Implicarea partenerului responsabil cu asigurarea calităţii în toate fazele proiectului. • Avand in vedere vasta experienta profesionala a expertilor, certificarile variate si specializate pe subiectul in cauza, acestia sunt factori care contribuie la intarirea faptului ca depunem toate eforturile necesare indeplinirii tuturor conditiilor de calitate	Activitatile de asigurare a calitatii livrabilelor conform standardelor Deloitte dar si a celor solicitate de catre Client (Quality Assurance). 1.6.2; 2.14.2; 2.18.2 din planul de activitati.

	asteptate de catre Autoritatea Contractanta.	

f. Strategia utilizată de Ofertant pentru prevenirea conflictului de interese

Procesul de acceptare a clienților și a proiectelor prevede o fază obligatorie de verificare a independenței și conflictelor de interese a companiei Deloitte faţă de client. Aceasta verificare este realizată de către o echipă dedicată la nivel regional. Rezultatul acestei verificări poate fi "aprobat cu condiții", caz în care echipa de proiect trebuie să întreprindă o serie de acțiuni pentru a minimiza expunerea în fața riscului de conflict de interese sau poate exista decizia de a interzice orice formă de colaborare cu potențialul client dacă riscul nu poate fi gestionat.

Toți membrii echipei au responsabilitatea de a identifica și a raporta Partenerului conflictele de interese personale care pot apărea ca urmare a participării în proiect. Aspecte care pot fi luate în considerare sunt: existența unui membru a familiei de pana la gradul 2 care lucrează în cadrul potențialului client, existența unui interes financiar în compania respectivă, existenta unei relații de muncă anterioare cu compania în cauză.

g. Prezentarea strategiei anti-corupție ce va fi implementată de Ofertant pentru prevenirea corupției

Managerul de proiect are responsabilitatea gestionării activității zilnice aferente fazelor proiectului precum și a facturilor emise către contractant în conformitate cu contractul încheiat.

Partenerul de proiect revizuiește toate livrabilele și este ultimul responsabil pentru conformitatea livrabilelor cu cerințele contractuale. De asemenea acesta are și responsabilitatea aprobării facturilor emise către Autoritatea contractantă după verificarea cu prevederile contractuale. Încasările aferente proiectului sunt monitorizate prin rapoarte dedicate atât de departamentul Financiar – prin echipa de Cash Collection cât și de managerul și partenerul de proiect.

h. Prezentarea modului de realizare a înregistrărilor pentru activitățile, deciziile și fluxul informațional și financiar în legătură cu acest Contract, astfel încât să se asigure trasabilitatea deciziilor în cazul în care acest Contract este supus verificărilor de terță parte

Deloitte a definit o politică de arhivare, care va fi implementată și în cadrul acestui proiect.

Accesul la locația aferentă documentației proiectului este restricționat echipei de proiect. După finalizarea activităților proiectului, efectuarea procedurilor de asigurare a calității și aprobarea livrabilelor de către Autoritatea contractantă, documentația aferentă proiectului este transferată spre arhivare într-o locație securizată care poate fi accesata de persoanele responsabile cu arhivarea. Accesarea documentației arhivate poate fi realizată doar pe baza de solicitare scrisă aprobată de partenerul de proiect.

5. Modalitatea de efectuare a înregistrărilor și înregistrările efectuate în legătură cu indicatorii de performanță incluși în Documentația de atribuire

Managerul de proiect are responsabilitatea gestionării activității zilnice aferente fazelor proiectului în conformitate cu contractul încheiat. In fiecare saptamana se va organiza o sedinta generala in care sunt implicate toate resursele Deloitte parte din proiect. In cadrul acestei intalniri se vor evalua statusul activitatilor desfasurate pana in acel moment, activitatile ce urmeaza a se desfasura, eventuale restrictii si situatii neprevazute identificate si propuneri de remediere.

La fiecare 2 saptamani se va organiza cate o sedinta comuna de lucru la care participa reprezentantii Deloitte si persoanele desemnate din partea BNM. Aceste intalniri au rolul de a armoniza eforturile comune de livrare a proiectului in cauza.

In cazul in care informatii noi apar in timpul derularii activitatilor proiectului, informatii de natura care sa afecteze semnificativ parametrii si timpi de livrare a proiectului, acestea vor fi prezentate cu celeritate de catre expertii tehnici atat managerului de proiect Deloitte, urmand ca mai apoi managerul de proiect Deloitte sa aplice eventuale corectii si, eventual, anuntarea persoanelor responsabile din partea BNM.

Partenerul de proiect revizuiește toate livrabilele și este ultimul responsabil pentru conformitatea livrabilelor cu cerințele contractuale.

29.10.2021

Andrei Ionescu

Administrator

Deloitte Consultanta SRL