“Oferta pentru servicii de evaluare şi de analiză a asigurării calităţii sistemelor (servicii de testare a securitatii sistemului informatic al BNM)

Ofertant: SC SAFETECH INNOVATIONS S.R.L.
Adresa sediu social: Str. Frunzei nr. 12-14, etaj 1 si 2, sector 2, Bucuresti
Tel/Fax: +4 021 316 05 65, **E-mail:** office@safetech.ro

Persoana de contact: Alin Valentin DRAGAN
Tel: +40 722 283 481, **E-mail:** alin.dragan@safetech.ro

Digitally signed by Odobescu Viorica
Date: 2019.12.13 11:54:06 EET
Reason: MoldSign Signature
Location: Moldova

1. SUMAR EXECUTIV SI IPOTEZE DE LUCRU

SAFETECH INNOVATIONS a citit caietul de sarcini, a inteles obiectivele proiectului si a conturat modul in care le va realiza.

In acest context, obiectivul principal al prezentei propuneri tehnice si financiare a SAFETECH INNOVATIONS (Prestator) este acela de a inainta si a supune atentiei Bancii Nationale a Moldovei (BNM) in calitate de Beneficiar un raspuns privind cererea de oferta pentru ***"Servicii de evaluare şi de analiză a asigurării calităţii sistemelor (servicii de testare a securitatii sistemului informatic al BNM)".***

In cazul in care este desemnat castigator al acestei licitatii, conform criteriilor mentionate in Caietul de Sarcini, SAFETECH INNOVATIONS este de acord sa se angajeze printr-un contract cadru pentru realizarea serviciilor de tip ethical hacking conform cerintelor Beneficiarului si va desemna un manager de proiect pentru gestionarea relatiilor contractuale.

Securitatea IT nu este o tinta absoluta, prin urmare nici o organizatie nu poate fi securizata in mod absolut. Intotdeauna pot fi luate masuri suplimentare pentru a imbunatati securitatea unei organizatii si pentru a minimiza riscurile induse de bresele de securitate. In plus, in fiecare zi se descopera vulnerabilitati noi sau se rezolva alte vulnerabilitati.

Un sistem informatic securizat nu este rodul unui accident. Sistemele securizate nu sunt produsele modificarilor, adaugarilor intamplatoare la functionalitatile acestora. Sistemele informatice securizate sunt fundamentate pe o solida cunoastere a modului in care acestea functioneaza, pe politici si proceduri solide, pe practicile si standardele din industrie si pe un management coerent si eficient

Sistemele informatice sunt amenintate atat din interior cat si din exterior. Pot fi persoane bine intentionate care fac erori de operare, sau persoane rau intentionate, care isi pun in valoare cunostintele si resursele intr-un mod negativ, pentru penetrarea sistemelor informatice. Orice retea poate fi insa penetrata avand la dispozitie suficient timp si resurse.

Secretul prevenirii unei asemenea brese de securitate este de a avea suficiente straturi de securitate si controale, incat atacatorului sa-i fie foarte greu sa-si indeplineasca actiunea si astfel sa renunte.

Ameliorarea securitatii sistemelor informatice trebuie sa fie un obiectiv important al oricarei organizatii. Cu toate acestea, nu toate masurile de securitate reprezinta o investitie eficienta a resurselor IT. Securitatea IT este prin urmare un process continuu de management al riscului, care tinteste sa obtina o balanta intre functionalitate, securitate si cost.

De asemenea, trebuie pastrat un raport corect dintre securitate si disponibilitatea sau accesibilitatea resurselor unei retele informatice, pentru ca o securitate prea riguroasa poate duce la blocarea sau ingreunarea utilizarii unor sisteme sau servicii de retea. Pe de alta parte, lipsa securitatii poate duce de asemenea la aceleasi rezultate.

Trebuie avut in vedere faptul ca securitatea nu se bazeaza numai pe tehnologie. Un drum de „aprovizionare" la un furnizor pentru achizitionarea unui firewall de ultima generatie nu va face reteaua mai sigura in mod necesar. A ne baza doar pe tehnologie este cu siguranta gresit, pentru ca scapam din vedere un element cheie: factorul uman. Sau, mai bine spus, nu ne putem baza intru totul pe tehnologie, pentru ca tehnologia este facuta de oameni – care nu sunt perfecti. De aceea este foarte important sa existe standarde si proceduri, control dual, planuri si proceduri in caz de incidente de securitate sau de dezastre care pot afecta siguranta infrastructurii informatice. Toate acestea contribuie, alaturi de tehnologie, la construirea unei securitati informatice eficiente.

Componentele ofertei sunt prezentate in paginile care urmeaza.

SAFETECH INNOVATIONS isi asuma raspunderea legalitatii utilizarii instrumentelor folosite in cadrul acestui proiect. Marea majoritate a acestor instrumente sunt programe de tip open-source.

Oferta este valabila 35 zile incepand cu 13.12.2019.

2. PREZENTAREA OFERTANTULUI

SAFETECH INNOVATIONS este o companie infiintata in martie 2011, in Romania, pentru a raspunde uneia dintre cele mai mari provocari ale zilelor noastre: necesitatea companiilor si organizatiilor de a-si desfasura activitatea intr-un mediu securizat.
Compania **SAFETECH INNOVATIONS** este lider pe piata serviciilor de securitate a informatiei din Romania si fondatorul, proprietarul si operatorul **Centrului de Monitorizare si Raspuns la Incidente de Securitate, STI CERT**, care functioneaza in regim 24/7. Acesta este un CERT privat recunoscut si acreditat de organisme internationale precum **Trusted Introducer** si **CERT Division of the Software Engineering Institute (SEI)**.
Dorim sa contribuim la crearea viitorului clientilor nostri prin asigurarea unui mediu de lucru securizat si prin oferirea unor avantaje de business care sa-i ajute sa genereze mai departe valoare. Misiunea noastra este de a deveni partenerul potrivit de dumneavoastra pentru a proteja cel mai valoros bun al companiei – informatia si de a stabili relatii de colaborare sanatoase, bazate pe incredere.
Prin profesionalism, solutii practice si eficiente din punctul de vedere al costurilor, **SAFETECH INNOVATIONS** s-a remarcat intr-un timp scurt pe piata Securitatii Informatiei din Romania.
SAFETECH INNOVATIONS este prima si singura companie din Romania si printre putinele din Europa, acreditate de catre NATO pe tema Securitatii Cibernetice. Compania noastra dispune si de urmatoarele certificari NATO:

- **NCAGE Code (NATO Commercial and Goverment Entity Code)**
- **AQAP 2110 - NATO QUALITY ASSURANCE REQUIREMENTS FOR DESIGN, DEVELOPMENT AND PRODUCTION**
- **AQAP 2210 - NATO SUPPLEMENTARY SOFTWARE QUALITY ASSURANCE REQUIREMENTS TO AQAP-2110 OR AQAP-2310**

SAFETECH INNOVATIONS este specializata in furnizarea de servicii privind asigurarea Securitatii Informatiei, dar si in designul, implementarea si monitorizarea infrastructurilor IT.
Experienta ne permite sa oferim un spectru larg de servicii care imbina produse IT si de securitate, tehnologii, standarde si cerinte ale clientilor. In plus, serviciile de tip Ethical Hacking /Penetration Testing/Vulnerability Assessment sunt reprezentative pentru compania noastra si ne-au adus recunoasterea in piata de Securitatea Informatiei din Romania si de peste hotare.
Ca o recunoastere a competentelor pe aceasta tematica, echipa **SAFETECH INNOVATIONS** a fost invitata sa participe si a participat la exercitiile cibernetice organizate de catre **NATO: CYBER COALITION 2019; CYBER COALITION 2018**, **CYBER COALITION 2017, CYBER COALITION 2016, CYBER COALITION 2015** si la **CYBER EUROPE 2016**, organizat de catre **Agentia Uniunii Europene pentru Securitatea Retelelor si a Informatiilor (ENISA).**

De asemenea, **SAFETECH INNOVATIONS** a fost invitata sa participe si a participat la exercitiile cibernetice **CyDex18, CyDex17** organizate de catre **Serviciul Roman de Informatii (SRI)** prin intermediul Centrului National CyberInt, in conformitate cu Strategia de Securitate Cibernetica a Romaniei si in parteneriat cu **MApN, MAI, MAE, STS, SPP, SIE, ORNISS si CERT-RO**.

SAFETECH INNOVATIONS a implementat o serie de proiecte de penetration testing/vulnerability assessment/ethical hacking la peste 15 banci si institutii financiare si de asigurari din Romania si din alte tari din Europa precum: **Banca Nationala a Moldovei**, **BRD - Groupe Société Générale, Banca Comerciala Romana (BCR) Raiffeisen Leasing, Raiffeisen Bank, OTP Bank, First Bank, ING Shared Business BV Amsterdam – Bucharest Branch, Alpha Bank, Alpha Finance, ING Life Assurance, OTP Bank, Idea Bank, Libra Bank, Garanti Bank, Legal & General, Volksbank,** etc.

Totodata, **SAFETECH INNOVATIONS** a fost acreditata drept **Furnizor Oficial de servicii de Penetration Testing** pentru **Raiffeisen Bank International Group, BRD - Groupe Société Générale ING Shared Business BV Amsterdam – Bucharest Branch** si **UNIQA ASIGURARI S.A**.

De asemenea, **SAFETECH INNOVATIONS a efectuat** o serie de proiecte de ethical hacking, audit de securitate, audit de risc si analiza vulnerabilitatilor, standarde de securitate, monitorizarea incidentelor de securitate, scanare si analiza de vulnerabilitate pentru pentru o serie de clienti foarte importanti din Romania dar si de peste hotare precum: **ArcelorMittal** (Luxemburg), **World Customs Organizations** (Belgia), **Electrica S.A., ApaNova Bucuresti S.A.,** etc.

Totodata, **SAFETECH INNOVATIONS este una dintre cele patru companii din lume si prima din Europa Centrala si de Est** acreditata pentru **"Global Professional Services"** de catre HID Global, liderul mondial in furnizarea solutiilor pentru controlul si securitatea accesului.

SAFETECH INNOVATIONS este singura companie ce activeaza exclusiv in domeniului securitatii informatiei din Romania, acreditata de Check Point ca **Check Point's Certified Collaborative Support Provider (CCSP)**. Check Point Software Technologies Ltd. este unul dintre cei mai mari furnizori de solutii de securitate de varf la nivel global. Compania care protejaza peste 100.000 de organizatii de toate dimensiunile, este recunoscuta pentru rata crescuta de detectare a malware-urilor si

a altor tipuri de atacuri si de asemenea, pentru capacitatea de a oferi o arhitectura de securitate completa, care poate securiza intreaga companie de la retea la dispozitive mobile.

Ne adresam celor trei obiective de securitate dintr-o organizatie (confidentialitate, integritate si disponibilitate) pentru informatiile si bunurile importante catre toate nivelele: procese, proceduri, aplicatii, sisteme, retea si infrastructura. Oferim o gama larga de servicii ce se adreseaza produselor diversificate de securitate si IT, tehnologiilor si cerintelor de servicii si standarde ale oricarui client asigurand astfel:

- Reducerea costurilor operationale asociate securitatii informatiei.
- Reducerea semnificativa a riscurilor de securitate.
- Un Return on Security Investment (ROSI) crescut.
- Solutii de securitate eficiente din punct de vedere al costurilor
- Interactiunea cu un singur partener ce acoperta toate aspectele securitatii informatiei.

De ce este SAFETECH INNOVATIONS partenerul potrivit si ce ne diferentiza?

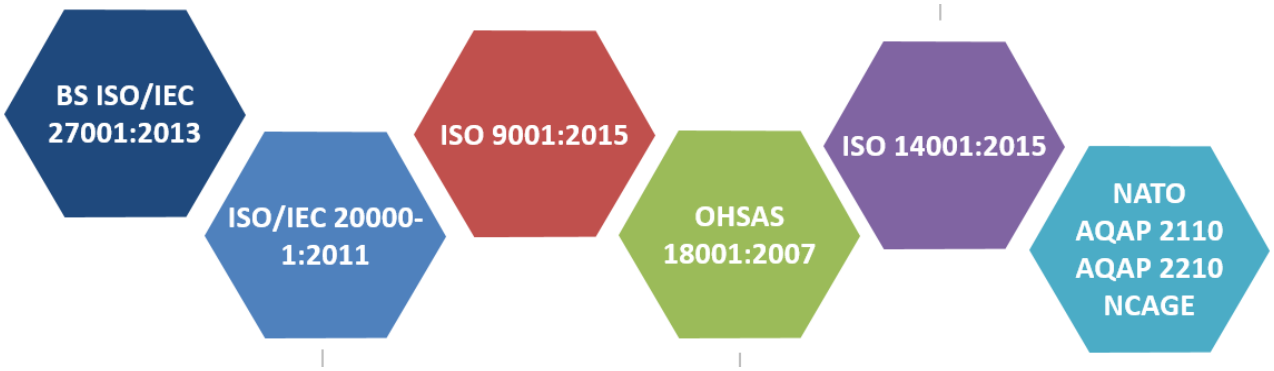
- **Clientii nostri beneficiaza de experienta vasta a unor profesionisti in domeniul securitatii cibernetice.**

  Acoperirea nevoii de securitate a companiilor este unicul scop al activitatii companiei noastre si este domniul in care avem experienta dovedita si dobandita in companii pentru care securitatea inseamna business-ul in sine (secorul bancar ar fi un exemplu).
  Ne-am specializat in identificarea vulnerabilitatilor, in reducerea riscurilor si in creerea programelor de securitate care sa asigure pe termen lung conditiile de care compania are nevoie pentru a se dezvolta.
- **Clientii nostri simt exigenta cu care este condusa compania SAFETECH INNOVATIONS, specifica domeniului securitatii**

  Echipa noastra de management este formata de experti in securitatea informatiilor, fapt care imprima exigenta in privinta calitatii serviciilor livrate. Actionam in domeniul securitatii cibernetice urmand tactici si proceduri specifice. Ne organizam ca o unitate de elita in apararea cibernetica si suntem ghidati de: respect si loialitate, etica si responsabilitate, puterea echipei (includem aici si parteneriatele).
- **Clientii nostri beneficiaza de expetiza in domeniul securitatii cibernetice.**

  Avem know how certificat in ceea ce priveste tehnica de atac si de aparare in domeniul cibernetic si expertiza in ceea ce priveste:
  - **Analiza** amenintarilor si a vulnerabilitatilor existente/potentiale
  - **Evaluarea** riscurilor si al impactului de business
  - **Consultanta** in vederea asigurarii confidentialitatii, integritatii si disponibilitatii informatiilor
  - **Implementarea** solutiilor necesare in vederea realizarii unui nivel optim de securitate, care sa mentina un business sanatos pe termen lung.

Inca din anul 2012, **SAFETECH INNOVATIONS** a obtinut urmatoarele certificari emise de **MOODY INTERNATIONAL si ulterior de Intertek si BUREAU VERITAS**:



- Management System Certified Against **27001:2013** (**ISO/IEC 27001**) - Standardul care reglementeaza politicile si procedurile de securitate la nivel de organizatie sau unitate functionala; astfel se atesta ca organizatia a implementat un sistem standardizat de management al securitatii
- Management System Certified Against **20000:2011** (**ISO/IEC 20000**) - Standardul international pentru managementul serviciilor IT, atat interne, cat si externe.
- Management System Certified Against **9001:2015** (**ISO 9001**) - Certificarea care stabileste standardele pentru sistemul de management al calitatii, dar si pentru sistemul de management, in general.
- Management System Certified Against **OHAS 18001:2007 -** Certificarea care demonstreaza orientarea companiei catre un mediu de lucru sigur prin integrarea sigurantei muncii in toate procesele existente, precum si protejarea angajatilor impotriva accidentelor de munca.
- Management System Certified Against **14001:2015** (**ISO 14001**) - Standardul care specifica procesele necesare pentru controlul si imbunatatirea actiunilor companiei cu privire la mediul inconjurator.

Personalul tehnic al companiei noastre detine urmatoarele certificari:

- **C|EH** - Certified Ethical Hacker (EC-COUNCIL)
- **LPT** - Licensed Penetration Tester (EC-COUNCIL)
- **ECSA** - EC Council Certified Security Analyst
- **OSCP** - Offensive Security Certified Professional (Offensive Security)
- **OSWP** – Offensive Security Wireless Professional (Offensive Security)
- **QUALYSGuard** - Qualys Guard Certified Specialist – Vulnerability Management
- **GISCP** - Global Industrial Cyber Security Professional
- **CSSA** – Certified SCADA Security Architect
- **CSSLP** – Certified Secure Software Lifecycle Professional (ISC2)
- **CISSP** – Certified Information Systems Security Professional (ISC2)
- **CISA** - Certified Information Systems Auditor (ISACA)
- **CISM** - Certified Information Security Manager
- **CIPP/IT** - Certified Information Privacy Professional/Information Technology
- **CPSSE** - Certified Professional for Secure Software Engineering
- **CompTIA Security+**
- **CompTIA Linux+**

Cativa dintre clientii nostri:


PUBLIC ADMINISTRATION
ANAF
Agenția Națională de Administrare Fiscală
ANCOM
Autoritatea Națională pentru Administrare și Reglementare în Comunicații
ROMÂNIA
AGENȚIA NAȚIONALĂ DE INTEGRITATE
ROMÂNIA
MINISTERUL JUSTIȚIEI
CNADNR
FINANCE-BANKING INSURANCE
TRANSFOND
Raiffeisen BANK
Reusim impreună.
BRD
GROUPE SOCIETE GENERALE
ING
BCR
ALPHA BANK
ING
ASIGURĂRI DE VIAȚĂ
Banca Națională a Moldovei
FIRSTBANK
otpbank
Avem încredere
Bancpost
UNIQA
Idea Bank
CRÉDIT AGRICOLE
VIG
VIENNA INSURANCE GROUP
Gothaer
CRITICAL INFRASTRUCTURES ENERGY / UTILITIES
APA NOVA
BUCUREȘTI
Member of VEOLIA
INFORMATICĂ FEROVIARĂ
electrica
s.a.
ArcelorMittal
TAROM
enisa
romstal
UNIVERSUL INSTALAȚIILOR
Kandia Dulce
World Customs Organization
Organisation Mondiale des Douanes
MEDICAL /GDPR
synevo
romstal
UNIVERSUL INSTALAȚIILOR
INSTITUTUL NAȚIONAL DE BOLI INFECȚIOASE
"PROF. DR. MATEI BALȘ"
Spitalul Monza
Standarde de Excelență
Dosarul Electronic de Sănătate
Pro Estetica

2.1. PROIECTE SIMILARE

SAFETECH INNOVATIONS a implementat o serie de proiecte de penetration testing/vulnerability assessment/ethical hacking la peste 15 banci si institutii financiare si de asigurari din Romania si din alte tari din Europa, la institutii publice, institutii de importanta statala, etc. Amintim cativa dintre clientii importanti:

Autoritatea Nationala pentru Administrare si Reglementare in Comunicatii

- Evaluare a vulnerabilitatilor informatice prin teste specifice de penetrare din interiorul si exteriorul infrastructurii de comunicatii, cu urmatoarele livrabile:
  - Plan de proiect
  - Plan de testare
  - Plan de actiuni (SOW - State of Work)
  - Raport de testare securitate aplicatie web
  - Raport analiza securitate aplicatie web
  - Audit report

Compania Nationala de Transporturi Aeriene Romane - TAROM SA

- Evaluare a Starii Securitatii Informatiei in Sistemele si Infrastructura IT

Raiffeisen Bank – contract cadru

- Testare de penetrare a aplicatiilor online si mobile Banking precum si a tuturor aplicatiilor expuse in internet – (operatiune efectuata periodic)
- Testare de penetrare pentru infrastructura expusa in Internet– (operatiune efectuata periodic)

BRD - Groupe Société Générale – contract cadru

- Testare de penetrare anuala a aplicatiilor de online si mobile Banking precum si a tuturor aplicatiilor expuse in Internet - (operatiune efectuata periodic)
- Testare de penetrare anuala pentru infrastructura interna si *core banking* (operatiune efectuata periodic)

ING Shared Business BV Amsterdam – Bucharest Branch – contract cadru

- Testare de penetrare a aplicatiilor online si mobile Banking precum si a tuturor aplicatiilor expuse in internet – (operatiune efectuata periodic)

OTP Bank – contract cadru

- Testare de penetrare anuala a aplicatiilor de online si mobile Banking precum si a tuturor aplicatiilor expuse in Internet – (operatiune efectuata periodic)
- Testare de penetrare anuala pentru infrastructura expusa in Internet (operatiune efectuata periodic)

Alpha Bank – contract cadru

- Testare de penetrare anuala a aplicatiilor de online si mobile Banking precum si a tuturor aplicatiilor expuse in Internet – (operatiune efectuata periodic)
- Testare de penetrare anuala pentru infrastructura expusa in Internet (operatiune efectuata periodic)

Banca Comerciala Romana (BCR) – Membru Erste Group

- Testari de penetrare periodice ale aplicatiilor de online si mobile Banking precum si a tuturor aplicatiilor expuse in Internet – (operatiune efectuata periodic)
- Testare de penetrare anuala pentru infrastructura expusa in Internet (operatiune efectuata periodic)

First Bank

- Testare de penetrare anuala a aplicatiilor de online si mobile Banking precum si a tuturor aplicatiilor expuse in Internet – (operatiune efectuata periodic)
- Testare de penetrare anuala pentru infrastructura expusa in Internet (operatiune efectuata periodic)

Arcelor Mittal Europe Group – contract cadru

- Testare de penetrare periodica pentru aplicatiile si infrastructurile expuse in Internet (operatiune efectuata periodic)

ApaNova Bucuresti – membru Veolia Group

- Testare de penetrare periodica pentru aplicatiile si infrastructurile expuse in Internet (operatiune efectuata periodic)

World Customs Organizations

- Testare de penetrare periodica pentru diverse aplicatii si infrastructuri expuse in Internet (operatiune efectuata periodic)

Libra Bank

- Testare de penetrare a aplicatiilor online si mobile Banking precum si unor aplicatii expuse in Internet

Raiffeisen Leasing

- Testare de penetrare a aplicatiilor online

ING Life Assurance

- Testare de penetrare a aplicatiilor online

Idea Bank

- Testare de penetrare a aplicatiilor online

Totodata, compania SAFETECH INNOVATIONS a fost acreditata drept Furnizor Oficial de servicii de Penetration Testing pentru Raiffeisen Bank International Group si pentru Banca Comerciala Româna (BCR – membru ERSTE GROUP).

Pentru Electrica S.A. si ApaNova Bucuresti S.A.– testari de penetrare periodice in infrastructura critica.

De asemenea, SAFETECH INNOVATIONS a implementat o serie de proiecte de penetration testing/vulnerability assessment/ethical hacking, audit de securitate, audit de risc si analiza vulnerabilitatilor, standarde de securitate, monitorizarea incidentelor de securitate, scanare si analiza de vulnerabilitate pentru o serie de clienti foarte importanti din Romania dar si de peste hotare precum: ArcelorMittal (Luxemburg), World Customs Organizations (Belgia), Electrica S.A., ApaNova Bucuresti S.A., SIVECO Romania S.A. etc.

Va putem pune la dispozitie recomandari si referinte despre proiectele in care am fost implicati.

3. DESCRIERE ABORDARI, METODOLOGII, TEHNICI SI STANDARDE

3.1. DESCRIERE SERVICII IDENTIFICARE SI EVALUARE DE VULNERABILITATI

Serviciile de tip “Ethical Hacking” cuprind teste de penetrare, care reprezinta simularea unor atacuri informatice din perspectiva unui hacker asupra unei retele, sistem, aplicatie sau site web. In efectuarea acestui test se vor folosi metode si tehnici folosite de hackeri pentru a descoperi vulnerabilitatile si slabiciunile sistemului tinta.

Testul de penetrare va evalua nivelul de securitate al aplicatiei din perspectiva asigurarii confidentialitatii, integritatii si disponibilitatii informatiilor gestionate. Vor fi evaluate si nivelele de securitate ale componentelor de retea si server care asigura protectia aplicatiei.

In urma testarii, se va livra un raport detaliat in care se vor prezenta toate vulnerabilitatile si riscurile de securitate descoperite, impreuna cu recomandari pentru rezolvarea lor.

Analiza cuprinde atat identificarea vulnerabilitatilor cunoscute folosind unelte de scanare automate, cat si atacuri manuale personalizate pentru specificul sistemului tinta corelate cu listele de vulnerabilitati top ten OWASP, top twenty SANS. Atacurile de la nivelul retelei pot fi corelate cu cele de la nivelul aplicatiei pentru generarea unor scenarii complexe. Testele de penetrare pot fi efectuate din exterior, utilizand toate nivelurile de privilegii disponibile in sistem, dar fara a cunoaste detalii privind arhitectura sistemului informatic (teste de tip-ul “blackbox”).

3.1.1 Metodologii privind identificarea si evaluarea vulnerabilitatilor

Tehnicile utilizate in identificarea si evaluarea vulnerabilitatilor se bazeaza pe cele mai bune practice in domeniu la nivel international:

- National Institute of Standards and Technology – NIST;
- Open Source Security Testing Methodology – OSSTM;
- Open Information Systems Security Group - OISSG;
- Open Web Application Security Project – OWASP;
- Information Systems Audit and Control Association – ISACA
- Information Systems Security Assessment Framework ISSAF

3.1.2 Etape pentru desfasurarea serviciilor de evaluare:

- Pre-assessment
- Assessment
- Post-assessment

- Follow –up

Pre-assessment

Reprezinta faza premergatoare identificarii si evaluarii vulnerabilitatilor si este importanta pentru determinarea specificatiilor precise si regulilor de desfasurare a testelor.
In aceasta etapa se va defini si agrea un contract de confidentialitate, se vor stabili scenariile de atac si se vor obtine autorizatiile necesare desfasurarii testului de penetrare.

Definirea domeniului de evaluare

La initierea proiectului, impreuna cu beneficiarul, se va delimita aria de acoperire a domeniului de evaluare.

Se vor stabili modalitatile de simulare a atacurilor:
- blackbox (fara a avea nici un fel de date despre obiectul auditat);
- whitebox/greybox (avand la dispozitie unele informatii despre sistemul tinta).

In vederea obtinerii unor rezultate optime, se recomanda corelarea rezultatelor din ambele modalitati de analiza.

Stabilirea nivelului de agresivitate al atacului: cat de departe se va merge cu tentativele de exploatare a unei vulnerabilitati.

Colectare informatii publice disponibile despre sistemul informatic al companiei.

Informatiile continute pe site-ul companiei, informatii continute in inregistrarile Whois, DNS, RNC;
Informatii despre sistemul informatic al companiei ce se pot obtine din alte surse.

Assesment

Reprezinta etapa de identificare si evaluare a vulnerabilitatilor.

Etapele de desfaurare includ evaluarea conectivitatii intre sistemele utilizate pentru test si sistemele testate, culegerea de informatii despre sistemele testate din domeniul

public si privat, descoperirea sistemelor si serviciilor active si scanarea sistemelor pentru descoperirea vulnerabilitatilor.

Utilizand informatiile descoperite in evaluarea vulnerabilitatilor, se vor construi arbori de atac (attack trees) si se vor implementa actiunile din aceste structuri.

Scanarea vulnerabilitatilor si implementarea testului de penetrare va include in mod minimal analiza urmatoarelor vulnerabilitati ale aplicatiilor web:

- Verificarea input-ului utilizatorului
- Controlul accesului
- Cross Site Scripting (XSS)
- Buffer overflow
- Tratarea erorilor
- Injectare de cod arbitrar
- Criptarea si stocarea informatiei in executia aplicatiei
- Erori de configurare a aplicatiei
- Comportamentul aplicatiei la un atac de tip Denial of Service (DoS)

Scanarea vulnerabilitatilor si implementarea testului de penetrare la nivelul retelei va include in mod minimal:

- Obtinerea informatiilor din domeniul public
- Scanarea sistemelor din SOW
- Tehnici de enumerare
- Obtinerea accesului neautorizat prin exploatarea vulnerabilitatilor
- Consolidarea accesului
- Stergerea tuturor fisierelor utilizate in cadrul atacului si a altor dovezi ale accesului

Aplicatii software si resurse hardware utilizate:

- Aplicatii pentru culegerea de informatii din domeniul public;
- Aplicatii necesare identificarii sistemelor si serviciilor active;
- Scannere de vulnerabilitati specifice sistemelor si retelelor incluse in SOW;
- Aplicatii necesare exploatarii vulnerabilitatilor descoperite.

Resurse necesare:

Disponibilitatea unei persoane de contact pentru notificari de urgenta in cazul descoperirii unor vulnerabilitati critice sau comportari anormale a sistemului testat.

Post –assesment

Reprezinta etapa de analiza a rezultatelor descoperite in etapa Assessment.

Aceste rezultate vor fi detaliate intr-un raport care va cuprinde:

- Sumar Executiv;
- Obiectivele si scopul evaluarii;
- Prezentare succinta a metodologiei utilizate;
- Descrierea contextului in care s-a desfasurat evaluarea;
- Prezentarea individuala a vulnerabilitatilor descoperite dupa cum urmeaza:
    - descrierea vulnerabilitatii;
    - catalogarea vulnerabilitatii;
    - descrierea tehnica;
    - analiza severitatii si probabilitatii
    - calcularea riscului;
    - contramasuri recomandate pentru remediere;
- Alte detalii si recomandari;
    - Anexa cu lista testelor de securitate efectuate;

Follow-up

Reprezinta etapa de verificare si confirmare a inlaturarii riscurilor semnalate in etapele precedente, dupa ce Beneficiarul implementeaza masurile mentionate in raportul de test.

3.1.3 Metodologie calcul nivel risc

Riscul reprezinta probabilitatea ca o anumita amenintare-sursa sa exploateze o vulnerabilitate, precum si impactul acelui eveniment asupra organizatiei sau sistemului respectiv.

NIVEL RISC	VALOARE	MASURI NECESARE
MAXIM	**75 – 100**	Actiune imediata pentru reducerea nivelului de risc.
CRITIC	**25 – 74**	Implementare de masuri corective cat mai curand posibil.
MEDIU	**5 - 24**	Implementare de masuri corective intr-o perioada rezonabila de timp.
SCAZUT	**2 - 4**	Pot fi implementate anumite masuri corective sau se accepta riscul.
INFORMATIONAL	**1**	Reprezinta o observatie care nu determina un risc de securitate.

Nivelul de risc pentru fiecare vulnerabilitate este calculat folosind urmatoarea formula:

NIVEL RISC = VALOARE SEVERITATE (IMPACT) x VALOARE PROBABILITATE

VALOARE SEVERITATE (IMPACT TEHNIC)
Impactul negativ asupra informatiei gestionate de aplicatie si sistem, pierdere sau degradare sau o combinatie a acestora a urmatoarelor obiective ale securitatii: integritate, disponibilitate, confidentialitate.

NIVEL	SCOR	DESCRIERE
SCAZUT	**1 – 5**	Afectarea limitata a informatiilor sau sistemului; obtinerea de informatii utile pentru generarea unor atacuri.
MEDIU	**6 – 14**	Afectarea semnificativa a informatiilor sau sistemului; pierdere de informatii,

		indisponibilitate serviciu; acces limitat la sistem.
SEVER	**15 - 20**	Pierderi foarte importante ale informatiei, acces nelimitat la sistem; prejudicii la nivelul organizatiei

VALOARE PROBABILITATE

Probabilitatea ca o anumita vulnerabilitate sa fie exploatata de catre un atacator. La calcularea probabilitatii se are in vedere: motivatia atacatorului, nivelul de cunostinte necesar, usurinta in detectare si exploatare a vulnerabilitatii, nivelul de acces necesar si existenta unor masuri de detective si prevenire.

NIVEL	SCOR	DESCRIERE
FOARTE MICA	**1**	Vulnerabilitatea nu este direct exploatabila
MICA	**2**	Vulnerabilitatea necesita un efort semnificativ si cunostinte avansate pentru a fi exploatata manual. Atacatorul ar putea avea nevoie de acces si cunostinte interne ale sistemului.
MEDIE	**3**	Vulnerabilitatea necesita cunostinte specifice si poate fi exploata cu instrumente disponibile public.
MARE	**4**	Vulnerabilitatea necesita anumite cunostinte si poate fi exploata fara instrumente speciale sau foarte usor de gasit si utilizat.
FOARTE MARE	**5**	Vulnerabilitatea necesita cunostinte foarte putine si poate fi exploata fara instrumente speciale.

Livrabile:

- Plan de proiect detaliat;
- Plan de testare
- Planul de actiuni;
- Raport de testare

Rapoartele furnizate 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 (cel puțin diagrame, grafice sau harți). Partea tehnică va detalia din punct de vedere tehnic problemele și vulnerabilitățile identificate.

Partea tehnică va conține cel puțin următoarele capitole:

- Sumar executiv;
- Obiectivele și scopul evaluării;
- Prezentare succintă a metodologiei utilizate în cadrul testării;
- Descrierea contextului în care s-a desfășurat testarea;
- Prezentarea individuală a vulnerabilităților descoperite, după cum urmează:
    - descrierea vulnerabilității;
    - catalogarea vulnerabilității;
    - descrierea tehnică;
    - analiza severității și probabilității;
    - calcularea riscului;
    - 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.

Cerinte minime acoperite:

Identificarea și evaluarea vulnerabilităților informatice vor adresa cel puțin următoarele concepte și tipuri de atac:

- RFI – Remote File Inclusion;
- LFI – Local File Inclusion;
- XSS – Cross Site Scripting;
- HTTP Header Injection;
- SQL Injection;

- LoginByPass – evitarea autentificării;
- Arbitrary File Upload;
- Remote Code and Command Execution;
- Full Path Disclosure;
- Metodele nesigure de utilizare a cookie-urilor;
- Cross Site Request Forgery;
- Directory Traversal;
- HTTP Parameter Pollution;
- Script Source Code Disclosure;
- CRLF Injection;
- XFS - Cross Frame Scripting;
- PHP Code Injection;
- XPath Injection;
- LDAP Injection;
- Email Injection;
- Arbitrary File Creation;
- File Tampering;
- Remote XSL Inclusion;
- MultiRequest Parameter Manipulation;
- Input Validation;
- Buffer Overflows;
- Unrestricted File Uploads.

Vor fi descoperite eventualele vulnerabilităţi de securitate existente cel puțin în cadrul:

- Paginilor Web caracteristice protocoalelor SSL/TLA;
- Paginilor Web caracteristice protocolului HTTPS;
- Paginilor Web care să adreseze conceptul de Directory Checks;
- Paginilor Web care să adreseze conceptul de Text Search;
- Aplicaţiei OWA – Outlook Web Application;
- Reţelelor de comunicaţii legate de protocolul SNMP;
- Rețelelor de comunicații legate de protocolul TCP/IP;
- Rețelelor de comunicații legate de protocolul LDAP;
- Rețelelor de comunicații legate de tehnologia DNS;
- Rețelelor de comunicații legate de protocolul TELNET;
- Rețelelor de comunicații legate de protocolul SSH;
- Rețelelor de comunicații legate de metodele de autentificare utilizate – weak passwords, default passwords, etc;
- Rețelelor de comunicații legate de protocolul ARP;
- Rețelelor de comunicații legate de protocolul UDP;
- Rețelelor de comunicații legate de protocolul SMTP;
- Rețelelor de comunicații legate de protocolul FTP;
- Rețelelor de comunicații legate de funcționalitățile NetBIOS;

- Reţelelor de comunicații legate de funcționalitățile Microsoft RDP.

Alte vulnerabilități vor fi evidențiate prin:

- Analiza sintaxei parolelor și a posibilelor puncte slabe ale acestora (Weak Password Check) – weak HTTP password, authentication attacks, weak FTP passwords;

- Scanarea porturilor/rețelei – Open Ports on Servers, Network Banner of port, DNS Server Vulnerability – Open Zone Transfer, Open Recursion, Cache Poisoning, List of writable FTP Directories, FTP Anonymous Access Allowed, Badly Configured Proxy Servers, Weak SNMP Community Strings, Weak SSL Cyphers);

Soluția propusă va identifica cel puțin majoritatea vulnerabilităților prezente în următoarele baze de date: CVE (Common Vulnerabilities and Exposures), CWE (Common Weakness Enumeration), CCE (Common Configuration Enumeration), Bugtraq (SecurityFocus).

3.2. DESCRIERE SERVICII DE PENETRATION TESTING

Serviciile de tip “Ethical Hacking” cuprind teste de penetrare care simuleaza atacuri informatice din perspectiva unui hacker asupra unei retele, sistem, aplicatie sau site web. In efectuarea acestui test se vor utiliza metode si tehnici folosite de hackeri pentru a descoperi vulnerabilitatile si slabiciunile sistemului tinta.

Testul de penetrare va evalua nivelul de securitate din perspectiva asigurarii confidentialitatii, integritatii si disponibilitatii informatiilor gestionate.

Analiza cuprinde atat identificarea vulnerabilitatilor cunoscute folosind unelte de scanare automate, cat si atacuri manuale personalizate pentru specificul sistemului tinta, corelate cu listele de vulnerabilitati TOP 10 OWASP, TOP 20 SANS. Atacurile de la nivelul retelei pot fi corelate cu cele de la nivelul aplicatiei pentru generarea unor scenarii complexe.

In functie de nivelul initial de cunostinte asupra sistemului/aplicatiei tinta, expertii SAFETECH INNOVATIONS pot utiliza in cadrul testelor de penetrare 3 abordari principale:

• **BLACKBOX:** Intr-un test de penetrare de tip BlackBox se efectueaza evaluarea de securitate fara nici o cunostinta despre sistemele sau aplicatiile in scop.

• **WHITEBOX:** Intr-un test de penetrare de tip WhiteBox sunt puse la dispozitia expertilor SAFETECH INNOVATIONS informatii detaliate despre sistemele sau aplicatiile in scop.

• **GREYBOX:** O combinatie dintre cele doua tipuri amintite mai sus, in care se simuleaza un atacator cu anumite cunostinte despre infrastructura Beneficiarului, dar care e un utilizator neprivilegiat, sau care nu are drepturi in sistemul tinta, acesta trebuind sa reuseasca o escaladare a privilegiilor pentru a reusi un atac.
In urma testarii, se va livra un raport detaliat in care se vor prezenta toate vulnerabilitatile si riscurile de securitate descoperite, impreuna cu recomandari pentru rezolvarea lor.

70% din activitatea de testare este realizata manual iar 30% automat (cu ajutorul tool-urilor de testare) urmarind urmatoarele aspecte:

- ***Testele automate*** identifica erori de programare, probleme de configurare, lipsa aplicarii update-urilor de securitate la nivelul sistemelor de operare sau tool-urilor care stau la baza rularii diverselor aplicatii, cu ajutorul unor programe specializate (vulnerability scanners, fuzzers, code scanners, etc).

- ***Testele manuale*** analizeaza aspecte ale aplicatiilor care necesita intuitia si interventia umana si abilitatea de a combina cunostinte din mai multe domenii, pentru a identifica Vulnerabilitati care nu pot fi descoperite folosind programe automate de testare.

3.2.1 Teste de penetrare pentru aplicatii Web

Testarea de securitate la nivelul aplicatiilor web este realizata in concordanta cu metodologia OWASP, certificata la nivel mondial.
Atacurile din planul de testare vizeaza in principal urmatoarele aspecte:

- Testarea mecanismelor de pastrare a confidentialitatii si integritatii datelor
- Testarea procesului de Management al Identitatii
- Testarea mecanismelor de Management al configuratiilor
- **Testarea mecanismelor de Autentificare**
- Testarea mecanismelor de Autorizare
- Testarea mecanismelor de Management al Sesiunilor
- Testarea mecanismelor de Validare a Datelor
- Testarea mecanismelor de management al Exceptiilor (erorilor)
- Testarea mecanismelor Criptografice
- Testarea problemelor de Logica de Business

3.2.2 Teste de penetrare infrastructura IT si WiFi

Testarea securitatii la nivel de infrastructura IT are ca scop obtinerea unei perspective asupra daunelor potentiale si a riscului de business pe care vulnerabilitatile existente le-ar putea provoca.
Testarea de securitate la nivel de infrastructura va include in mod minimal:

- Obtinerea informatiilor din domeniul public
- Scanarea sistemelor din scop
- Tehnici de enumerare
    - Identificarea sistemelor de operare
    - Identificarea patch-urilor de securitate lipsa pe un anumit sistem de operare
    - Determinarea vulnerabilitatilor cunoscute la nivelul sistemelor de operare
    - Identificarea tuturor porturilor deschise
    - Identificarea serviciilor care ruleaza pe un anumit port
    - Determinarea vulnerabilitatilor cunoscute la nivelul serverelor de aplicatii
    - Determinarea vulnerabilitatilor cunoscute pentru bazele de date
    - Determinarea vulnerabilitatilor cunoscute la nivelul serviciilor active identificate
    - Identificarea problemelor de configurare

- Obtinerea accesului neautorizat prin exploatarea vulnerabilitatilor respectiv a problemelor de configuratie
- Consolidarea accesului
- Stergerea tuturor fisierelor utilizate in cadrul atacului si a altor dovezi ale accesului

Expertii **SAFETECH INNOVATIONS** vor identifica vulnerabilitatile, bazandu-se pe cele mai bune practici in domeniu la nivel international si folosind baze de date precum: CVE (Common Vulnerabilities and Exposures), CWE (Common Weakness Enumeration), CCE (Common Configuration Enumeration), Bugtraq (SecurityFocus).

4.DESCRIEREA MANAGEMENTULUI PROIECTULUI

Întreaga echipă de proiect a SAFETECH INNOVATIONS va fi condusă de un manager de proiect (PM), care va avea responsabilitatea principală în faţa BNM pentru prestarea tuturor serviciilor contractate. Managerul de proiect va avea sprijinul logistic şi metodologic necesar din partea organizației furnizorului.

4.1. SERVICII DE MANAGEMENT DE PROIECT

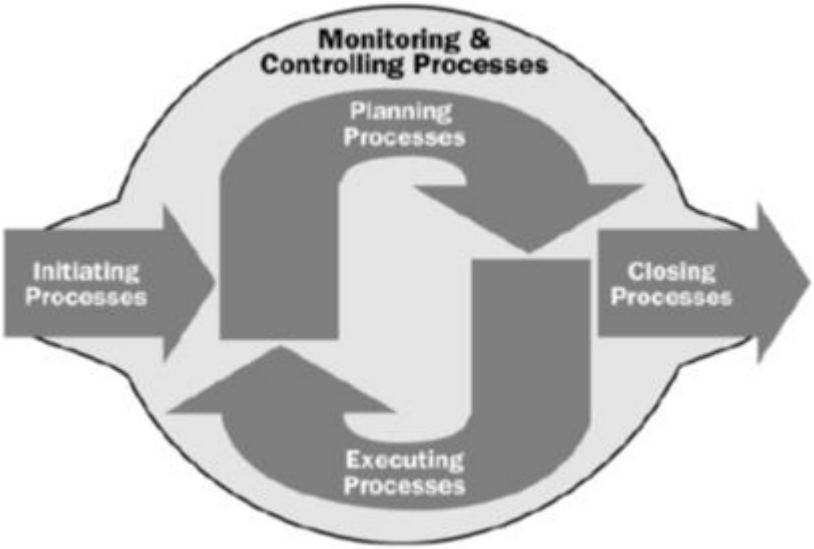
Metodologia de management de proiect utilizata in cadrul acestui proiect este bazata pe standardul PMBOK (Project Management Body of Knowledge: editia 2004) elaborata de Project Management Institute (PMI). PMBOK® Guide este standardul global recunoscut pentru conducerea proiectelor si aprobat ca si American National Standard (ANS) de catre American National Standards Institute (ANSI).

Procedura de Project Management bazata pe aceasta metodologie urmareste principiile generale existente in PMBOK si contine descrierea proceselor, instrumentelor si metodelor folosite in procesul de conducere a proiectelor.

Exista cinci procese majore de management de proiect:

1. **Initierea** este procesul de autorizare formala a unui nou proiect sau de continuare in faza urmatoare a unui proiect existent**;**
2. **Planificare** este procesul prin care se definesc si se rafineaza obiectivele proiectului si se selecteaza cea mai buna cale de atingere a acestora;
3. **Executia** este procesul prin care se coordoneaza oamenii si alte resurse pentru a indeplini obiectivele proiectului;
4. **Monitorizarea si Controlul** sunt procesele prin care se asigura faptul ca obiectivele proiectului sunt indeplinite; acesta lucru se realizeaza prin monitorizarea si masurarea regulata a progresului pentru a identifica variatiile fata de planul de proiect si elaborarea actiunilor corective necesare pentru a mentine proiectul in parametrii aprobati.
5. **Terminarea** este procesul prin care se formalizeaza sfarsitul proiectului sau a fazei. In cadrul acestui proces se formalizeaza terminarea contractelor cu furnizorii sau clientii.

Principale procesele de Project Management si legaturile dintre acestea sunt prezentate in diagrama urmatoare:



O scurta definitie a proceselor de management de proiect este prezentata in continuare:

a. PROCESUL DE INITIERE

Initierea este procesul de autorizare formala a unui nou proiect sau de continuare in faza urmatoare a unui proiect existent.

Rezultate specifice ale acestui proces:

- **Project Charter**
- Constrangeri
- Premise

b. PROCESUL DE PLANIFICARE

Planificarea este procesul prin care se definesc si se rafineaza obiectivele proiectului si se selecteaza cea mai buna cale de atingere a acestora.

Rezultate specifice ale acestui proces:

- **Planul de Proiect (PP)**

c. PROCESUL DE EXECUTIE

Executia este procesul prin care se coordoneaza oamenii si alte resurse pentru a indeplini obiectivele proiectului.

Rezultate specifice ale acestui proces:

- **Rezultatele activitatilor**
- **Livrabile ale proiectului**
- Solicitari de modificare a proiectului
- Rapoarte de stare a proiectului
- Corespondenta

d. PROCESUL DE MONITORIZARE SI CONTROL

Monitorizarea si Controlul sunt procesele prin care se asigura faptul ca obiectivele proiectului sunt indeplinite; acesta lucru se realizeaza prin monitorizarea si masurarea regulata a progresului pentru a identifica variatiile fata de planul de proiect si elaborarea actiunilor corective necesare pentru a mentine proiectul in parametrii aprobati.

Rezultate specifice ale acestui proces:

- **Actualizarea Planului de Proiect**
- Rezultate ale controlului de calitate
- Solicitari de modificare a proiectului
- Actiuni corective
- Lectii invatate

e. PROCESUL DE TERMINARE

Terminarea este procesul prin care se formalizeaza sfarsitul proiectului sau a fazei. In cadrul acestei faze se formalizeaza terminarea contractelor cu furnizorii sau clientii.

Rezultate specifice ale acestui proces:

- **Procesul verbal de acceptanta**
- Sedinta de bilant a proiectului
- Arhivarea proiectului
- Lectii invatate

Management de Proiect si Responsibilitati

Proiectul va necesita eforturi coordonate ale echipei mixte formate din membrii desemnati de Beneficiar şi Ofertant. Administrarea comuna a proiectului este esenţială pentru a asigura succesul proiectului. Se vor folosi templateuri comun agreate pentru a raporta progresul şi pentru a identifica, urmări şi rezolva problemele si riscurile identificate.

Manager de Proiect

Managerii de proiect vor juca rolul de reprezentare în ceea ce priveşte administrarea şi a altor aspecte referitoare la activitatea tehnică a proiectului. Managerii de proiect trebuie să aibă autoritate in propriile organizatii. Responsabilităţile managerului de proiect trebuie să fie clar definite în Planul de Management al Proiectului.

Planul de Proiect

Managerul de proiect al Ofertantului impreuna cu managerul de proiect al Beneficiarului vor superviza dezvoltarea Planului de Management al Proiectului. In acest plan se definesc sarcinile cerute si termenele de executie. Trebuie sa contina principalele milestone-uri si livrabile, confirmarea resurselor utilizate precum si data de inchiere a proiectului.

PROCEDURA DE CONTROL A MODIFICARILOR

Obiectivele acestei proceduri sunt:

- De a gestiona fiecare cerere de modificare pentru a mentine 'scope'-ul proiectului sub control si in deplina trasabilitate,
- De a asigura ca fiecare cerere de modificare este evaluata de principalele persoane implicate in proiect
- De a asigura ca fiecare cerere de modificare evaluata este acceptata (sau rejectata sau amanata) de catre entitatea cu autoritatea corespunzatoare.
- De a permite implementarea controlata a fiecarei cereri de modificare acceptata
- De a permite ca impactul tuturor cererilor de modificare sa fie intelese, documentate si administrate.

Rezumatul procedurii

O cerere de modificare este o solicitare de a modifica un document sau un aspect al proiectului care este plasat sub controlul modificarilor.

Cererile de modificare pot afecta unul sau mai multe dintre urmatoarele:

- Activitatea de efectuat sau in progres (aria de cuprindere – 'scope', definirea solutiei, definitia livrabilelor, etc.),
- Planurile de management de proiect sau procedurile,
- Obligatiile din cadrul contractului.

Procedura de management a modificarilor este lansata atunci cand apare nevoia unei modificari.

Rezultatul final al procedurii este fie "modificarea este implementata", fie "cererea este amanata", fie "cererea este rejectata".

Procedura de Cerere de Modificare este prezentata in continuare:

Solicitantul (de regula beneficiarul) completeaza si semneaza un formular de **Cerere de Modificare** (schimbare) pe care apoi il adreseaza partii care urmeaza sa analizeze si implementeze cererea respectiva (de regula furnizorul). Acesta din urma analizeaza cererea de modificare si reflecta rezultatul analizei in formularul **Raspuns la Cererea de Modificare**, pe care o adreseaza solicitantului.

Dacă solicitantul este de acord cu consecintele (impactul) ce s-ar produce in cazul implementarii cererii (eventuale schimbari asupra sistemului existent, costuri suplimentare, extinderea termenelor partiale sau finale de implementare, etc), atunci va aproba si semna formularul in sectiunea corespunzatoare.

Planul Proiectului

Planul de proiect se va agreea si se va elabora de catre echipele desemnate de catre Ofertant si Beneficiar, dupa semnarea contractului.

Nota:

1. Durata proiectului se modifica cu un numar de zile egal cu intarzierile induse in proiect din cauza exclusiva a beneficiarului.
2. Furnizorul isi rezerva dreptul de a propune un plan revizuit de proiect la sfarsitul etapei de analiza initiala daca se identifica modificari substantiale intre cerinte si situatia reala, constatata pe parcursul analizei. Planul de proiect de executat se va stabili impreuna cu clientul in urma atribuirii contractului.

Managementul calitatii

SAFETECH INNOVATIONS va întreţine pe întreaga durată a proiectului un Registru de calitate în care va înregistra toate verificările de calitate care vor fi realizate asupra livrabilelor proiectului.

Planul de Calitate realizat de către SAFETECH INNOVATIONS va identifica tipurile de teste care vor fi realizate, precum şi momentele în care aceste teste vor fi realizate. Testele vor fi grupate pe tipuri de funcţionalităţi, si se vor pregăti scenarii de test. Scenariul de test va include de asemenea informaţii referitor la sistemul care va fi testat, configurări ale livrabilului necesare în vederea realizării testului, echipamente necesare, precum şi resursele umane necesare şi pregătirea acestora. Scenariile de test vor fi pregătite în comun de către Furnizor şi Beneficiar şi vor trebui aprobate de către Expertul Sef in Securitatea Sistemelor Informatice înainte de începerea testelor de acceptanţă.

Managementul riscului

Riscurile ce pot avea impact asupra executiei proiectului precum si recomandarile de reducere/eliminare a riscurilor identificate, fara a se afecta cerintele caietului de sarcini, sunt prezentate in tabelul urmator.

Descrierea riscului	Posibile consecinte	Masuri de prevenire, gestionare a riscului	Impact	Probabi-litate
Lipsa de coordonare intre echipa de proiect și alți factori de decizie implicați în derularea proiectului.	Pot exista pe parcursul derulării proiectului neconcordante privind interacțiunea și colaborarea actorilor implicați.	Pentru a preveni aceste neconcordante, Managerul de Proiect va functiona ca punct unic de contact intre Beneficiar si Prestator.	Redus	Medie
Întârzieri în implementarea proiectului.	Exista riscul ca activitățile prevăzute în proiectul aflat în implementare să nu se încadreze în termenele din Graficul actual de implementare a proiectului.	Pentru a preveni acest risc, Managerul de Proiect verifică în mod regulat activitatea personalului de executie si incadrarea acestora conform planului de proiect.	Mediu	Minora
Arhivarea necorespunzătoare a documentelor.	Exista riscul ca documentele elaborate în cadrul proiectului să fie arhivate necorespunzător.	Pentru evitarea unui astfel de risc este indicat sa fie desemnata o persoana responsabila pentru arhivarea corespunzatoare.	Sever	Minora
Indisponibilitatea resurselor echipei de management.	Resursele echipei de management pot fi indisponibile pe anumite perioade de timp (concedii, deplasări, activități extra-proiect, etc.).	Perioadele de concedii, deplasari, activitat extra-proiect, etc vor fi planificate astfel incat sa nu interfereze cu perioada de desfasurare a proiectului.	Sever	Minora

Complexitatea proiectului.	Complexitatea Proiectului este un risc care trebuie luat în considerare și a cărui probabilitate creşte odată cu identificarea tuturor activităților subsecvente care compun lista activităților de baza din cadrul Proiectului. Realizarea obiectivelor prevăzute prin Proiect presupune parcurgerea mai multor etape, realizarea de activități complexe, în care sunt implicate mai multe entități. Acest risc poate provoca întârzieri în derularea proiectului sau poate duce la neatingerea tuturor obiectivelor stabilite în cadrul proiectului.	Acest risc poate fi mitigat printr-o buna planificare a activitatilor si graficului de realizare al acestora.	Redus	Minora

Managerul de Proiect verifică în mod regulat faptul că acțiunile planificate și puse în practică au efectul dorit asupra riscurilor identificate și dacă în urma aplicării planurilor riscul rezidual este în limita de acceptabilitate. Fiecare semnal de apariție a unui risc trebuie supus analizei de risc.

Pe lângă Manager de Proiect, o sarcina importanta în managementul riscurilor îl are Expertul Sef securitate sisteme informatice, care:

- atenționează Managerul de Proiect relativ la eventualele riscuri externe care pot afecta proiectul;
- ia decizii pe baza recomandărilor Managerului de Proiect referitor la diferitele riscuri;
- sesizează impactul pe care riscurile proiectului le pot avea asupra desfășurării acestuia.

Managerul de Proiect va realiza următoarele activități componente fazei de analiza a riscurilor:

- identificarea riscurilor care pot afecta proiectul;
- estimarea riscului, adică efectuarea unei analize cantitative a riscului care va avea drept rezultat determinarea importantei fiecărui risc pe baza evaluării consecințelor pe care le are asupra proiectului;
- evaluarea riscului, adică efectuarea unei analize calitative, acțiune care are drept scop deciderea acceptabilității nivelului riscului. In cazul în care se determina ca riscul nu poate fi acceptat, se vor întreprinde o serie de contramăsuri care au drept scop reducerea riscului la un nivel acceptabil, prin:
    - **Prevenire** – oprește producerea riscului sau previne impactul asupra proiectului;
    - **Reducere** –reduce probabilitatea apariției riscului sau limitează impactul;
    - **Transfer** – reduce impactul riscului prin transferarea către o terța parte;
    - **Masuri de rezerva** – se iau în cazul riscurilor reziduale;
    - **Acceptare** – se accepta riscul din diferite considerente.

Managementul resurselor

Personalul implicat in proiect dispune de logistica si birotica necesara derularii activitatilor:

- Spatiu de birou amenajat corespunzator
- Calculator si licentele software necesare
- Conexiune Internet si acces la e-mail
- Acces la servicii de comunicatii: fax, telefon, e-mail
- Acces la servicii de imprimare, scanare si copiere
- Servicii de secretariat
- Acces la mijloace de transport pentru deplasarea in interesul proiectului

Echipa de proiect, dotarile existente precum si obligatiile Safetech Innovations sunt prezentate si in capitolul Echipa de proiect.

4.2. ORGANIZAREA SI PLANIFICAREA IN TIMP A ACTIVITATILOR

Echipa de proiect propusa corespunde in totalitate cerintelor formulate de BNM fiind condusa de un grup de experti cheie compus din:

- **Expert Sef securitate sisteme informatice**
  - Alocare 95% in etapele:
    - Coordonarea echipei de experti
    - Testarea de penetrare a sistemelor informatice
    - Realizarea rapoartelor
  - Alocare 5% in etapa:
    - Derularea procedurii de achizitie
- **Expert testare securitate infrastructura retea**
  - Alocare 95% in etapele:
    - Testarea de penetrare a infrastructurii de retea
    - Realizarea rapoartelor
  - Alocare 5% in etapa:
    - Derularea procedurii de achizitie
- **Expert testare securitate sisteme informatice**
  - Alocare 95% in etapele:
    - Testarea de penetrare a sistemelor informatice
    - Realizarea rapoartelor
  - Alocare 5% in etapa:
    - Derularea procedurii de achizitie
- **Expert testare securitate sisteme informatice si infrastructurilor de tip WiFi**
  - Alocare 95% in etapele:
    - Testarea de penetrare a sistemelor informatice si infrasrtructurii de tip WiFi
    - Realizarea rapoartelor
  - Alocare 5% in etapa:
    - Derularea procedurii de achizitie
- **Expert testare securitate sisteme informatice - suplimentar**
  - Alocare 95% in etapele:
    - Testarea de penetrare a sistemelor informatice
    - Realizarea rapoartelor
  - Alocare 5% in etapa:
    - Derularea procedurii de achizitie
- **Manager de Proiect**
  - Alocare 95% in etapele:
    - Realizarea managementului de proiect
  - Alocare 5% in etapa:
    - Derularea procedurii de achizitie

4.3 ECHIPA TEHNICA

Managerul de proiect este responsabil pentru implementarea cu succes a activităţilor proiectului şi atingerii rezultatelor planificate în proiect.
Realizează managementul zilnic al proiectului – organizaţional şi conceptual

- Întocmește planurile detailate de lucru şi monitorizează respectarea implementării acestora
- Asigură și coordonează executarea la timp a activităţilor din planul de proiect
- Asigură transformarea efectivă şi la timp a resurselor proiectului în activităţi şi produse concrete, care vor duce la atingerea rezultatelor scontate
- Supraveghează desfășurarea zilnică a proiectului și gestionează echipa proiectului
- Asigură un circuit informaţional adecvat (discuţii şi feedback) între diferiţi actori – echipa de proiect a furnizorului, echipa de management a autorității contractante, terțe părți, etc.
- Monitorizează în timp progresul atins față de obiectivele propuse
- Face propuneri de imbunatățire a stilului de lucru pentru a maximiza eficiența atingerii obiectivelor propuse și le transmite comitetului de conducere a proiectului
- Pregătește rapoartele proiectului, cît şi alte rapoarte necesare pentru echipa de coordonare a proiectului
- Verifică pontajul echipei de proiect
- Asigură rezolvarea problemelor apărute în realizarea proiectului și informează la timp echipa de management despre problemele apărute și pe care nu le poate rezolva la nivelul său
- Participă la diferite şedinţe ale echipei de proiect interne ale furnizorului, precum și la şedinţele organizate de BNM pe tema proiectului
- Arhivează corespunzator toată documentația legată de proiect
- Participă la toate evenimentele proiectului, asigurând pregătirea adecvată a acestora.
- Motivează echipa de proiect prin comunicare și prin evaluarea permanentă a performanțelor acestora în raport cu sarcinile trasate
- Răspunde de păstrarea confidențialității informațiilor la care are acces
- Asigură un climat de colaborare între toți cei implicați în proiect

Echipa alocata proiectului este formata din persoane cu o vasta experienta in domeniul IT si al securitatii informatiei precum si cu o expertiza deosebita in **Penetration Testing**, demonstrata de numarul si complexitatea proiectelor implementate. Pentru o confirmare a calitatilor serviciilor prestate, mai jos este prezentata Echipa Tehnica si certificarile detinute de experti.

Toti membrii Echipei Tehnice propuse au participat din partea **SAFETECH INNOVATIONS** la exercitiile cibernetice organizate de catre **NATO - CYBER**

COALITION 2019; CYBER COALITION 2018; CYBER COALITION 2017; CYBER COALITION 2016; CYBER COALITION 2015. De asemenea, acestia au participat la exercitiul paneuropean de protectie a infrastructurilor UE impotriva atacurilor cibernetice coordonate **- CYBER EUROPE 2016,** care a fost organizat de catre **Agentia Uniunii Europene pentru Securitatea Retelelor si a Informatiilor (ENISA) si la CyDex18 si CyDex17 e**xercitii organizate de catre **Serviciul Roman de Informatii (SRI)** prin intermediul **Centrului National Cyberint.**
Mai jos puteti gasi profilele expertilor, CV-urile acestora fiind atasate.

Adrian VLADA – Manager Proiect Sisteme Informatice

Adrian VLADA are o experienta profesionala de peste 11 ani in managementul proiectelor IT si de peste 7 ani in domeniul securitatii informatiilor: noua ani pentru o mare banca europeana in Romania (**Raiffeisen Bank**) si din 2011 este Manager de Proiect si Director Operatiuni al SAFETECH INNOVATIONS, o firma de consultanta avand ca domeniu principal de activitate securitatea informatiilor.

Dl. VLADA detine un bagaj deosebit de aptitudini tehnice, combinate cu capacitati manageriale performante in securitatea informatiilor si de gestionare a riscurilor IT & C.

Totodata, printre sarcinile sale principale enumeram:

- Managementul proiectelor cu specific IT;
- Coordonare activitati, resurse, timinng mitigare riscuri, integrare echipe, validarea solutiilor;
- Coordonarea rezolvarii incidentelor in timpul proiectului;
- Managementul proiectelor si al activitatilor de upgrade si imbunatatire a infrastructurii IT
- Identificarea si analiza riscurilor la adresa securitatii informatiei prin identificarea vulnerabilitatilor la nivelul sistemului informatic, a amenintarilor care le pot exploata, prin evaluarea impactului si a probabilitatii de manifestare a riscului;
- Identificarea vulnerabilitatilor la nivelul sistemelor IT precum si managementul acestora;
- Analiza si evaluarea infrastructurii sistemului informatic si capacitatii;
- Verificarea si evaluarea procedurilor operationale;
- Evaluarea si implementarea de solutii si produse de securitate informatica;
- Dezvoltarea si revizia politicilor si standardelor interne privind securitatea informatiei;
- Evaluarea conformitatii cu standardele de securitate in domeniu (ISO27001).

Dl. VLADA detine urmatoarele certificari:

· **Manager de Proiect**

· **Formare Auditori Sefi -** pentru Sisteme de Managementul Securitatii Informatiei - ISO/IEC 27001:2005

Victor GANSAC – Expert Sef Securitate Sisteme Informatice

Dl. Victor GANSAC este un Senior Expert in Managementul Securitatii cu o experienta aplicata deosebita in sectorul Financiar-Bancar si cu o expertiza dovedita in Business Continuity, in proiectarea arhitecturilor de securitate IT, cu background in toate dimensiunile IT, cu precadere in zona de networking.

Victor GANSAC are o experienta profesionala de peste 15 ani in managementul proiectelor IT si managementul IT si de peste 10 ani in domeniul securitatii informatiilor: 9 ani pentru o mare banca europeana in Romania (**Raiffeisen Bank**) si din 2011 este Director General al SAFETECH INNOVATIONS.

Din pozitia de Director General al companiei **SAFETECH INNOVATIONS**, Dl. GANSAC a participat la executarea (la nivel de coordonare sau executie tehnica) a peste 250 de proiecte de evaluare a securitatii informatiei prin activitati de tipul **Penetration Testing / Vulnerability Assessment / Ethical Hacking**.

Totodata, printre sarcinile sale principale enumeram:

- Activitati in securitatea informatiilor: penetration testing, vulnerability assessment, ethical hacking, audit si evaluare, verificare a conformitatii, identificare si analiza a riscurilor, politica si procesul de securitate, securitatea in Software Development Life Cycle (SDLC);
- Design de securitate pentru solutii noi: metode de autentificare si de autorizare, profiluri de utilizatori, securitate in retea;
- Dezvoltarea programelor de instruire in domeniul securitatii;
- Elaborarea si revizuirea politicilor de securitate, a standardelor si a liniilor de baza;
- Dezvoltarea analizei riscurilor de securitate si a planurilor de securitate;
- Elaborarea reglementarilor si politicilor de securitate;
- Design de securitate pentru solutii noi: metode de autentificare si de autorizare, profiluri de utilizatori, securitate in retea;
- Coordonarea Grupului de Strategie si Planificare de Securitate.
- Coordonarea, organizarea si controlul activitatilor legate de securitatea informatiilor si activitatile de continuitate a activitatii
- Testarea de securitate pentru software;
- Coordonarea, organizarea si controlul urmatoarelor activitati:
    - Analiza Impactului Afacerilor pentru produsele software;
    - Definirea cerintelor de securitate pentru software din punct de vedere al continuitatii;

- Stabilirea designului de software din punctul de vedere al securitatii informatiilor si al continuitatii (inclusiv modelarea amenintarilor);
- Acceptata software-ului din punctul de vedere al securitatii informatiilor;
- Teste periodice de continuitate a activitatii si de recuperare in caz de catastrofe;
- Monitorizarea software-ului si a infrastructurii din punctul de vedere al securitatii informatiilor.

- Experienta vasta in diferite pozitii cu responsabilitati diferite: dezvoltarea afacerii, coordonarea securitatii, strategiei si planificarii, administratorul de retea, administratorul de sistem.

Dl. Victor GANSAC:

- a coordonat echipa SAFETECH INNOVATIONS in cadrul exercitiilor cibernetice organizate de catre **NATO - CYBER COALITION 2019; CYBER COALITION 2018; CYBER COALITION 2017; CYBER COALITION 2016; CYBER COALITION 2015**.
- a coordonat echipa SAFETECH INNOVATIONS in cadrul exercitiului paneuropean de protectie a infrastructurilor UE impotriva atacurilor cibernetice coordonate - **CYBER EUROPE 2016**, care a fost organizat de catre **Agentia Uniunii Europene pentru Securitatea Retelelor si a Informatiilor (ENISA)**.
- A coordonat echipa SAFTECH INNOVATIONS **CyDex18 si CyDex17 e**xercitii organizate de catre **Serviciul Roman de Informatii (SRI)** prin intermediul **Centrului National Cyberint.**
- a coordonat organizarea CTF-USV 2016 - un concurs international Capture the Flag pentru studenti, gazduit de Universitatea Suceava.
- a coordonat furnizarea de servicii de **Penetration Testing** catre Centrul de Guvernare Electronica al Republicii Moldova (platforma electronica e-Guvernare, ce faciliteaza interactiunea digitala intre institutiile guvernamentale si cetateni), care a inclus testarea a 17 platforme electronice nationale care ofera servicii cetatenilor cum ar fi: **Mpass** - Platforma de autentificare si autorizare pentru cetateni, **Msign** - platforma guvernamentala care ofera semnatura digitala, **E-Factura** - platforma guvernamentala care asigura servicii de facturare electronica si altele;

Dl. GANSAC detine urmatoarele certificari:

- **CIPT** - Certified Information Privacy Technologist
- **CISSP** - Certified Information Systems Security Professional;
- **GICSP** - Global Industrial Cyber Security Professional
- **CSSLP** - Certified Secure Software LifeCycle Professional;
- **CISM** - Certified Information Security Manager;
- **CISA** - Certified Information Systems Auditor;
- **Certificate in "Security of classified information" from The National Registry Office for Classified Information (ORNISS)**

Teodor LUPAN – Expert Testare Securitate Infrastructura Retea

Dl. LUPAN este un Senior Expert in Securitatea Informatiei care detine o expertiza deosebita in sectorul Financiar-Bancar, prin prisma proiectelor implementate. Teodor LUPAN are o baza deosebita de cunostinte despre metodologiile, instrumentele, atacurile si contramasurile legate de Penetration Testing / Vulnerability Assessment / Ethical Hacking si o experienta foarte bogata in domeniul testelor de securitate si scenariilor reale de hacking. Ca o dovada, in 2011, a fost parte a echipei care a elaborat materia de testare pentru examenul pentru obtinerea certificatului Certified Ethical Hacker – CEHv.7 in cadrul EC-Council si Prometric.

Teodor LUPAN a obtinut Diploma de Master "Implementarea si gestionarea retelelor de calculatoare". Tema lucrarii de disertatie a fost implementarea si testarea securitatii retelelor informatice folosind instrumente de tip open source si a fost clasificata cu cel mai mare punctaj in comitetul de evaluare.

Din punct de vedere profesional, a inceput ca Specialist in Linux (New Era Computer Communications - IT), continuand apoi ca Administrator de retea (Profilux), Administrator Linux (Rompetrol), Designer de solutii (Rompetrol), Expert in securitate (Raiffeisen Bank) si in prezent este responsabil pentru conducerea echipei tehnice de la **SAFETECH INNOVATIONS**, compania in care este si co-fondator.

In calitate de Director Tehnic in cadrul unei firme de consultanta in domeniul securitatii informatiilor, el este responsabil cu furnizarea serviciilor de securitate clientilor, cum ar fi Penetration Testing, consultanta in domeniul securitatii cloud si consultanta securizare software etc.

Dat fiind ca tehnologia Cloud Computing este din ce in ce mai adoptata de catre companii, dar este si o tehnologie noua si provocatoare, nevoia de securitate in fiecare aspect este o cerere foarte reala. Din pozitia sa de la **SAFETECH INNOVATIONS**, dl. LUPAN a oferit cu succes consultanta de securitate si / sau teste de penetrare pentru infrastructurile sau proiectele cloud, transmiterea pe o cercetare puternica, cunostinte tehnice solide, o buna intelegere a cerintelor de reglementare, client si business.

Din pozitia de Director Tehnic al companiei **SAFETECH INNOVATIONS**, Dl. LUPAN a participat la executarea (la nivel de coordonare sau executie tehnica) a peste 250 de proiecte de evaluare a securitatii informatiei prin activitati de tipul **Penetration Testing / Vulnerability Assessment / Ethical Hacking**. Fiecare dintre aceste proiecte a fost finalizat printr-un raport continand informatii detaliate despre problemele identificate, riscurile induse respectiv modalitati de remediere a acestora.
Directorul Tehnic al **SAFETECH INNOVATIONS:**

- a condus echipa SAFETECH INNOVATIONS in cadrul exercitiilor cibernetice organizate de catre **NATO - CYBER COALITION 2019; CYBER COALITION 2018; CYBER COALITION 2017; CYBER COALITION 2016; CYBER COALITION 2015**.

• a condus echipa **SAFETECH INNOVATIONS** in cadrul exercitiului paneuropean de protectie a infrastructurilor UE impotriva atacurilor cibernetice coordonate - **CYBER EUROPE 2016**, care a fost organizat de catre **Agentia Uniunii Europene pentru Securitatea Retelelor si a Informatiilor (ENISA)**.

• a condus echipa SAFTECH INNOVATIONS **CyDex18 si CyDex17 e**xercitii organizate de catre **Serviciul Roman de Informatii (SRI)** prin intermediul **Centrului National Cyberint.**

• a coordonat dezvoltarea exercitiilor de securitate si organizarea CTF-USV 2019; CTF-USV 2018; CTF-USV 2017 si la CTF-USV 2016 - concursuri internationale Capture the Flag pentru studenti, gazduite de Universitatea Suceava.

• a coordonat furnizarea de servicii de **Penetration Testing / Vulnerability Assessment / Ethical Hacking** catre Centrul de Guvernare Electronica al Republicii Moldova (platforma electronica e-Guvernare, ce faciliteaza interactiunea digitala intre institutiile guvernamentale si cetateni), care a inclus testarea a 17 platforme electronice nationale care ofera servicii cetatenilor cum ar fi: **Mpass** - Platforma de autentificare si autorizare pentru cetateni, **Msign** - platforma guvernamentala care ofera semnatura digitala, **E-Factura** - platforma guvernamentala care asigura servicii de facturare electronica si altele;

De asemenea, a participat si in prezent este implicat in calitate de cercetator si expert in probleme de securitate in diferite proiecte precum:

• "Infrastructura de tip cloud pentru institutiile publice din Romania - ICIPRO" coordonat de Institutul National de Cercetare-Dezvoltare in Informatica din Romania.

• "Elaborarea unor standarde tehnice pentru sprijinirea programului national de reducere a vulnerabilitatilor si amenintarilor cibernetice" - Proiectul national de cercetare care vizeaza reducerea vulnerabilitatilor si criminalitatii informatice.

• "Formalizarea unui cadru standardizat privind masuri de securitate adecvate pentru companiile mici si mijlocii pentru prelucrarea datelor cu caracter personal" proiect implementat de **SAFETECH INNOVATIONS** pentru **ENISA**.

De-a lungul timpului, a dobandit competente deosebite in domeniul securitatii tranzactiilor bancare si online, securitatii IT, sistemelor de operare, retelelor, programarii, criptografiei, tehnologiilor web, monitorizarii de securitate, administrarii sistemelor, telefoniei VoIP, tehnologiilor RFID etc.

Experienta sa este sustinuta si de numeroasele certificari obtinute la nivel international:

- **CEH -** Certified Ethical Hacker
- **OSCP -** Offensive Security Certified Professional
- **OSWP** – Offensive Security Wireless Professional
- **LPT -** Licensed Penetration Tester
- **ECSA –** EC-Council Certified Security Analyst
- **RHCE -** Red Hat Certified Engineer

Ionut GEORGESCU - Expert Testare Securitate Sisteme Informatice

Ionut GEORGESCU este un Expert in Securitatea Informatiei cu o experienta de peste 7 ani in domeniu si peste 14 ani in domeniul IT.

In contextul pozitiei detinute in **SAFETECH INNOVATIONS**, Dl. GEORGESCU a participat la executarea (la nivel de coordonare sau executie tehnica) a peste 200 de proiecte de evaluate a securitatii informatiei prin activitati de tipul Ethical Hacking & Penetration Testing printre care merita mentionate: ArcelorMittal, World Bank Organization, Electrica S.A., ApaNova Bucuresti S.A., Raiffeisen Bank, BRD Groupe Societe Generale, Volksbank, ING Life Assurance, Credit Europe Bank , Alpha Bank, Idea Bank, Gothaer Asigurari Reasigurari S.A., ArcelorMittal, Siveco Romania S.A., Radet S.A, JT International

Fiecare dintre aceste proiecte a fost finalizat printr-un raport continand informatii detaliate despre problemele identificate, riscurile induse respectiv modalitati de remediere a acestora.

Totodata, Dl. GEORGESCU:

- a facut parte din echipa **SAFETECH INNOVATIONS** care a participat la exercitiile cibernetice organizate de catre **NATO - CYBER COALITION 2016; CYBER COALITION 2015**.
- a facut parte din echipa SAFETECH INNOVATIONS care a participat la exercitiul pan-european de protectie a infrastructurilor UE impotriva atacurilor cibernetice coordonate - CYBER EUROPE 2016, care a fost organizat de catre Agentia Uniunii Europene pentru Securitatea Retelelor si a Informatiilor (ENISA).
- a participat la dezvoltarea provocarilor tehnice si organizarea CTF-USV 2016 - un concurs international Capture the Flag pentru studenti, gazduit de Universitatea Suceava.
- a participat la proiectul de furnizare de servicii de Penetration Testing catre Centrul de Guvernare Electronica al Republicii Moldova (platforma electronica e-Guvernare, ce faciliteaza interactiunea digitala intre institutiile guvernamentale si cetateni), care a inclus testarea a 17 platforme electronice nationale care ofera servicii cetatenilor cum ar fi: Mpass - Platforma de autentificare si autorizare pentru cetateni, Msign - platforma guvernamentala care ofera semnatura digitala, E-Factura - platforma guvernamentala care asigura servicii de facturare electronica si altele;
- Este implicat in prezent in proiectul SICAP, care reprezinta un nou sistem informatic pentru dezvoltarea achizitiilor publice (care va inlocui sistemul SEAP), unde efectueaza servicii de consultanta in securitate si servicii de Teste de penetrare;

Pe langa expertiza in Securitatea Informatiei, Ionut GEORGESCU are o experienta vasta de peste 12 ani in domeniul administrarii si configurarii de sisteme, baze de date, storage, clustere ESX etc. Abilitatile sale tehnice constau in administararea si configurarea de sisteme (Unix si Linux), administrarea si configurarea de baze de date SQL Server si Oracle, administrarea si configurarea de clustere ESX, administrarea si configurarea storage EMC/HP/HITACHI si securitate (scanare si analiza de vulnerabilitati, audit de securitate, implementari de standarde de securitate etc.)

Dl. GEORGESCU detine urmatoarele certificari:

- **CEH** - Certified Ethical Hacker
- **ECSA** - Certified Security Analyst
- **CISSP** - Certified Information Systems Security Professional
- **ISSECO_CPSSE** - Certified Professional for Secure Software Engineering
- **QualysGuard** -Vulnerability Management
- **VMware VCP4**
- **VMware VCP5**
- **RHCE** - Red Hat Certified Engineer
- **RHCSA** - Red Hat Certified System Administrator
- **Oracle Database 10g**: Administration I
- **Oracle Database 10g**: Administration II
- **Oracle Database 11g**: New Features for Administrators

Oana STOIAN – Expert Testare Securitate Sisteme Informatice si Infrastructurilor de tip WiFi

Dna Oana STOIAN a absolvit in anul 2011 Universitatea "A.I.Cuza", Iasi - Facultatea de Drept. A absolvit cu succes titlul de master "Dreptul afacerilor", Universitatea Titu Maiorescu, Bucuresti.

Dna STOIAN este un expert pasionat de securitatea informatiilor cu accent pe Ethical Hacking & Penetration Testing/Vulnerability Assessment/. A inceput sa lucreze in domeniul IT cu 5 ani in urma ca Software Tester la Printec Group Romania, fiind implicata in testarea securitatii terminalelor POS.

La SAFETECH INNOVATIONS a devenit unul dintre membrii-cheie ai echipei tehnice, fiind in prezent adjunctul directorului tehnic.

Face parte din echipa Safetech din 2015, unde a demonstrat o mare capacitate de a-si dezvolta abilitatile tehnice. In acest moment a obtinut trei certificari. In calitate de adjunct al directorului tehnic, ea s-a dovedit a avea bune abilitati de organizare si management si asigura un rol important in interactiunea cu celelalte Directii, optimizarea activitatilor si colaborarea cu managerii departamentului pentru a-si indeplini indatoririle.

Prin prisma pozitiei detinute in cadrul SAFETECH INNOVATIONS a fost implicata in diferite proiecte importante, cum ar fi:

- a facut parte din echipa SAFETECH INNOVATIONS care a participat la exercitiile cibernetice organizate de catre NATO - CYBER COALITION 2018; CYBER COALITION 2017; CYBER COALITION 2016.
- a facut parte din echipa SAFETECH INNOVATIONS care a participat la exercitiul pan-european de protectie a infrastructurilor UE impotriva atacurilor cibernetice coordonate - CYBER EUROPE 2016, care a fost organizat de catre Agentia Uniunii Europene pentru Securitatea Retelelor si a Informatiilor (ENISA).

· a participat la dezvoltarea exercitiilor tehnice si organizarea CTF-USV 2018; CTF-USV 2017 si la CTF-USV 2016 - concursuri internationale Capture the Flag pentru studenti, gazduite de Universitatea Suceava.
· a participat la proiectul de furnizare de servicii de Teste de penetrare catre Centrul de Guvernare Electronica al Republicii Moldova (platforma electronica e-Guvernare, ce faciliteaza interactiunea digitala intre institutiile guvernamentale si cetateni), care a inclus testarea a 17 platforme electronice nationale care ofera servicii cetatenilor cum ar fi: Mpass - Platforma de autentificare si autorizare pentru cetateni, Msign - platforma guvernamentala care ofera semnatura digitala, E-Factura - platforma guvernamentala care asigura servicii de facturare electronica si altele;
· In timpul carierei sale, a obtinut diverse competente tehnice cum ar fi: competenta in identificarea vulnerabilitatilor, recomandarea masurilor corective adecvate si asigurarea unor controale adecvate privind securitatea informatiilor; Abilitatea de a defini, dezvolta si monitoriza gestionarea riscurilor; Experienta in lucrul cu instrumentele de evaluare a vulnerabilitatii, precum Rapid7 Nexpose, Accunetix; Experienta in metodologii, instrumente, atacuri si contramasuri legate de pentration testing / vulnerability assessment / ethical hacking; Experienta in intelegerea functionarii si lucrului cu echipamentele de retea; cunostiinte solide despre TCP / IP, stack OSI; Experienta in monitorizarea evenimentelor, gestionarea incidentelor si raportarea problemelor de securitate gasite; Experienta in elaborarea politicilor, standardelor si procedurilor de securitate.

Dna. STOIAN detine urmatoarele certificari:

- **CEH** - Certified Ethical Hacker
- **OSWP** – Offensive Security Wireless Professional
- **OSCP –** Offensive Security Certified Professional (Offensive Security)
- **Security+** - CompTIA Security+ (ID COMP001020999382)
- **Project Manager**

Marinel STĂNILĂ - Expert în securitate

DI STĂNILĂ este un profesionist fiabil și muncitor, cu o abilitate tehnică puternică în domeniile tehnologiei informației și securității informațiilor. El a acumulat cativa ani de experienta tehnica de la cercetarea si implementarea solutiilor de securitate si furnizarea de servicii de securitate cum ar fi training-uri de constientizare a securitatii, evaluari de vulnerabilitate, audituri si configuratii de securitate la administrarea infrastructurii virtuale, administrarea firewall-ului, administrarea mesageriei și implementarea proiectelor BYOD.

A absolvit Academia de Studii Economice din București cu Master în Sisteme Informatice pentru Managementul Proceselor și Resurselor Economice. Tema lucrării de disertație a fost implementarea unui sistem integrat de management al procesului educațional. A fost acordată cea mai înaltă clasă în comitetul de evaluare.

În timpul carierei sale, a fost implicat în activități tehnice și de formare într-o gamă largă de aspecte legate de tehnologia informației și securitate.

A început ca ofițer IT pentru compania Smurfit Kappa Corporation, care lucra la biroul din București. Ulterior, el a mers la instituția de învățământ Lumina ca administrator de sistem, de unde a fost recrutat de un furnizor de servicii, Zeconda Systems (Global Eye Technologies), axat pe soluții de securitate și infrastructură de vârf pentru clienții corporativi mari.

În prezent, lucrează la Safetech Innovations ca inginer de securitate, fiind responsabil de cercetarea, dezvoltarea, testarea și implementarea portofoliului de soluții de securitate pe de o parte, cu evaluări de vulnerabilitate și audituri de securitate și cele mai bune practici de configurare pe de altă parte.

Este foarte informat în domeniile soluțiilor de securitate, întăririi sistemului, evaluărilor vulnerabilității, auditurilor de securitate și celor mai bune practici de configurare.

Dl. STANILA detine urmatoarele certificari:

- **CISSP** - Certified Information Systems Security Professional
- **CISA** Certified Information Systems Auditor
- **CCSA** - Check Point Certified Security Administrator
- **MCSA** – Microsoft Windows Server 2003
- **MCP** – Microsoft Windows Server 2003 Environment – 70-290
- **MCP** – Microsoft Windows Server 2003 Network Infrastructure – 70-291
- **MCP** – Microsoft Windows XP – Installing, Administering, Configuring – 70-270
- **MCTS** – Microsoft Windows 7: Configuring – 70-680
- **VTSP 5** – VMWare Technical Solutions Professional
- **VSP 5** – VMWare Sales Professional
- **VTSP** – Veeam Technical Sales Professional
- MobileIron Bootcamp Certificate
- Certified Linux System and Network Administrator by the Romanian Government

IT, experiență în domeniul securității și securității informațiilor (ani)

- Experienta de cinci ani in urmatoarele domenii IT & C: Solutii de Securitate IT - Proiectare si Implementare, Evaluare Vulnerabilitati, Audit de Sisteme Informatice, Sisteme de Operare, Infrastructura IT
- Experiență de patru ani în domeniul securității informațiilor începând cu 2012
- Referințe:
- A participat ca membru al echipei SAFETECH pentru proiectul ENISA: "Un cadru privind măsurile de securitate adecvate pentru prelucrarea datelor cu caracter personal"
- Implementarea serviciilor de securitate la inovațiile Safetech;
- Implementarea soluțiilor de infrastructură și de securitate în proiectele derulate de clienți în România;

**** Atasat puteti gasi CV-urile si certificarile expertilor. Subliniem ca am inclus doar certificarile considerate relevante pentru aceasta licitate, expertii nostri detin si alte certificari pe care le putem pune la dispozitie daca sunt solicitate.***
***** Atasat puteti gasi si o serie de recomandari obtinute de expertii nostri, care sunt relevante pentru aceasta licitatie.***

5 MATRICE DE COMPLIANTA CU CERINTELE SPECIFICATE IN CAIETUL DE SARCINI

SPECIFICATIILE CERUTE IN DOCUMENTATIA DE ATRIBUIRE	CONFORM	SPECIFICATIILE OFERTATE
2.2 Scopul serviciilor prestate		
2.2.1 Scopul testelor de penetrare este de a analiza comportamentul sistemelor informatice în contextul diferitelor atacuri informatice, fiind analizate inclusiv vulnerabilitățile care pot exista în aplicațiile dezvoltate sau utilizate. Un test de penetrare complet va cuprinde atît teste automate cît și manuale.	DA	Testele de penetrare vor analiza comportamentul sistemelor informatice în contextul diferitelor atacuri informatice, fiind analizate inclusiv vulnerabilitățile care pot exista în aplicațiile dezvoltate sau utilizate. Testele de penetrare oferite de catre SAFETECH INNOVATIONS vor cuprinde atît teste automate cît și manuale.

- *Testele automate* vor identifica erori de programare în aplicațiile utilizate și vor fi efectuate cu ajutorul unor programe specializate precum instrumentele de scanare a vulnerabilităților, a aplicațiilor web și a codului, instrumente de testare și identificare a eventualelor erori de programare din aplicații în vederea exploatării lor.	DA	Testele automate efectuate de SAFETECH INNOVATIONS vor identifica erori de programare în aplicațiile utilizate și vor fi efectuate cu ajutorul unor programe specializate precum instrumentele de scanare a vulnerabilităților, a aplicațiilor web și a codului, instrumente de testare și identificare a eventualelor erori de programare din aplicații în vederea exploatării lor. In cadrul procesului de testare, sunt folosite instrumente de scanare specializate şi scripturi care ajuta la reducerea timpului de evaluare şi contribuie la descoperirea unor vulnerabilităţi greu de detectat. Aceste instrumente includ: fuzzers personalizate, analizoarele statice si dinamice, decodoare, proxy pentru a captura şi manipula traficul, regex matchers etc. De asemenea, sunt utilizate scripturi personalizate care pot fi utilizate pentru a simula atacuri complexe. Expertii nostri dispun de o combinatie de instrumente comerciale, open source si dezvoltate intern pentru a complementa efortul manual. Folosirea uneltelor automate, pentru a realiza scanari in urma carora se identifica vulnerabilitati comune, este combinata cu tehnici manuale de identificare a vulnerabilitatilor. Pentru o lista detaliata a instrumentelor folosite de catre expertii nostri pentru testarea automata, consultati documentul atasat: **Lista unelte Penetration Testing**
Testele manuale vor analiza aspecte ale aplicațiilor care necesită intuiția umană, identificîndu-se erori logice de programare, și vor analiza și confirma sau infirma rezultatele testelor automate. Pentru atingerea acestor obiective, serviciile de penetrare si evaluare a vulnerabilităților informatice în cadrul Sistemului Informatic al BNM prin teste specifice de penetrare din exteriorul infrastructurii de rețea urmează să fie prestate de Ofertantul selectat conform cerințelor stabilite în acest caiet de sarcini.	DA	Testele manuale analizează aspecte ale aplicațiilor care necesită intuiția și intervenția umană și abilitatea de a combina cunoștințe din mai multe domenii, pentru a identifica vulnerabilități care nu pot fi descoperite folosind programe automate de testare și vor analiza și confirma sau infirma rezultatele testelor automate. Intrucat eficienta testarii manuale este dependenta direct de abilitatile profesionale ale personalului implicat in activitatea de testate, prin echipa alocata in acest proiect, care are o vasta experienta in teste de penetrare complexe, certificarile detinute in acest domeniu, se va asigura un inalt nivel de calificare in efectuarea testelor de penetrare manuale necesare acestui proiect.

2.2 Ofertantul trebuie să descrie activitățile ce vor fi desfășurate de acesta pentru a răspunde acestor cerințe. Ofertantul trebuie să prezinte informație despre modul în care intenționează să presteze serviciile solicitate la nivelul cerut, precum și informație privind capacitățile sale tehnice, organizatorice și de competența, ce confirmă capacitatea sa de a presta la nivelul cerut.	DA	Tehnicile utilizate in identificarea si evaluarea vulnerabilitatilor se bazeaza pe cele mai bune practici in domeniu la nivel international: ● The Penetration Testing Execution Standard – PTES; ●National Institute of Standards and Technology – NIST; ● Open Source Security Testing Methodology – OSSTM; ● Open Information Systems Security Group - OISSG; ● Open Web Application Security Project - OWASP. Etapele realizarii unui test de penetrare cuprind urmatorii pasi: ● Construirea unui model al amenintarilor. Investigarea arhitecturii aplicatiei si a tehnologiei. Identificarea specificatiilor cheie de securitate si a amenintarilor. Crearea unui model al amenintarilor care documenteaza activele care trebuie protejate, potentialele amenintari la adresa acestor active, atacuri care ar putea fi realizate, precum si conditiile care ar duce la atacuri de succes. ● Construirea unui plan de evaluare si actiune. Convertirea amenintarilor posibile in atacuri care vor fi realizate de ingineri de securitate. Conditiile unui atac, descrise in modelarea amenintarilor, sunt testate. ● Executarea evaluarii. Executarea atacurilor, asa cum sunt descrise in planul de actiune. Descoperirea vulnerabilitatilor si a variatiilor acestora. Activitatile includ evaluarea conectivitatii intre sistemele utilizate, culegerea de informatii despre sistemele testate din domeniul public si privat, descoperirea sistemelor si serviciilor active si scanarea sistemelor pentru descoperirea vulnerabilitatilor. Utilizand informatiile descoperite in evaluarea vulnerabilitatilor, se vor construi arbori de atac (attack trees) si se vor implementa actiunile din aceste structuri. In cazul aplicatiilor aflate in scop, testele de penetrare vor include in mod minimal urmatoarele: ● Testare de tip "Information Gathering" ● Testarea managementului configuratiilor ● Testarea managementului identitatilor ● Testarea mecanismelor de autentificare

		● Testarea mecanismelor de autorizare ● Testarea mecanismelor de management al sesiunii ● Testarea mecanismelor de validare a datelor de input ● Testarea managementului exceptiilor si erorilor ● Testarea mecanismelor criptografice ● Teastarea logicii de business ● Testarea securitatii "client-side" ● Raportarea rezultatelor. Documentarea problemelor identificate si prezentarea unor recomandari pentru remediere. In primul rand, inginerii SAFETECH INNOVATIONS vor lucra cu echipa tehnica a beneficiarului pentru a identifica riscurile la nivelul aplicatiilor si sistemelor informatice. In evaluarea riscurilor, vulnerabilitatile potentiale sunt identificate in functie de caracteristicile aplicatiei, incluzand aici mediul, modul de utilizare si maturitatea organizatiei in domeniul securitatii. Rezultatul final este o modelare a amenintarilor care este utilizata pentru a intelege mai bine activele aplicatiilor si sistemelor informatice, amenintarile, modalitatile de atac si conditiile in care un atac ar avea succes. Dupa determinarea riscurilor, zone individuale care urmeaza a fi testate sunt identificate in functie de aceste riscuri. O zona de test poate acoperi o vulnerabilitate specifica, cunoscuta, precum predispozitia de aparitie a unei probleme de tipul denial of service, poate fi specifica functionalitatilor de securitate ale aplicatiilor (ex: un utilizator poate accesa datele personale ale altui utilizator) sau poate implica erori de logica la nivelul aplicatiei. Atacurile individuale pentru fiecare zona de test sunt dezvoltate utilizand cele mai bune practici in domeniu si sunt documentate in Planul de Testare a Securitatii. Odata ce atacurile individuale sunt dezvoltate, testarea de securitate este efectuata pentru a se descoperi vulnerabilitatile si a se propune optiuni pentru remedierea acestora. SAFETECH INNOVATIONS dispune de o serie de unelte de testare a securitatii si de expertiza extensiva in securitatea aplicatiilor; astfel testarile sunt efectuate intr-o maniera eficienta.

		La finalul testarilor, este pregatit un raport final. Acest raport descrie problemele identificate, detaliile tehnice ale acestora, prezentarea generala, precum si metode de remediere. In plus, pentru fiecare vulnerabilitate identificata va fi pregatit un raport individual, care documenteaza vulnerabilitatea, scenariile de risc, severitatea, pasii de reproducere si metode de remediere.
2.3 Cerințele față de serviciile de penetrare		
2.3.1 Serviciile de penetrare vor avea ca rezultat o analiză complexă a securității sistemelor informatice ale Beneficiarului, testînd eficacitatea măsurilor de securitate implementate prin simularea unor atacuri informatice. Activitățile echipei de testare se vor baza pe practici de “ethical hacking”, iar posturile pe care le va lua echipa vor fi următoarele:	DA	Serviciile de penetrare vor avea ca rezultat o analiză complexă a securității sistemelor informatice ale Beneficiarului, testand eficacitatea măsurilor de securitate implementate prin simularea unor atacuri informatice. Activitățile echipei de testare se vor baza pe practici de “ethical hacking”, iar posturile pe care le va lua echipa vor fi următoarele:
a. ***Black box*** – în această situație echipa de testare nu va cunoaște nici o informație despre sistemele auditate, cu excepția informației de accesare a aplicațiilor (pagini web, adrese IP). Această metodă va fi utilizată pentru testarea infrastructurii externe a Beneficiarului.	DA	Pentru testarea infrastructurii externe a Beneficiarului, SAFETECH INNOVATIONS va utiliza metodologia de testare ***Black box*** – care implica scenariul urmator: echipa de testare nu va cunoaște nici o informație despre sistemele auditate, cu excepția informației de accesare a aplicațiilor (pagini web/adrese URL, adrese IP). Avantajul acestei metodologii, care va fi efectuata de catre SAFETECH INNOVATIONS este ca simuleaza un scenariu foarte realistic de atac.

2.3.2 Ofertantul va trebui să utilizeze echipamente și aplicații, și să dețină experiență pentru realizarea de teste de penetrare la nivel de rețea, inclusiv wireless, sistem de operare, baze de date și aplicații, inclusiv cele web, atacuri informatice simulînd aplicații malițioase, cît și de negare a serviciului (DoS).	DA	SAFETECH INNOVATIONS a implementat o serie de proiecte de penetration testing/vulnerability assessment/ethical hacking la peste 15 banci si institutii financiare si de asigurari din Romania si din alte tari din Europa precum: Banca Nationala a Moldovei, BRD - Groupe Société Générale, Banca Comerciala Romana (BCR) Raiffeisen Leasing, Raiffeisen Bank, OTP Bank, First Bank, ING Shared Business BV Amsterdam – Bucharest Branch, Alpha Bank, Alpha Finance, ING Life Assurance, OTP Bank, Idea Bank, Libra Bank, Garanti Bank, Legal & General, Volksbank, etc. Totodata, SAFETECH INNOVATIONS a fost acreditata drept Furnizor Oficial de servicii de Penetration Testing pentru Raiffeisen Bank International Group, BRD - Groupe Société Générale ING Shared Business BV Amsterdam – Bucharest Branch, UNIQA ASIGURARI S.A si ArcelorMittal Europe Group. De asemenea, SAFETECH a efectuat o serie de proiecte de ethical hacking, audit de securitate, audit de risc si analiza vulnerabilitatilor, standarde de securitate, monitorizarea incidentelor de securitate, scanare si analiza de vulnerabilitate pentru pentru o serie de clienti foarte importanti din Romania dar si de peste hotare precum: ArcelorMittal (Luxemburg), World Customs Organizations (Belgia), Electrica S.A., ApaNova Bucuresti S.A., etc. Echipa tehnica alocata acestui proiect, detine multiple certificari care atesta nivelul inalt de pregatire pentru efectuarea acestui proiect, dintre care mentionam: **C|EH** - Certified Ethical Hacker (EC-COUNCIL) **LPT** - Licensed Penetration Tester (EC-COUNCIL) **OSCP** - Offensive Security Certified Professional (Offensive Security) **OSWP** – Offensive Security Wireless Professional (Offensive Security) **QUALYSGuard** - Qualys Guard Certified Specialist – Vulnerability Management **GISCP** - Global Industrial Cyber Security Professional

		CSSLP – Certified Secure Software Lifecycle Professional (ISC2) **CRISC** - Certified in Risk and Information Systems Control **ECSA** - EC Council Certified Security Analyst **CISSP** – Certified Information Systems Security Professional (ISC2) **CompTIA Security+** **CompTIA Linux+** **CISA** - Certified Information Systems Auditor (ISACA) **CISM** - Certified Information Security Manager **CIPP/IT** - Certified Information Privacy Professional/Information Technology **CPSSE** - Certified Professional for Secure Software Engineering

2.3.3 Ofertantul va trebui să dețină și să utilizeze echipamente și aplicații dedicate pentru identificarea și obținerea informațiilor despre sistemele informatice țintă, identificarea de vulnerabilități, și formularea unor recomandări de remediere.	DA	SAFETECH INNOVATIONS deține și utilizeaza echipamente și aplicații dedicate pentru identificarea și obținerea informațiilor despre sistemele informatice țintă, identificarea de vulnerabilități, și formularea unor recomandări de remediere.

2.3.4 Ofertantul va trebui să dețină proceduri de lucru conforme standardelor în domeniu, prin care este redus riscul de a afecta sistemele informatice aflate în scopul testării.	DA	**SAFETECH INNOVATIONS** a obtinut urmatoarele certificari emise de **MOODY INTERNATIONAL**: ● Management System Certified Against **BS ISO/IEC 27001:2013** - Standardul care reglementeaza politicile si procedurile de securitate la nivel de organizatie sau unitate functionala; astfel se atesta ca organizatia a implementat un sistem standardizat de management al securitatii ● Management System Certified Against **ISO/IEC 20000-1:2011** - Standardul international pentru managementul serviciilor IT, atat interne, cat si externe. ● Management System Certified Against **ISO 9001:2015** - Certificarea care stabileste standardele pentru sistemul de management al calitatii, dar si pentru sistemul de management, in general. ● Management System Certified Against **OHAS 18001:2007 -** Certificarea care demonstreaza orientarea companiei catre un mediu de lucru sigur prin integrarea sigurantei muncii in toate procesele existente, precum si protejarea angajatilor impotriva accidentelor de munca. Management System Certified Against **ISO 14001:2015** - Standardul care specifica procesele necesare pentru controlul si imbunatatirea actiunilor companiei cu privire la mediul inconjurator In ceea ce priveste efectuarea testelor de penetrare, echipa tehnica lucreaza dupa metodologii internationale, cum ar fi: • The Penetration Testing Execution Standard – PTES; • National Institute of Standards and Technology – NIST; • Open Source Security Testing Methodology – OSSTM; • Open Information Systems Security Group - OISSG; • Open Web Application Security Project - OWASP. Aceste metodologii adoptate de catre expertii nostri, cat si vasta experienta dobandita in proiecte complexe, atesta faptul ca riscul de a afecta sistemele testate este foarte scazut.

2.4. Cerințe față de etapele procedurii de evaluare și testare

Serviciile de penetrare și evaluare a vulnerabilităților informatice în cadrul SI al BNM prin teste specifice de penetrare din exteriorul infrastructurii de rețea se vor derula în trei etape distincte, și anume: 1. Pre-evaluare (Pre-assesment) 2. Evaluare (Assesment) 3. Post-evaluare (Post-assesment)	DA	Serviciile de penetrare și evaluare a vulnerabilităților informatice în cadrul SI al BNM prin teste specifice de penetrare din exteriorul infrastructurii de rețea se vor derula în trei etape distincte, și anume: 1. Pre-evaluare (Pre-assesment) 2. Evaluare (Assesment) 3. Post-evaluare (Post-assesment)

2.4.1 Etapa de Pre-evaluare (Pre-assesment) - reprezintă faza premergătoare evaluării vulnerabilităților și este importantă pentru determinarea specificațiilor precise și a regulilor de desfășurare a evaluării. În această etapă se vor stabili și elabora Planul de testare, Planul de acțiuni (SOW – State of Work), precum și, scenariile de atac, și se vor obține autorizațiile necesare desfășurării testelor de penetrare. Această etapă se va desfășura pe parcursul numărului de zile lucrătoare stabilit în cadrul planului de proiect și se va finaliza cu elaborarea Planului de testare și a Planului de acțiuni (SOW – State of Work) în care se vor înscrie cel puțin: - activitățile întreprinse, - sistemele incluse în activitatea de testare, - termenul propus de realizare, - persoane responsabile atît din partea Beneficiarului, cît și a Prestatorului.	DA	**Etapa de Pre-evaluare (Pre-assesment)** În această etapă se vor stabili și elabora Planul de testare, Planul de acțiuni (SOW – State of Work), precum și, scenariile de atac, și se vor obține autorizațiile necesare desfășurării testelor de penetrare. In aceasta etapa se vor desfasura intalniri si discutii cu echipa de proiect a beneficiarului pe urmatoarele subiecte: - Intelegerea scopului testarii (ce aplicatii, ce componente/module trebuie testate) - Intelegerea motivatiei beneficiarului (ce isi propune sa obtina in urma acestui test, care este motivatia testului - a avut incidente de securitate, are cerinte de conformitate, are cerinte legale pe care trebuie sa le indeplineasca, s.a. -) - Care sunt datele considerate sensibile de catre beneficiar - Care sunt tehnologiile utilizate de catre sistem - Daca testele vor fi efectuate pe mediul de productie sau pe mediul de testare - Daca exista mecanisme suplimentare de protectie (Web Application Firewall, IDS/IPS) - Daca exista restrictii de interval orare cand testele nu trebuie sa se desfasoare - Daca sunt implicate terte-parti (operatori de servicii, ISP, etc.) care ar trebui notificati de derularea unor teste de securitate <u>Definirea domeniului de evaluare</u> La initierea proiectului, impreuna cu beneficiarul, se va delimita aria de acoperire a domeniului de evaluare. Se vor stabili modalitatile de simulare a atacurilor: - *blackbox* (fara a avea nici un fel de date despre obiectul auditat); - *whitebox* (avand la dispozitie informatii despre sistemul tinta). In vederea obtinerii unor rezultate optime, se recomanda corelarea rezultatelor din ambele modalitati de analiza. Stabilirea nivelului de agresivitate al atacului: cat de departe se va merge cu tentativele de exploatare a unei vulnerabilitati.

		<u>Colectare informatii publice disponibile despre sistemul informatic al companiei</u> Informatiile continute pe site-ul beneficiarului, informatii continute in inregistrarile Whois, DNS, RNC; Informatii despre sistemul informatic al beneficiarului ce se pot obtine din alte surse. Această etapă se va desfășura pe parcursul numărului de zile lucrătoare stabilit în cadrul planului de proiect care va fi dezvoltat in colaborare cu beneficiarul și se va finaliza cu elaborarea Planului de testare și a Planului de acțiuni (SOW – State of Work) în care se vor înscrie cel puțin: - activitățile întreprinse, - sistemele incluse în activitatea de testare, - termenul propus de realizare, - persoane responsabile atît din partea Beneficiarului, cît și a Prestatorului.

2.4.2. Etapa de Evaluare (Assesment) - reprezintă etapa de identificare și evaluare a vulnerabilităților de securitate a sistemelor informatice. Această etapă a testării include evaluarea conectivității între sistemele utilizate pentru test și sistemele testate, culegerea informațiilor despre sistemele testate din domeniul public și privat, descoperirea sistemelor și serviciilor active, precum și, scanarea sistemelor pentru descoperirea vulnerabilităților. Utilizînd informațiile descoperite în evaluarea vulnerabilităților, se vor construi arbori de atac și se vor implementa acțiunile definite în aceste structuri. Scanarea vulnerabilităților și implementarea testului de penetrare va include, dar nu se va limita la analiza următoarelor vulnerabilități ale aplicațiilor: ● Injectarea de cod malițios ● Managementul defectuos al procesului de autentificare și al sesiunii de lucru ● Cross-Site Scripting (XSS) ● Referențierea directă a obiectelor în mod nesecurizat ● Erori privind configurația de securitate ● Tratarea erorilor în mod nesecurizat și lipsa de măsuri de protecție a informațiilor sensibile ● 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 aflate în scop la un atac de tip Denial of Service (DoS)	DA	**Etapa de Evaluare (Assesment)** - reprezintă etapa de identificare și evaluare a vulnerabilităților de securitate a sistemelor informatice. Această etapă a testării include evaluarea conectivității între sistemele utilizate pentru test și sistemele testate, culegerea informațiilor despre sistemele testate din domeniul public și privat, descoperirea sistemelor și serviciilor active, precum și, scanarea sistemelor pentru descoperirea vulnerabilităților. Utilizînd informațiile descoperite în evaluarea vulnerabilităților, se vor construi arbori de atac și se vor implementa acțiunile definite în aceste structuri. Scanarea vulnerabilitatilor si implementarea testului de penetrare va include in mod minimal analiza urmatoarelor vulnerabilitati ale aplicatiilor tinta: ● Injectarea de cod malițios ● Managementul defectuos al procesului de autentificare și al sesiunii de lucru ● Cross-Site Scripting (XSS) ● Referențierea directă a obiectelor în mod nesecurizat ● Erori privind configurația de securitate ● Tratarea erorilor în mod nesecurizat și lipsa de măsuri de protecție a informațiilor sensibile ● 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 aflate în scop la un atac de tip Denial of Service (DoS) Pentru o lista completa de teste, va rugam sa consultati documentul atasat: **Metodologii de testare**

În privința managementului sesiunii de lucru se vor identifica cel puțin următoarele aspecte: ● Implementarea managementului sesiunii printr-un Framework cunoscut și de încredere, care a fost testat în practică din punct de vedere al securității. ● Procesul de generare a identificatorilor de sesiune și protecția acestora împotriva abuzurilor. ● Procesul de generare a cookie-urilor ce conțin generatori de sesiune și stabilire a atributelor acestora. ● Procesul de creare și terminare a sesiunii și identificatorilor din perspectiva server și client. ● Intervaluri de inactivitate și posibilitatea de inițializare de multiple sesiuni active. ● Măsurile implementate pentru păstrarea confidențialității informațiilor privind autentificarea și sesiunea de lucru. ● Implementarea de măsuri adiționale de securitate pentru operațiile sensibile, precum cele administrative.	DA	În privința managementului sesiunii de lucru se vor identifica cel puțin următoarele aspecte: ● Implementarea managementului sesiunii printr-un Framework cunoscut și de încredere, care a fost testat în practică din punct de vedere al securității. ● Procesul de generare a identificatorilor de sesiune și protecția acestora împotriva abuzurilor. ● Procesul de generare a cookie-urilor ce conțin generatori de sesiune și stabilire a atributelor acestora. ● Procesul de creare și terminare a sesiunii și identificatorilor din perspectiva server și client. ● Intervaluri de inactivitate și posibilitatea de inițializare de multiple sesiuni active. ● Măsurile implementate pentru păstrarea confidențialității informațiilor privind autentificarea și sesiunea de lucru. ● Implementarea de măsuri adiționale de securitate pentru operațiile sensibile, precum cele administrative. Pentru o lista completa de teste care vor fi efectuate pe parcursul desfasurarii activitatii, va rugam sa consultati documentul atasat: **Metodologii de testare**

În privința configurației de securitate se vor identifica cel puțin următoarele aspecte: ● Versiunile de software ale serverelor, platformelor de dezvoltare a aplicației și componentelor sistemului. ● Existența actualizărilor de securitate aflate pe serverele, platformele de dezvoltare a aplicației și componentele sistemului. ● Existența configurațiilor prestabilite de la producătorul sistemului, cum ar fi utilizatori și parole implicite. ● Utilizatorii de aplicații și configurația acestora. ● Metodele și extensiile protocolului HTTP folosite în cadrul sistemului. ● Informații relevante ce se afla în header-ul HTTP. ● Existența mecanismelor de criptare pentru autentificarea în cadrul sistemelor și transmisia de informații.	DA	În privința configurației de securitate SAFETECH INNOVATIONS va identifica cel puțin următoarele aspecte: ● Versiunile de software ale serverelor, platformelor de dezvoltare a aplicației și componentelor sistemului. ● Existența actualizărilor de securitate aflate pe serverele, platformele de dezvoltare a aplicației și componentele sistemului. ● Existența configurațiilor prestabilite de la producătorul sistemului, cum ar fi utilizatori și parole implicite. ● Utilizatorii de aplicații și configurația acestora. ● Metodele și extensiile protocolului HTTP folosite în cadrul sistemului. ● Informații relevante ce se afla în header-ul HTTP. ● Existența mecanismelor de criptare pentru autentificarea în cadrul sistemelor și transmisia de informații Pentru o lista completa de teste care vor fi efectuate pe parcursul desfasurarii activitatii, va rugam sa consultati documentul atasat: **Metodologii de testare**
În privința tratării erorilor de sistem și protejării informațiilor sensibile se vor identifica cel puțin următoarele aspecte: ● Identificarea posibilității ca aplicațiile să divulge informații sensibile, inclusiv detalii despre sistem, identificatori de sesiune sau informații despre cont, în mesaje de erori. ● Conținutul mesajelor de eroare din punct de vedere tehnic.	DA	În privința tratării erorilor de sistem și protejării informațiilor sensibile se vor identifica cel puțin următoarele aspecte: ● Identificarea posibilității ca aplicațiile să divulge informații sensibile, inclusiv detalii despre sistem, identificatori de sesiune sau informații despre cont, în mesaje de erori. ● Conținutul mesajelor de eroare din punct de vedere tehnic. Pentru o lista completa de teste care vor fi efectuate pe parcursul desfasurarii activitatii, va rugam sa consultati documentul atasat: **Metodologii de testare**

În privința managementului accesului se vor identifica cel puțin următoarele aspecte: ● Procesul de identificare, autentificare si autorizare a accesului la informații. ● Identificarea credențialelor hard-codate în sisteme, dacă acestea există. ● Identificarea utilizatorilor și credențialelor de acces stocate în fișiere de configurație în clar. ● Identificarea credențialelor transmise in clar, daca este cazul. ● Identificarea rolurilor de acces și maparea acestora pe drepturi și posibilitatea de ocolire a acestora pentru a obține acces neautorizat la informații. ● Identificarea metodelor HTTP folosite în procesul de autentificare.	DA	În privința managementului accesului se vor identifica cel puțin următoarele aspecte: ● Procesul de identificare, autentificare si autorizare a accesului la informații. ● Identificarea credențialelor hard-codate în sisteme, dacă acestea există. ● Identificarea utilizatorilor și credențialelor de acces stocate în fișiere de configurație în clar. ● Identificarea credențialelor transmise in clar, daca este cazul. ● Identificarea rolurilor de acces și maparea acestora pe drepturi și posibilitatea de ocolire a acestora pentru a obține acces neautorizat la informații. ● Identificarea metodelor HTTP folosite în procesul de autentificare Pentru o lista completa de teste care vor fi efectuate pe parcursul desfasurarii activitatii, va rugam sa consultati documentul atasat: **Metodologii de testare**
În privința validării parametrilor de intrare se vor identifica cel puțin următoarele aspecte: ● Filtrarea și validarea datelor provenite din afara sistemelor ● Existența unei metode centralizate de validare a datelor în sistem. ● Existența unor seturi de caractere corespunzătoare pentru datele de intrare ● Codificarea datelor într-un set comun de caractere înainte de validare ● Validarea datelor provenite de la utilizatori, înainte de procesarea acestora, inclusiv toți parametrii, conținutul URL si HTTP.	DA	În privința validării parametrilor de intrare SAFETECH INNOVATIONS va identifica cel puțin următoarele aspecte: ● Filtrarea și validarea datelor provenite din afara sistemelor ● Existența unei metode centralizate de validare a datelor în sistem. ● Existența unor seturi de caractere corespunzătoare pentru datele de intrare ● Codificarea datelor într-un set comun de caractere înainte de validare ● Validarea datelor provenite de la utilizatori, înainte de procesarea acestora, inclusiv toți parametrii, conținutul URL si HTTP. Pentru o lista completa de teste care vor fi efectuate pe parcursul desfasurarii activitatii, va rugam sa consultati documentul atasat: **Metodologii de testare**

Pentru validarea datelor de intrare se vor verifica: ● tipurile de date așteptate (integer, string etc,) ● setul de date ● lungimea datelor ● Implementarea de măsuri suplimentare de control pentru caractere cu potențial riscant (< > " ' % ( ) & + \ \' \")	DA	Pentru validarea datelor de intrare se vor verifica: ● tipurile de date așteptate (integer, string etc,) ● setul de date ● lungimea datelor ● Implementarea de măsuri suplimentare de control pentru caractere cu potențial riscant (< > " ' % ( ) & + \ \' \") Pentru o lista completa de teste care vor fi efectuate pe parcursul desfasurarii activitatii, va rugam sa consultati documentul atasat: **Metodologii de testare**
Testarea securității la nivelul infrastructurii Wi-Fi va include, dar nu se va limita la : ● Descoperirea rețelelor Wi-Fi și punctelor de acces atît cunoscute cît și neautorizate ● Identificarea dispozitivelor care interacționează cu rețeaua ● Colectarea de informații despre puterea de rețea, protocoale de securitate și a dispozitivelor conectate ● Atacul și penetrarea rețelelor criptate cu WEP, WPA-PSK si WPA2-PSK ● Impersonare SSID ● Atacuri de tip Man-in-the-middle (MITM) ● Monitorizare automată trafic pentru a găsi fluxuri de date sensibile ● Aderarea la rețelele compromise și testarea sistemelor de backend ● Raportare cuprinzătoare a activităților de testare a rețelelor de tip Wi-Fi	DA	SAFETECH INNOVATIONS va efectua testarea securității la nivelul infrastructurii Wi-Fi va include, dar nu se va limita la : ● Descoperirea rețelelor Wi-Fi și punctelor de acces atît cunoscute cît și neautorizate ● Identificarea dispozitivelor care interacționează cu rețeaua ● Colectarea de informații despre puterea de rețea, protocoale de securitate și a dispozitivelor conectate ● Atacul și penetrarea rețelelor criptate cu WEP, WPA-PSK si WPA2-PSK ● Impersonare SSID ● Atacuri de tip Man-in-the-middle (MITM) ● Monitorizare automată trafic pentru a găsi fluxuri de date sensibile ● Aderarea la rețelele compromise și testarea sistemelor de backend ● Raportare cuprinzătoare a activităților de testare a rețelelor de tip Wi-Fi Expertii SAFETECH INNOVATIONS detin certificarea Offensive Security Wireless Proffessional care atesta nivelul de pregatire profesionala pentru testarea securitatii retelelor WiFi si vor aplica pe parcusul testelor cele mai bune practici in domeniu, care includ testele enumerate mai sus si utilizarea uneltelor specifice acestui tip de teste de penetrare. O lista de unelte utilizate se regaseste in documentul atasat: **Lista unelte Penetration Testing**

Scanarea vulnerabilităților și implementarea testului de penetrare la nivelul rețelei va include, dar nu se va limita la : Obținerea informațiilor din domeniul public; ● Scanarea sistemelor din SOW; ● Tehnici de enumerare; ● Obținerea accesului neautorizat prin exploatarea vulnerabilităților; ● Consolidarea accesului; ● Ștergerea tuturor fișierelor utilizate în cadrul atacului și a altor dovezi ale accesului; ● Aplicații software utilizate în cursul testării; ● Aplicații pentru culegerea de informații din domeniul public; ● Aplicații necesare identificării sistemelor și serviciilor active; ● Scannere de vulnerabilități specifice sistemelor și rețelelor incluse în Planul de acțiuni (SOW - State of Work); ● Aplicații necesare exploatării vulnerabilităților descoperite.	DA	Scanarea vulnerabilităților și implementarea testului de penetrare la nivelul rețelei va include, dar nu se va limita la : Obținerea informațiilor din domeniul public; ● Scanarea sistemelor din SOW; ● Tehnici de enumerare; ● Obținerea accesului neautorizat prin exploatarea vulnerabilităților; ● Consolidarea accesului; ● Ștergerea tuturor fișierelor utilizate în cadrul atacului și a altor dovezi ale accesului; ● Aplicații software utilizate în cursul testării; ● Aplicații pentru culegerea de informații din domeniul public; ● Aplicații necesare identificării sistemelor și serviciilor active; ● Scannere de vulnerabilități specifice sistemelor și rețelelor incluse în Planul de acțiuni (SOW - State of Work); ● Aplicații necesare exploatării vulnerabilităților descoperite.

Prin testarea automată va trebui să se detecteze cel puțin următoarele tipuri de vulnerabilități: ● Parole inițiale neschimbate pe echipamente ● Posibilitatea de acces în sistem fără autentificare, cu autentificare cu credențiale inițiale sau credențiale ușor de ghicit ● Configurații inițiale neschimbate pe echipamente ● Corecții și actualizări de securitate neimplementate ● Escaladarea privilegiilor ● Software cu versiuni vechi și foarte vechi ce prezintă vulnerabilități ● Buffer Overflow ● Negarea accesului la serviciu (DoS Denial of Service) ● Remote Code Execution ● Posibilitatea injectării de comenzi sau scripturi în servere web, servere de aplicații și baze de date ● Directory Traversal ● File and Path Disclosure ● Cross Site Scripting (XSS) ● Cross Site Request Forgery (CSRF) ● Configurarea defectuoasă a serverelor ● Managementul defectuos al sesiunilor și autentificării ● Parametri de intrare nevalidați ● Control al accesului defectuos ● Tratarea defectuoasă a erorilor	DA	Solutia de testare automata utilizata (Rapid7 Nexpose) va detecta cel putin urmatoarele tipuri de vulnerabilitati: ● Parole initiale neschimbate pe echipamente ● Posibilitatea de access in sistem fara autentificare, cu autentificare cu credentiale initiale sau credentiale usor de ghicit ● Configuratii initiale neschimbate pe echipamente ● Corectii si actualizari de securitate neimplementate ● Escaladarea privilegiilor ● Software cu versiuni vechi si foarte vechi ce prezinta vulnerabilitati ● Buffer Overflow ● Negarea accesului la serviciu (DoS Denial of Service) ● Remote Code Execution ● Posibilitatea injectarii de comenzi sau scripturi in servere web, servere de aplicatii si baze de date ● Directory Traversal ● File and Path Disclosure ● Cross Site Scripting (XSS) ● Cross Site Request Forgery (CSRF) ● Configurarea defectuoasa a serverelor ● Managementul defectuos al sesiunilor si autentificarii ● Parametri de intrare nevalidati ● Control al accesului defectuos ● Tratarea defectuoasa a erorilor
Soluția de testare automată utilizată trebuie să fie capabilă să integreze capabilitățile de descoperire și remediere a vulnerabilităților cu informații despre *aplicațiile malware* prezente în infrastructură, cît și toate aplicațiile malware cunoscute cu ajutorul cărora se pot exploata vulnerabilitățile prezente și ușurința cu care aceste vulnerabilități se pot exploata.	DA	Solutia de testare automata utilizata (Rapid7 Nexpose) este capabilă să integreze capabilitățile de descoperire și remediere a vulnerabilităților cu informații despre *aplicațiile malware* prezente în infrastructură, cît și toate aplicațiile malware cunoscute cu ajutorul cărora se pot exploata vulnerabilitățile prezente și ușurința cu care aceste vulnerabilități se pot exploata. Pentru fiecare vulnerabilitate detectata, Rapid7 Nexpose indica daca exista exploituri publice cunoscute si referinte catre acestea, cat si existenta unor

		programe malware care exploateaza acea vulnerabilitate.
Această etapă se va desfășura pe parcursul numărului de zile lucrătoare stabilit în cadrul planului de proiect și se va finaliza cu elaborarea de către Prestator a rapoartelor de test care vor include toate problemele și vulnerabilitățile descoperite pe parcursul testării.	DA	Etapa de Evaluare (Assesment) se va desfășura pe parcursul numărului de zile lucrătoare stabilit în cadrul planului de proiect și se va finaliza cu elaborarea de către SAFETECH INNOVATIONS a rapoartelor de test care vor include toate problemele și vulnerabilitățile descoperite pe parcursul testării.

2.4.3 Etapa de Post-evaluare (Post-assesment) - această etapă se va desfășura pe parcursul numărului de zile lucrătoare stabilit în cadrul planului de proiect și se va finaliza cu elaborarea de către Prestator a rapoartelor de analiză, a rezultatelor testelor efectuate în care se vor identifica și vor fi incluse cele mai bune măsuri și metode de remediere a problemelor și vulnerabilităților descoperite, în funcție de severitate și impact.	DA	**Etapa de Post-evaluare (Post-assesment)** - această etapă se va desfășura pe parcursul numărului de zile lucrătoare stabilit în cadrul planului de proiect și se va finaliza cu elaborarea de către SAFETECH INNOVATIONS a rapoartelor de analiză, a rezultatelor testelor efectuate în care se vor identifica și vor fi incluse cele mai bune măsuri și metode de remediere a problemelor și vulnerabilităților descoperite, în funcție de severitate și impact. Rezultatele obtinute in urma testelor de securitate vor fi detaliate intr-un raport care va cuprinde: • Sumar Executiv; • Obiectivele si scopul evaluarii; • Prezentare succinta a metodologiei utilizate; • Descrierea contextului in care s-a desfasurat evaluarea; • Prezentarea individuala a vulnerabilitatilor descoperite dupa cum urmeaza: o descrierea vulnerabilitatii; o catalogarea vulnerabilitatii; o descrierea tehnica; o analiza severitatii si probabilitatii; o calcularea riscului; o contramasuri recomandate pentru remediere; • Alte detalii si recomandari; • Anexa cu lista testelor de securitate efectuate;

În această etapă Prestatorul va acorda suport Beneficiarului pentru înțelegerea deplină a problemelor identificate și alegerea măsurilor/metodelor aplicabile pentru remedierea acestora (din cadrul celor propuse), în scopul minimizării riscurilor de securitate informatică asociate problemelor și vulnerabilităților descoperite. Totodată Prestatorul va efectua test de penetrare repetat la resursele cu probleme identificate pentru a verifica daca au fost aplicate corect măsurile/metodele de remediere.	DA	În această etapă SAFETECH INNOVATIONS va acorda suport Beneficiarului pentru înțelegerea deplină a problemelor identificate și alegerea măsurilor/metodelor aplicabile pentru remedierea acestora (din cadrul celor propuse), în scopul minimizării riscurilor de securitate informatică asociate problemelor și vulnerabilităților descoperite. Totodată SAFETECH INNOVATIONS va efectua teste de penetrare repetate la resursele cu probleme identificate pentru a verifica daca au fost aplicate corect măsurile/metodele de remediere.
2.5 Cerințe față de livrabilele proiectului		
Ca urmare a serviciilor prestate, Ofertantul selectat va oferi cel puțin următoarele livrabile: ● Plan de proiect;	DA	SAFETECH INNOVATIONS va dezvolta un plan de proiect in urma consultarilor cu beneficiarul, la inceputul proiectului.
● Plan de testare;	DA	SAFETECH INNOVATIONS va dezvolta un plan de testare in urma colectarii de informatii relevante despre sistemele aflate in scop, intelegerea motivatiei beneficiarului (ce isi propune sa obtina in urma acestui test, care este motivatia testului - a avut incidente de securitate, are cerinte de conformitate, are cerinte legale pe care trebuie sa le indeplineasca s.a., care sunt datele considerate sensibile de catre beneficiar, care sunt tehnologiile utilizate de catre sistem, s.a. Pentru o lista completa de teste, va rugam sa consultati documentul atasat: **Metodologii de testare**
● Planul de acțiuni (SOW – Scope of Work);	DA	SAFETECH INNOVATIONS va dezvolta un Plan de acțiuni (SOW – Scope of Work), in etapa de Preassessment.

• Rapoarte de test care vor include toate problemele și vulnerabilitățile detectate pe parcursul testării, catalogate în funcție de gravitatea lor;	DA	SAFETECH INNOVATIONS va dezvolta Rapoarte de test care vor include toate problemele și vulnerabilitățile detectate pe parcursul testării, catalogate în funcție de gravitatea lor; Un model de raport (demo) poate fi consultat documentul atasat: **Model raport testare**
• 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/măsuri/metode ce trebuie întreprinse/luate/folosite pentru eliminarea sau micșorarea riscului generat de vulnerabilitățile detectate.	DA	SAFETECH INNOVATIONS va dezvolta 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/măsuri/metode ce trebuie întreprinse/luate/folosite pentru eliminarea sau micșorarea riscului generat de vulnerabilitățile detectate. Un model de raport (demo) poate fi consultat documentul atasat: **Model raport testare**

Rapoartele furnizate de Prestator 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. *Partea tehnică* va detalia din punct de vedere tehnic problemele și vulnerabilitățile identificate. Partea tehnică 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,) 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.	DA	SAFETECH INNOVATIONS va dezvolta rapoartele care 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. *Partea tehnică* va detalia din punct de vedere tehnic problemele și vulnerabilitățile identificate. Partea tehnică 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,) 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.	DA	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.