



Banca Nationala a Moldovei (BNM)

kpmg.com/romania

CYBER & TECHNOLOGY

**Propunere tehnica pentru servicii de evaluare
și de analiză a asigurării calității sistemelor
(servicii de testare a securității SI al BNM).**

30 October 2021



KPMG Advisory SRL
DN.1 Bucuresti-Ploiesti nr. 69-71
Sector 1, Bucuresti 013685,
Romania

Tel +40 372 377 800
Fax +40 372 377 700
www.kpmg.com/romania

Confidential

Banca Nationala a Moldovei

București

30 October 2021

Ca urmare a Caietului de sarcini pentru Servicii de evaluare și de analiză a asigurării calității sistemelor (servicii de testare a securității SI al BNM) am pregătit oferta noastră tehnico-economica pentru a răspunde cerințelor dvs.

Abordarea și metodologia noastră se bazează pe înțelegerea nevoilor dumneavoastră și poate fi modificată și adaptată în continuare pentru a îndeplini cerințele dumneavoastră specifice.

Pentru realizarea acestui proiect, am alcătuit o echipă din cadrul departamentului Securitate Cibernetică (Cyber) din KPMG, cu experiența semnificativă în furnizarea acestor servicii. Pe lângă experiența locală, beneficiem și de experiența internațională în domeniul auditului IT și de securitate.

Dorim de asemenea să vă atragem atenția asupra experienței noastre în acest domeniu. Mai exact, am realizat mai multe proiecte de evaluare a nivelului de securitate informatica pentru institutii financiare si companii activand in diverse industrii din România si alte tari din Europa: financiar – bancar, asigurari, telecom, retail, petrol si gaz, energie.

Mai mult, KPMG Advisory a obtinut din partea CERT-RO Atestatul de Auditor de Securitate Cibernetica, in conformitate cu Legea 362/2018 in Romania.

Sperăm că această propunere să îndeplinească așteptările Dumneavoastră. Furnizarea serviciilor incluse în această propunere este condiționată de finalizarea cu succes a procedurilor de management al riscului ale KPMG, care vor identifica eventualele conflicte de interese care ne-ar împiedica să furnizăm aceste servicii.

Vă rugăm să nu ezitați să ne contactați dacă aveți întrebări legate de propunerea noastră sau pentru a obține orice alte informații de care aveți nevoie.

Cu stimă,

Gabriel Mihai Tanase

Partener, KPMG în România & Moldova
Tehnologie & Securitate Cibernetică



De ce KPMG?

Vă punem la dispoziție o echipa de profesioniști cu experiență și cunoștințe aprofundate în Securitatea cibernetică.

De-a lungul anilor, KPMG a construit o reputație pentru excelență în livrarea serviciilor de Securitate cibernetică.

Calitățile KPMG	Cum răspundem la nevoile clienților	Beneficiile pentru dumneavoastră
Experiența	<ul style="list-style-type: none"> — Executăm proiecte similare în mod regulat. Echipa noastră de securitate cibernetică are experiență extensivă atât în România cât și în regiune. — În prezent oferim servicii atât unor clienți locali cât și unor clienți cu amprentă globală, prin care analizăm conformitatea sistemelor IT și securității acestora cu diverse standarde naționale sau internaționale. — Avem o relație apropiată cu Asociația pentru Controlul și Auditul Sistemelor Informatice (ISACA) pentru care punem la dispoziție personal calificat în vederea livrării unor cursuri de pregătire, ori de câte ori este necesar. 	<ul style="list-style-type: none"> — Competențe de top, gata să fie puse la dispoziția Dvs. — Perspectivă practică observată în cadrul unui număr mare de organizații — Încredere
Echipa	<ul style="list-style-type: none"> — Oamenii noștri sunt pregătiți și au experiență în domenii relevante, precum : Securitate cibernetică, Reziliență și continuitatea afacerii, riscuri și controale, auditul sistemelor informatice etc. Aceștia au urmat programe relevante de studii și dețin certificări profesionale recunoscute (așa cum sunt prezentate în secțiunea Echipa KPMG). 	<ul style="list-style-type: none"> — Lucrăm împreună pentru atingerea termenelor și a obiectivelor stabilite — Specialiști în auditul IT cu experiența necesară conform nevoilor Dvs. — Cunoștințe temeinice în multe arii de interes care pot fi împărtășite cu Dvs.
Întindere globală	<ul style="list-style-type: none"> — Suntem prezenți în 144 țări în toată lumea, dacă veți avea nevoie de o extindere globală în viitor. — Echipa noastră este distribuită global, cu centre de excelență peste tot în lume. 	<ul style="list-style-type: none"> — Echipa locală, care ajută la reducerea costurilor și timpului pierdut cu deplasările. Ajutor la nivel global, ce poate fi ușor accesat, dacă este nevoie. — Livrarea serviciilor într-un mod consistent și armonizat.
Suport specializat	<ul style="list-style-type: none"> — Punem la dispoziție un Coordonator specializat care va gestiona proiectul și să acționeze ca un punct unic de contact. Putem aduce specialiști suplimentari ori de câte ori este nevoie pentru a sprijini echipa de bază. 	<ul style="list-style-type: none"> — Expertiză specializată, ori de câte ori este nevoie — Transfer de abilități și competențe către personalul Dvs. — Profesioniști care înțeleg provocările cu care vă confrunțați
Gândire inovativă	<ul style="list-style-type: none"> — Căutăm tot timpul oportunități să aducem valoare sau să reducem costurile. De exemplu, KPMG vă poate ajuta să definiți un cadru extins de control, care să aducă laolaltă cerințele mai multor standarde sau cerințe de conformitate într-un singur sistem de guvernanță. 	<ul style="list-style-type: none"> — Idei de integrare a eforturilor de guvernanță și asigurarea conformității — Abordare de tip "o singură echipă" ce lucrează unitar, consistent și colaborativ
Independență	<ul style="list-style-type: none"> — KPMG este o firmă independentă cu reputație internațională, cu standarde ridicate în asigurarea eticii profesionale și a confidențialității clienților. — Suntem independenți de organisme de certificare 	<ul style="list-style-type: none"> — Fără agenda ascunsă — Concluzii independente, la un nivel ridicat de calitate pentru clienți și celelalte părți interesate.

De ce KPMG? (cont.)

Ce obțineți din acest proiect?



Oameni și expertiză

Apreciem importanța unei echipe experimentate și calificată. Pentru această oportunitate am pus laolaltă o echipă de top cu experiență în industrie și în serviciile de acest tip. Echipa va fi condusă de Gabriel Tanase, Partener responsabil cu serviciile de Securitate Cibernetică în cadrul KPMG, care are o experiență semnificativă în acest sector



Servicii de calitate

Avem un istoric consistent în oferirea de servicii de calitate clienților noștri ce operează în industria financiar-bancară din România și punem mare preț pe relațiile pe care le-am construit de-a lungul anilor. Ne ajutăm în mod constant clienții să răspundă numeroaselor cerințe legislative din domeniul IT și al securității informatice.



Perspectivă proaspătă

Ne vom folosi de experiența noastră în industria bancară și consultanță în servicii asemănătoare pentru a vă oferi o perspectivă nouă. De-a lungul proiectului vă vom oferi feed-back în mod continuu pentru a ne asigura ca ne concentrăm eforturile asupra celor aspecte care contează cel mai mult pentru Dvs. și clienții Dvs..

Scop și obiective

Pe baza caietului de sarcini publicat, vă prezentăm mai jos înțelegerea noastră asupra scopului și obiectivelor acestui proiect. Astfel, obiectivele principale ale proiectului vor include Identificarea și evaluarea vulnerabilităților informatice în cadrul sistemului informatic al BNM prin teste specifice de penetrare din exteriorul și interiorul infrastructurii de rețea.

Abordarea noastră

Abordarea noastră va fi realizată în conformitate cu metodologia KPMG, care este bazată pe cele mai bune practici în domeniu (e.g. standardele de audit și ghidurile ISACA, metodologiile NIST, ISO27001 precum și/ sau metodologiile de testare a securității sistemelor informatice precum OWASP, ISECOM (OSSTM), Offensive Security și SANS.

Abordarea și înțelegerea metodologiilor aplicate sunt susținute de certificările profesionale ale membrilor echipei și atasate la CV-urile lor.

Abordarea noastră (cont.)

Coordonarea acestui proiect va fi realizata de un Partener KPMG si un manager de proiect, ambii experimentati in aria de Securitate cibernetica. Partenerul KPMG va avea ca obiectiv principal asigurarea calitatii proiectului si mentinerea relatiilor si comunicarii continue cu BNM.

Ca si pasi principali ai proiectului mentionam:

- Etapa de planificare – etapa in care se defineste planul proiectului de realizare a testelor de securitate pe baza furnizarii informatiilor necesare din partea BNM cu privire la sistemele ce vor fi incluse in scopul proiectului.
- Etapa de realizare a testelor de Securitate.
- Etapa de raportare. Rapoartele vor fi pregatite utilizand modele de raportare propuse de KPMG, care includ toate elementele solicitate de BNM. De asemenea, daca BNM doreste utilizarea unui model specific de raport, acest lucru este posibil pe baza unei comunicati prealabile (la inceputul etapei de raportare).
- Etapa de inchidere a proiectului – pe baza rapoartelor livrate si agreeate cu BNM (inclusive prezentare in fata conducerii, daca este cazul) se vor completa si semna procesele verbale de acceptanta (utilizand modelele propuse de BNM).

Abordarea noastră (cont.)

Teste de securitate (teste de penetrare) vor fi realizate in conformitate cu metodologia KPMG, care este bazata pe cele mai bune practici in domeniu (e.g. standardele de audit și ghidurile ISACA, metodologiile NIST, ISO27001 precum si/ sau metodologiile de testare a securitatii sistemelor informatice precum OWASP, ISECOM (OSSTM), Offensive Security si SANS.

In continuare puteti regasi un extras din aceasta metodologie iar in Anexa la aceasta oferta tehnica este prezentata metodologia pe larg (conform caietului de sarcini care permite prezentarea unor sectiuni in alte limbi de circulatie internationala, am atast metodologia in limba Engleza pentru a evita alterarea sensului termenilor tehnici prin traducere).

I. Metodologia de testare

Pentru a vă îndeplini cerințele, vă propunem o abordare în faze. Vom direcționa tentative de penetrare (similar cu ceea ce ar putea face un atacator) de pe Internet împotriva tuturor dispozitivelor și serviciilor în scopul auditului. Aceasta se va efectua astfel:

01 Mapare

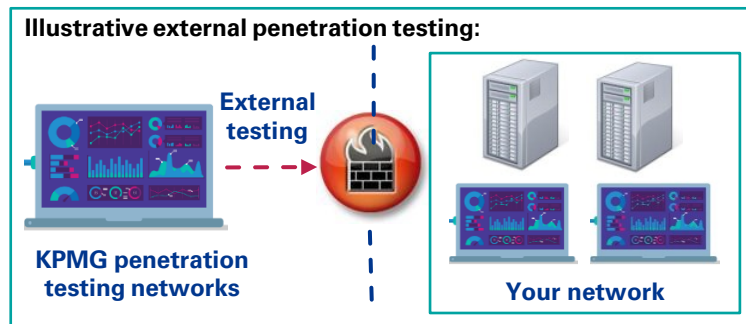
Maparea sistemelor și aplicațiilor IT în scop pentru a identifica serverele și porturile accesibile în rețeaua dvs. utilizând instrumente precum Nmap. Aceasta devine baza testării noastre.

02 Scanarea vulnerabilităților

Porturile deschise identificate sunt scanate pentru vulnerabilități cu instrumente precum Nessus, precum și testarea manuală folosind structura aplicației, maparea configurației și bazele de date cu vulnerabilități deschise (cum ar fi Bugtraq și listele proprii ale furnizorilor). Rezultatele sunt apoi verificate cu metode manuale.

03 Exploatarea

Exploatarea vulnerabilităților pentru a obține intrarea sau determinarea a cât de dificil ar fi să faci acest lucru acordând timp nelimitat, bazat pe un anumit nivel de abilități și experiență. Exploatarea este o formă de testare prin care se folosesc tehnicile unui hacker. Acestea servesc la testarea nivelului de eficiență a măsurilor de securitate implementate și se fac încercări reale de a pătrunde în mediul testat.



II. Vectorii de atac

In executarea testelor, vom executa următorii vectori de atac (precum si altii, identificati ad-hoc):

- Input validation attacks
- Access control attacks
- Authentication and Session;
- Cross Site Scripting (XSS);
- Cross-site Request Forgery (CSRF)
- Error treatment;
- Credential cracking;
- Buffer overflow
- Injection of arbitrary code;
- Insecure object references resulting in LFI/ RFI;
- RCE;
- Application/ infrastructure configuration errors;
- Horizontal escalation of privileges;
- Vertical escalation of privileges;
- Obtaining information from the public domain;
- Inter Domain attacks;
- Application specific vulnerabilities;
- Enumeration techniques;
- Simple basic logic attacks;
- Simple cryptographic/ encryption attacks;
- Unvalidated redirects and forwards;
- Gaining unauthorized access by exploiting vulnerabilities;
- The consolidation of access;
- Removal of traces in the attack;
- Web-services specific tests;
- Replay testing;
- SPA security testing;
- Expunerea la atacuri DoS and DDoS.

Toate testările sunt efectuate iterativ și atunci când un sistem este compromis, ciclul începe din nou pentru a extinde accesul la alte sisteme, toate într-un mod etic și cu scopul final de a vă ajuta să vă protejați sistemele. Pe lângă identificarea automată a vulnerabilității, efectuăm o cantitate semnificativă de lucrări manuale pentru a imita activitățile agenților amenințatori cunoscuți.

Atât echipa noastră de testare tehnică, cât și mediul de testare sunt strict controlate. Lucrările de la distanță sunt efectuate de la laboratorul nostru de securitate, care are controale de acces fizice și logice puternice, incluzând autentificarea de intrare cu doi factori și separarea completă a rețelei.

Abordarea noastră va implica raportarea în timp util și comunicarea deschisă între ambele părți. Rapoartele specifice vor fi pregătite separat pentru fiecare dintre elementele solicitate:

- Plan de proiect;
- Plan de testare;
- Planul de acțiuni (SOW – Scope of Work);
- Rapoarte de test care vor include toate problemele și vulnerabilitățile detectate pe parcursul testării, catalogate în funcție de gravitatea lor;
- Rapoarte de analiză, ce vor conține analiza rezultatelor testelor efectuate prin care se vor identifica și vor fi incluse recomandări de remediere conținând cele mai bune acțiuni/măsurile/metode ce trebuie întreprinse/luate/folosite pentru eliminarea sau micșorarea riscului generat de vulnerabilitățile detectate.
- Rapoarte de test repetate care vor include toate problemele și vulnerabilitățile detectate repetat, catalogate în funcție de gravitatea lor;

Obiectivul general al acestui ciclului de raportare este de a reduce timpul din momentul în care o problemă de securitate este identificată până când este remediată. Acest lucru este în contrast cu raportarea tradițională, atunci când furnizorul livrează raportul doar la sfârșitul angajamentului. Abordarea noastră permite ca fiecare problemă împreună cu evaluarea sa inițială a riscului tehnic să vă fie raportată la scurt timp după descoperirea sa, permițându-vă să acționați imediat asupra celor cu risc ridicat, după cum este necesar.

Procesul de raportare timpurie este descris mai jos :

- ✓ Identificarea vulnerabilității și jurnalizarea problemei - vulnerabilitatea este descoperită și înregistrată de noi împreună cu evaluarea inițială a riscului tehnic, recomandările pe termen scurt și dovezile de susținere.
- ✓ Mitigarea - aveți oportunitatea să reacționați imediat la acesta și să începeți procesul de remediere. Acest pas este executat de dvs. cu clarificări și asistență din partea noastră, dacă este necesar.
- ✓ Verificarea – după ce ați remediat vulnerabilitatea, vom verifica dacă aceasta este într-adevăr remediată și că nu a introdus efecte secundare nedorite.
- ✓ Analiza cauzelor ce au generat problema (root cause analysis) - se efectuează analiza cauzelor ce au generat problema identificate.
- ✓ Raportare - raportul final (de tip **Scrisoare către Management**) este emis cu problemele identificate și cauzele principale. Rapoartele constau într-un rezumat pentru conducere, un indice de constatări care oferă o imagine de ansamblu generală a ceea ce a fost identificat.

Livrabile

Rapoartele furnizate in urma realizarii testarilor de securitate vor fi structurate în două părți distincte:

- partea executivă, și
- partea tehnică.

Partea executivă va conține descrierea pe scurt a problemelor și vulnerabilităților identificate și va utiliza metode grafice. Inclusiv o matrice de evaluare a riscurilor identificate.

Partea tehnică va detalia din punct de vedere tehnic problemele și vulnerabilitățile identificate si va conține cel puțin următoarele capitole:

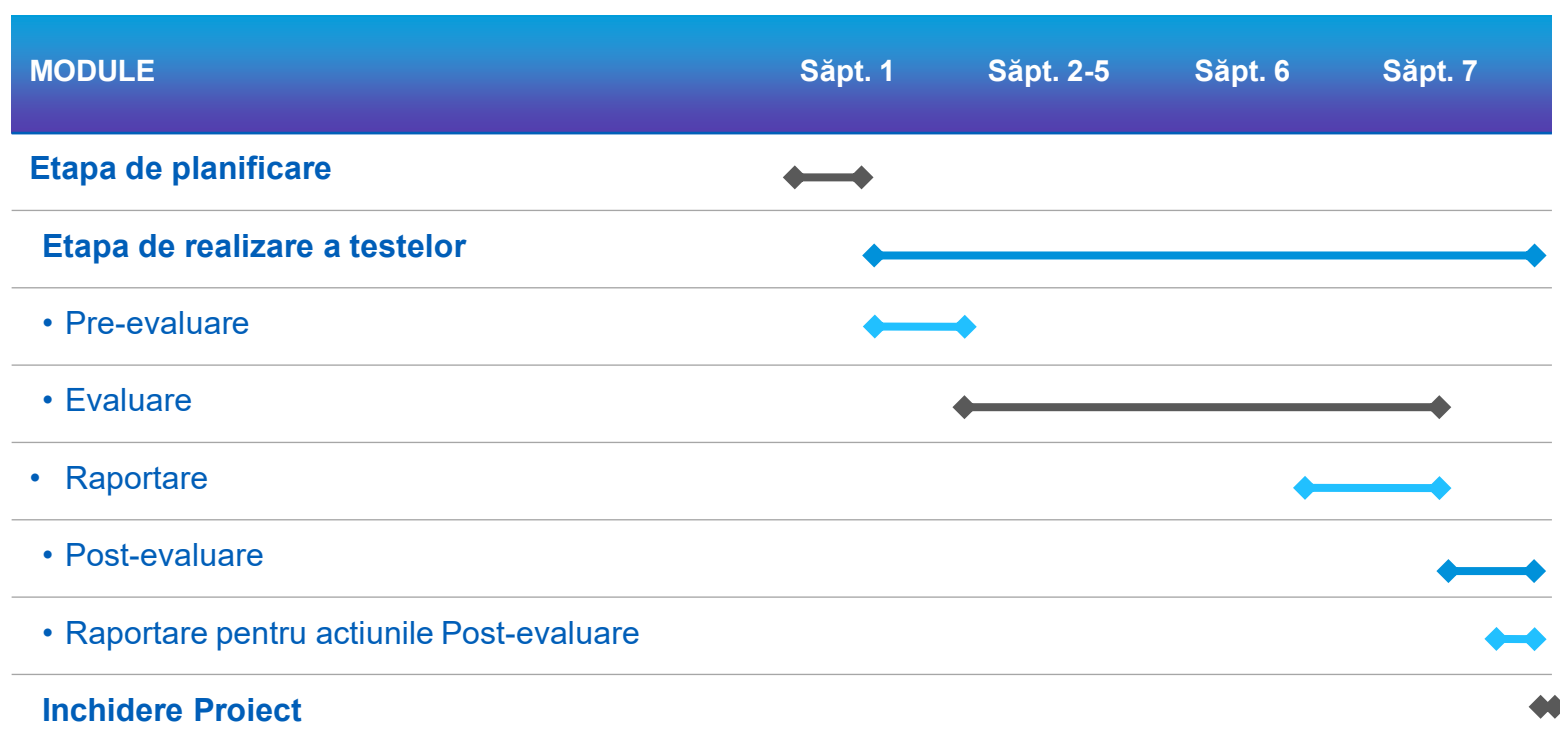
- Sumar executiv;
- Obiectivele și scopul evaluării;
- Prezentarea metodologiei utilizate în cadrul testării;
- Descrierea contextului în care s-a desfășurat testarea;
- Detalii despre rețeaua și sistemele evaluate :
 - o echipamentele și serviciile active (adrese IP, porturi deschise, protocoale utilizate, etc.)
 - o Tipul, versiunea, statusul actualizărilor aplicațiilor
 - o Sistemul de operare
- Prezentarea individuală a vulnerabilităților descoperite, după cum urmează:
 - o descrierea vulnerabilității;
 - o catalogarea vulnerabilității;
 - o descrierea tehnică;
 - o analiza severității și probabilității;
 - o calcularea riscului;
 - o contramăsuri recomandate pentru remediere.
- Alte detalii și recomandări;
- Anexa cu lista testelor de securitate efectuate.

Recomandările de remediere a problemelor și vulnerabilităților identificate vor cuprinde cele mai bune acțiuni/măsuri/metode ce trebuie întreprinse/luate/folosite pentru eliminarea sau micșorarea riscului generat de problemele și vulnerabilitățile detectate, precum și, recomandări și propuneri de implementare ale acestora.

Planul de proiect

Planul de proiect (estimat) este prezentat mai jos. Data exactă a începerii pentru fiecare activitate va fi convenită ulterior cu Dvs., odată ce procesul de contractare va fi finalizat.

Planificarea prezentată aici are caracter informativ și va depinde de data de începere, precum și de capacitatea BNM de a vă furniza la timp acces la sistemele informatice și/ sau informațiile solicitate sau de alți factori (precum evoluția pandemiei COVID-19).





Contact:

Gabriel Mihai Tănase

CISA, CRISC, CGEIT, OPST, MCSE Security

Partener, Tehnologie și Securitate Cibernetică

KPMG in Romania & Moldova
DN.1 Bucuresti-Ploiesti nr. 69-71
Sector 1, Bucuresti 013685, Romania
Tel +40 372 377 800
Fax +40 372 377 700
Mobile +40 747 333 025
E-mail mtanase@kpmg.com

kpmg.com/romania



Această propunere este formulată de KPMG Advisory SRL, o societate cu răspundere limitată de drept român, membră a organizației globale KPMG, compusă din societăți membre independente afiliate KPMG International Limited, societate privată engleză cu răspundere limitată la garanții, și este în toate privințele supusă negocierii, acceptării și semnării unei scrisori de angajament sau a unui contract.

Furnizarea serviciilor incluse în această propunere este condiționată de finalizarea cu un rezultat satisfăcător a procedurilor obligatorii de acceptare a clientilor și a altor proceduri de management al riscului incluzând (i) identificarea oricăror posibile conflicte de interese care ne-ar putea împiedica să prestăm aceste servicii.

KPMG International nu prestează servicii pentru clienți. Nicio firmă membră nu are autoritatea de a obliga sau a ține obligată KPMG International sau orice altă firmă membră față de terțe părți, așa cum nici KPMG International nu are vreo asemenea autoritate de a obliga sau a ține obligată vreo firmă membră.

