Caiet de Sarcini pentru

Servicii de audit informatic pentru identificarea și evaluarea vulnerabilităților și riscurilor informatice în conformitate cu Legea 362 / 2018 (NIS)

COD CPV 72810000-1

LEGEA nr. 362 / 2018 stabileşte cadrul juridic şi instituţional, măsurile şi mecanismele necesare în vederea asigurării unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice. Printre articolele esenţiale ale legii, operatorilor de servicii esenţiale le revine anumite obligaţii în scopul asigurării securităţii reţelelor şi sistemelor informatice.
Astfel, conform legii, Romgaz, trebuie să implementeze măsuri tehnice şi organizatorice adecvate şi proporţionale pentru îndeplinirea cerinţelor minime de securitate în domenii precum: Guvernanța de securitate, Protecţia reţelelor și sistemelor informatice, apărarea cibernetică şi rezilienţa serviciilor.

De asemenea există obligaţia legală de a preveni şi minimiza impactul incidentelor care afectează securitatea reţelelor şi a sistemelor informatice utilizate pentru furnizarea acestor servicii esenţiale, cu scopul dea asigura continuitatea serviciilor respective şi de a notifica la DNSC (Directoratul Național de Securitate Cibernetică) incidentele cu un impact semnificativ.

Serviciile de audit informatic de tip penetration testing sunt cea mai eficientă metodă de evaluare a securităţii unei infrastructuri IT, prin încercarea în condiţii de siguranţă de a identifica şi exploata vulnerabilităţile sistemului, inclusiv defectele sistemelor, reţelelor, serviciilor şi aplicaţiilor, configuraţiile necorespunzătoare şi chiar comportamentul riscant al utilizatorilor finali.

Începând cu data de 14 mai 2021, în baza Deciziei 5401/II/A a Directorului General al Centrului National de Răspuns la Incidente de Securitate Cibernetică-CERT-RO, SNGN Romgaz SA a fost înscrisă în Registrul Operatorilor de Servicii Esenţiale (ROSE).

Activitățile de audit de securitate necesare conformității cu Legea 362/2018 respectând cerințele Ordinului nr. 1323 / 2020 pentru aprobarea Normelor tehnice privind cerințele minime de asigurare a securității rețelelor și sistemelor informatice aplicabile operatorilor de servicii esențiale sunt:

a) activități speciale:
   i) Auditul de penetrare sau testarea de penetrare [AS4]
b) activități comune:
   i) Auditul arhitecturii [AS1]
   ii) Auditul de configurare [AS2]
   iii) Auditul securității organizației [AS5]
c) Activitati mixte
   i) Auditul sistemelor de control industrial [AS6]

Astfel Romgaz dorește să achiziționeze următoarele servicii:

1. Servicii de audit de securitate în conformitate cu cerințele din Legea 362 / 2018
2. Servicii de audit informatic de tip penetration testing pentru identificarea și evaluarea vulnerabilităților și riscurilor informatice

Având minim următoarele caracteristici:

1. Servicii de audit de securitate în conformitate cu cerințele din Legea 362 / 2018

În conformitate cu art. 10 alin. (4) din Legea nr. 362/2018 termenul de conformare a operatorilor de servicii esențiale privind implementarea măsurilor tehnice de securitate este de 6 luni de la data intrării în vigoare a normelor tehnice privind cerințele de securitate și notificare ori, după caz, de la data înscrierii în Registrul operatorilor de servicii esențiale.

Pentru implementarea cerințelor minime de securitate în rețelele și sistemele informatice care asigură furnizarea serviciilor esențiale ori furnizează serviciile digitale identificate în temeiul "Legii NIS" dar și pentru desfășurarea activității de audit de securitate a rețelelor și sistemelor informatice aparținând operatorilor de servicii esențiale sau furnizorilor de servicii digitale, DNSC a aprobat Lista standardelor și specificațiilor europene și internaționale care este aplicabilă atât operatorilor de servicii esențiale și furnizorilor de servicii digitale, cât și auditorilor de securitate a rețelelor și sistemelor informatice (Decizia nr. 88/2020 privind aprobarea Listei standardelor și specificațiilor europene și internaționale) În implementarea Cerințelor minime de securitate, grupate pe domenii

care includ cerințe și activități specifice, abordarea trebuie să fie globală și nu secvențială: măsurile de securitate trebuie privite în ansamblu, luând în considerare corelarea lor pentru o implementare eficientă și cronologică.

Pentru implementarea cu succes a cerințelor și obținerea unor asigurări rezonabile cu privire la asigurarea conformității, este critică implicarea personalului operatorului de servicii esențiale sub coordonarea responsabilului NIS, atât prin conștientizarea rolului și responsabilităților acestora, cât și prin instruire continuă.

Procesele si procedurile interne create (considerate controale administrative), precum și implementarea acestora însoțite de măsuri tehnice (considerate controale tehnice) sunt verificate și asumate la nivelul managementului OSE (Operator de Servicii Esențiale): prin audituri interne și externe și prin testarea și evaluarea periodică.

În cadrul auditului de conformitate vor fi revizuite **58 de cerințe de securitate, grupate pe 4 domenii** (Guvernanță, Protecție, Apărare cibernetică, Reziliență) așa cum sunt acestea impuse prin Ordinul nr. 1323/2020 și inspectarea fizică a amplasamentelor echipamentelor.

Auditul de conformitate a securității cibernetice este o activitatea prin care se realizează o evaluare sistematică a tuturor politicilor, procedurilor și măsurilor de protecție implementate la nivelul rețelelor și sistemelor informatice în vederea identificării disfuncțiilor și vulnerabilităților și a furnizării unor soluții de remediere a acestora prin raportare la cerințele Ordinului 1323/2020.

Obiectivele auditului sunt stabilite în conformitate cu legislația aplicabilă, după cum urmează:

- ✓ se verifică dacă au fost identificate corect rețelele și sistemele informatice de auditat, precum și interdependențele externe ale rețelelor și sistemelor informatice;
- ✓ se revizuie decizia și mapa de acreditare;
- ✓ se verifică plauzibilitatea metodologiei/tehnicilor utilizate, precum și măsurile de control implementate în vederea gestionării riscurilor operaționale identificate;
- ✓ se identifică existența și se determină eficacitatea politicilor și procedurilor de operare așa cum sunt acestea specificate în legislație și standardele adoptate de către OSE (Operator de Servicii Esențiale);
- ✓ se identifică existența și să determină eficacitatea controalelor tehnice.

pentru serviciile esențiale identificate în cadrul SNGN Romgaz SA

Tehnicile de audit implicate în timpul misiunii includ:

- ✓ **Examinare**: politici, proceduri, instrucțiuni de lucru, cerințe din bune practici sau de la producător, mecanisme, observarea directă a unui proces/activitate.
- ✓ **Interviuri** cu persoanele responsabile de executarea unei activități sau managementului unui proces.
- ✓ **Testarea** prin care se asigură că rezultatul unui proces este cel declarat și asumat.

1.1. Auditul arhitecturii [AS1]

Constă în verificarea conformității măsurilor de securitate legate de alegerea, poziționarea și implementarea dispozitivelor hardware/software în rețelele și sistemele informatice, cerințele minime de securitate și politicile interne ale operatorului economic. Auditul se va realiza și pentru interconectările cu rețele terțe, inclusiv Internetul;

1.2. Auditul de configurare [AS2]

Constă în verificarea implementării măsurilor de securitate în conformitate cu stadiul tehnicii, cerințele minime de securitate și politicile de securitate în ceea ce privește configurația dispozitivelor hardware/software componente ale rețelelor și sistemelor informatice. Aceste dispozitive sunt de

tipul echipamente de rețea, sisteme de operare (server sau stație de lucru), aplicații sau produse de securitate;

1.3. Auditul securității organizației [AS5]

Constă în auditul organizației cu privire la securitatea logică și fizică și urmărește să se asigure că politicile și procedurile de securitate definite de operatorul de servicii esențiale:

a) sunt conforme cu nevoile de securitate ale operatorului economic auditat, nivelul tehnologic și standardele în vigoare;
b) completează corect măsurile tehnice implementate;
c) sunt puse efectiv în practică.

1.4. Auditul sistemelor de control industrial [AS6]

Constă în evaluarea nivelului de securitate al unui sistem de control industrial și a dispozitivelor de control asociate. Evaluarea de securitate presupune aplicarea activităților de audit de la 1.1 la 1.3.

1.5. Livrabile

Prestatorul trebuie să întocmească un **Raport de audit de securitate a infrastructurii informatice** ce trebuie să cuprindă minim următoarele elemente:

- ✓ descrierea sistemelor auditate;
- ✓ descriere amenintari si vulnerabilitati identificate;
- ✓ analiza de risc aferenta amenintarilor identificate;
- ✓ analiza riscurilor implicate de activitate, a posibilelor vulnerabilităţi ale sistemului informatic auditat şi a măsurilor de reducere a riscurilor asociate;
- ✓ recomandari privind reducerea nivelului de risc (plan de masuri);
- ✓ evolutia nivelului de risc dupa aplicarea contramasurilor propuse;

2. Servicii de audit informatic de tip penetration testing pentru identificarea și evaluarea vulnerabilităților și riscurilor informatice

Serviciile de audit informatic de tip penetration testing sunt cea mai eficientă metodă de evaluare a securității unei infrastructuri IT prin încercarea în condiții de siguranță de a identifica și exploata vulnerabilitățile sistemului, inclusiv defectele sistemelor, rețelelor, serviciilor și aplicațiilor, configurațiile necorespunzătoare și chiar comportamentul riscant al utilizatorilor finali. În comparație cu scanarea vulnerabilităților (care face parte din orice test de penetrare), această abordare va elimina orice rezultate fals pozitive, iar procesul de atenuare va fi simplificat dintr-o perspectivă tehnică și din punctul de vedere al resurselor.

Analiza tehnică a securității sistemelor informatice existente în cadrul SNGN Romgaz SA trebuie efectuată prin derularea de teste de securitate efectuate din perspectiva unui atacator (extern) prin care să fie identificate eventualele breșe de securitate, cât și riscurile la care este supusă rețeaua informatică prin prisma acestora.

Prin testarea securității sistemelor informatice a SNGN Romgaz SA trebuie să fie asigurată identificarea posibilelor vulnerabilități existente la nivelul sistemelor hardware, bazelor de date și aplicațiilor software încorporate, furnizând echipelor care asigură operarea, întreținerea și dezvoltarea acestora recomandări/informații destinate remedierii vulnerabilităților identificate.

Prestatorul trebuie să efectueze testele de penetrare "pentest" prin evaluarea securității sistemelor informatice ale SNGN Romgaz SA prin simularea de atacuri informatice, prin exploatarea vulnerabilităților existente și cunoscute. Prestatorul trebuie să demonstreze exploatabilitatea vulnerabilităților identificate. Procesul trebuie să implice o analiză activă a sistemelor informatice pentru orice vulnerabilități existente care ar putea rezulta din configurația inadecvată și din breșe cunoscute sau necunoscute, hardware și software.

Prin efectuarea testelor de penetrare experții de securitate ai Prestatorului trebuie să analizeze comportamentul sistemelor informatice ale SNGN Romgaz SA în contextul diferitelor atacuri informatice, fiind analizate inclusiv vulnerabilitățile care pot exista în aplicațiile dezvoltate sau utilizate. Testele de penetrare complete trebuie să cuprindă atât teste automate cât și manuale. Testele automate trebuie să identifice erori de programare în aplicațiile utilizate și trebuie să fie efectuate cu ajutorul unor programe specializate (vulnerability scanners, fuzzers, code scanners, etc). Testele manuale trebuie să analizeze aspecte ale aplicațiilor care necesită intuiția umană, identificându-se erori logice de programare și vor analiza și confirma sau infirma rezultatele testelor automate.

În conformitate cu cerințele din LEGEA nr. 362 din 28 decembrie 2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice, REGULAMENTUL din 22 martie 2021 pentru atestarea și verificarea auditorilor de securitate cibernetică și Ordinul nr. 1323 / 2020 pentru aprobarea Normelor tehnice privind cerințele minime de asigurare a securității rețelelor și sistemelor informatice aplicabile operatorilor de servicii esențiale, auditurile necesare sunt:

2.1. Auditul de penetrare sau testarea de penetrare [AS4]

Constă în identificarea vulnerabilităților din rețelele și sistemele informatice și verificarea posibilităților de exploatare a acestora, precum și a impactului exploatării acestora asupra rețelei, în condițiile reale ale unui atac cibernetic asupra rețelelor și sistemelor informatice.

Activitatea de audit poate fi desfășurată fie din afara rețelei (în special din internet sau din rețeaua interconectată a unei terțe părți), fie din interiorul rețelei și reprezintă o activitate care trebuie efectuată în complementaritate cu alte activități de audit pentru a le îmbunătăți eficacitatea sau pentru a demonstra fezabilitatea exploatării vulnerabilităților descoperite.

În funcție de tipul de sistem vizat, se vor efectua teste specifice în conformitate cu standardele de securitate relevante:

- ✓ Activitățile realizate pentru testele de penetrare la nivelul rețelei
- ✓ Activitățile realizate pentru testele de penetrare la nivelul aplicațiilor web
- ✓ Activitățile realizate pentru testele de penetrare la nivelul infrastructurilor IT/OT
- ✓ Activitățile realizate pentru testele de penetrare la nivelul aplicațiilor mobile (Android /
- ✓ iOS)
- ✓ Activitățile realizate pentru testele de penetrare la nivelul infrastructurilor Cloud

2.2. Activitățile realizate pentru testele de penetrare la nivelul rețelei

La nivelul rețelei, vor utiliza tehnici specifice in conformitate cu standardele de securitate naționale și internaționale reprezentate pentru:

- ✓ Recunoastere
- ✓ Testele firewall-ului
- ✓ Identificarea serviciilor disponibile
- ✓ Obținerea accesului neautorizat la credentiale
- ✓ Expunerea unor date sensibile pe motoarele de căutare sau pe internet
- ✓ Analiza specifică a vulnerabilității sistemelor din domeniul de aplicare

- ✓ Identificarea punctelor slabe ale arhitecturii
- ✓ Identificarea punctelor slabe în implementare / configurare
- ✓ Identificarea deficiențelor în proiectarea și implementarea politicilor de securitate
- ✓ Evaluarea proiectării și implementării VPN și a politicilor de acces la distanță
- ✓ Exploatarea vulnerabilităților specifice serviciilor expuse extern
- ✓ Cracking al principalelor conturi identificate folosind dicționare / tehnici de tip brute force / tehnici hibride / atacuri spray
- ✓ Atacurile de tip Man-in-the-Middle
- ✓ Identificarea a porților de acces la distanță nesigure (backdoors)

2.3. Activitățile realizate pentru testele de penetrare la nivelul aplicațiilor Web

La nivelul aplicațiilor web, auditorul va utiliza tehnici specifice pentru a identifica următoarele categorii de vulnerabilitati, in conformitate si cu standardul OWASP WSTG.
Pentru a păstra sensul tehnic al activităților realizate, ce este imposibil de reprodus în limba romana datorită lipsei unui nomenclator standard avizat, rapoartele se vor prezenta aceste elemente în limba engleză:

- ✓ Input Validation Attacks
- ✓ Access Control Attacks
- ✓ Authentication & Session
- ✓ Cross Site Scripting (XSS)
- ✓ Error Treatment / Sensitive Data Leakage
- ✓ Cracking of credentials
- ✓ Injection of arbitrary code
- ✓ Insecure Object References with LFI/RFI (Local/Remote File Inclusion)
- ✓ Overflows
- ✓ RCE (Remote Command Execution)
- ✓ Encryption and storage of information during application execution
- ✓ Setting errors in the applications and infrastructure
- ✓ Horizontal escalation of privileges
- ✓ Vertical escalation of privileges
- ✓ Predisposition and behavior in case of a Denial of Service (DoS) attack
- ✓ Public vulnerabilities of Common Gateway Interface (CGI)
- ✓ Inter-Domain Attacks (CSRF)
- ✓ Application specific vulnerabilities
- ✓ Application scanning with automated tools
- ✓ Enumeration technique
- ✓ Attacks on business logic
- ✓ Cryptography / Encryption attacks
- ✓ Framework-related attacks
- ✓ Non-validated forwardings
- ✓ Obtain unauthorized access by exploiting vulnerabilities
- ✓ Consolidation of acquisitions
- ✓ Removal of traces of the attack and other evidence of access
- ✓ Specific tests for the Web Services

Lista de mai sus va fi dezvoltată sau adaptata aplicațiilor aflate in scopul auditului, pe baza rezultatelor și observațiilor obținute în primele etape din audit. La nivel macro, orice test nou va face parte în cel puțin una dintre categoriile de mai jos:

- ✓ Strângerea de informații

- ✓ Testarea proceselor de Configurare, Implementare, Instalare si Actualizare
- ✓ Testarea managementului identității
- ✓ Testarea autentificării
- ✓ Testarea autorizării
- ✓ Testarea managementului sesiunii
- ✓ Testarea validării datelor
- ✓ Erori de manipulare
- ✓ Criptografie
- ✓ Testarea logicii fluxurilor operaționale și de business
- ✓ Testarea pe partea clientului

2.4. Activitățile realizate pentru testele de penetrare la nivelul infrastructurilor IT/OT

La nivelul infrastructurilor IT/OT, se vor utiliza tehnici specifice in conformitate cu standardele de securitate naționale și internaționale reprezentate pentru:

- ✓ Recunoaştere
- ✓ Scanări de rețea
- ✓ Scanează stații de lucru, servere si alte sisteme
- ✓ Scanări retele WIFI
- ✓ Maparea vulnerabilitatilor după risc si impact potențial în conformitate cu standardele internaționale și înțelegerea specialistilor nostri cu privire la riscurile companiei
- ✓ Maparea platformelor, erorilor software și configurațiilor neadecvate
- ✓ Identificarea vulnerabilităților cunoscute de tip CVE (Common Vulnerabilities and Exposure)
- ✓ Măsurarea efectelor
- ✓ Eliminarea rezultatelor de tip false positive

2.5. Activitățile realizate pentru testele de penetrare la nivelul infrastructurilor Cloud sau Datacenter

- ✓ Recunoastere
- ✓ Teste de penetrare specifice în funcție de tipul infrastructurii (exemplu SaaS, IaaS sau PaaS)
- ✓ Vulnerabilități în arhitectură, design și modelarea amenințărilor
- ✓ Puncte slabe în stocarea și protecția datelor
- ✓ Teste de penetrare în funcție de modul de orchestrare al serviciilor sau / si infrastructurii (eg. masini virtuale, containere, kubernetes)
- ✓ Teste de penetrare specifice comunicatiilor prin API
- ✓ Evaluarea politicilor de securitate și a configurațiilor sistemului Cloud
- ✓ Teste de penetrare specifice rețelelor și infrastructurilor Cloud, în funcție de furnizor

2.6. Livrabile

- ✓ Plan de testare;
- ✓ Planul de acțiuni (SOW – State of Work);
- ✓ Rapoarte de test care vor include toate problemele și vulnerabilitățile detectate pe parcursul testării, catalogate în funcție de gravitatea lor;
- ✓ Rapoarte de analiză, conținând analiza rezultatelor testelor efectuate în care trebuie să fie identificate și 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.

- ✓ Rapoartele furnizate de prestator trebuie să fie structurate în două părți distincte: partea executivă și partea tehnică. Partea executivă trebuie să conțină descrierea pe scurt a problemelor și vulnerabilităților identificate și trebuie să utilizeze metode grafice (cel puțin diagrame, grafice sau hărți). Partea tehnică trebuie să detalieze din punct de vedere tehnic problemele și vulnerabilitățile identificate.
- ✓ Partea tehnică trebuie să conțină 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:
  - 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 trebuie să cuprindă 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.

3. Principalele tehnici și metodologii folosite

Tehnicile și metodologiile utilizate pentru identificarea și evaluarea vulnerabilităților se bazează pe cele mai bune practici din domeniu, la nivel internațional, incluzând, dar fără a se limita la:

- ✓ LEGE nr. 362 din 28 decembrie 2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice
- ✓ REGULAMENT din 22 martie 2021 pentru atestarea și verificarea auditorilor de securitate cibernetică
- ✓ Ordinul nr. 1323/2020 pentru aprobarea Normelor tehnice privind cerințele minime de asigurare a securității rețelelor și sistemelor informatice aplicabile operatorilor de servicii esențiale.
- ✓ Information Systems Audit and Control Association – ISACA
- ✓ Penetration Testing Framework
- ✓ Penetration Testing Execution Standard
- ✓ OWASP
- ✓ LSSEINIS - Listei standardelor și specificațiilor europene și internaționale publicată în DECIZIA nr. 88 din 30 aprilie 2020

Pași pentru un test de penetrare:

- ✓ Interacțiunea înainte de începere a proiectului
- ✓ Identificarea și stabilirea perioadei de realizare a testului de penetrare (cu aviz din partea Beneficiarului)
- ✓ Colectarea informațiilor
- ✓ Threat Modeling

- ✓ Analiza Vulnerabilitatilor (Autorizație, Logica de Business, Validarea datelor, Security Management, Managementul erorilor, Criptografie, Client Side, Validarea input-urilor)
- ✓ Exploatarea, Post Exploatare și Escaladarea Privilegiilor
- ✓ Raportare & Remediere, Eliminarea dovezilor

4. Raportare & Remediere

Toate rezultatele și concluziile colectate în timpul serviciilor de testare vor fi detaliate într-un raport cuprinzător care va conține:

- ✓ Limitări în ceea ce privește dezvăluirea și utilizarea acestui raport
- ✓ Introducere generală
- ✓ Rezumat executiv
- ✓ Metodologie și domeniu de aplicare
- ✓ Teste efectuate
- ✓ Vulnerabilitățile identificate:
  - Lista, distribuția și riscul fiecărei vulnerabilități
  - Descriere generala
  - Descriere tehnica
  - Severitatea și analiza probabilităților
  - Calculul riscului
  - Contramăsuri și referințe
- ✓ Raport detaliat cu privire la fiecare vulnerabilitate
- ✓ Concluzii
  - Recomandări generale
  - Măsuri generale de prevenire a vulnerabilitatilor similare pentru viitor
  - Remediere

La final, se vor verifica și confirma eliminarea riscurilor raportate, după ce Beneficiarul va implementa măsurile recomandate în raportul testului.

De asemenea, la sfârșitul testului, toate dovezile obținute vor fi arhivate prin metode standard care sunt considerate sigure din perspective tehnice ce fac referire la aceste servicii.

5. Certificări Prestator

Certificările pe care Prestatorul ce va realiza serviciile de audit prezentate mai sus trebuie să îndeplinească minim următoarele:

- ✓ Auditor acreditat pe Lista auditorilor IT gestionat de ADR, pentru procedura prevăzută la OMCSI 553/2019
- ✓ Prestatorul este înregistrat în Registrul național al auditorilor de Securitate cibernetică gestionat de Directoratul National de Securitate
- ✓ Trusted Introducer (TI)
- ✓ SR EN 150 9001:2008
- ✓ SR EN 150 20000-1:2011
- ✓ SR EN 150 IIEC 27001:2013

6. Certificări auditor

Echipa auditorilor trebuie să fie alcătuită din experți care să aibă minim următoarele certificări:

- ✓ GIAC Certified Incident Handler (GCIH)

- ✓ GIAC Certified Detection Analyst (GCDA)
- ✓ Certified Incident Handler (ECIH)
- ✓ GIAC Advisory Board
- ✓ Splunk Core Certified User
- ✓ Certified Penetration Testing Consultant by Mile2
- ✓ Certified Secure Web Application Engineer by Mile2
- ✓ Certified Ethical Hacker (CEH)
- ✓ CompTIA PenTest+
- ✓ Understanding of Cisco Network Devices
- ✓ Understanding Cisco Network Security
- ✓ OSCE - Offensive Security Certified Expert
- ✓ OSCP - Offensive Security Certified Professional
- ✓ OSWP - Offensive Security Wireless Professional
- ✓ CISA - Certified Information Systems Auditor
- ✓ CISSP - Certified Information Systems Security Professional
- ✓ LPIC-1 - Linux Professional Institute Certificate 1
- ✓ LPIC-2 - Linux Professional Institute Certificate 2
- ✓ ICWOD - Introduction into Cyber Warfare and Operations Design
- ✓ eCPPT - Certified Professional Penetration Tester
- ✓ eWPT - Certified Web Penetration Tester
- ✓ WSNIC - Windows Server 2008 Network Infrastructure Configuration
- ✓ GPEN - GIAC Penetration Tester
- ✓ ISO17799 Implementation Course
- ✓ CISM- Certified Information Security Manager
- ✓ ISO27001 Lead Auditor Course
- ✓ CGEIT - Certified in the Governance of Enterprise IT
- ✓ CRISC - Certified in Risk and Information Systems Control
- ✓ Comptia Security+
- ✓ CompTIA Linux+
- ✓ CIPM - Certified Information Privacy Manager
- ✓ CDPSE - Certified Data Privacy Solutions Engineer (COBIT si ITIL Foundation)

ANEXA nr. .....1..... la Caietul de sarcini nr. 10898/14.03.2024

Nr. de înregistrare ***11724 / 20.03.2024***

CERINŢE DE SECURITATE ŞI SĂNĂTATE ÎN MUNCĂ PENTRU ACHIZIŢIA
..... Servicii de audit informatic pentru identificarea si evaluarea vulnerabilităţilor si riscurilor informatice in conformitate cu Legea 362 / 2018 (NIS) .....

Serviciul Telecomunicaţii
– cod CPV 72810000-1

1. **Documente obligatorii în faza de adjudecare şi ulterior, la livrarea produselor sau prestarea serviciilor/lucrărilor**

1.1 Pentru serviciile desfăşurate pe amplasamente aparţinând S.N.G.N. Romgaz S.A.

X Lista cu persoanele care prestează serviciile (actualizată);
☐ **Autorizaţiile operatorului economic** prevăzute de legislaţia specifică (...);
☐ **Autorizaţiile personalului** pentru meseriile/profesiile prevăzute de legislaţia specifică (lucru în mediu exploziv şi/sau ISCIR şi/sau electricieni, ...);
☐ **Autorizaţiile echipamentelor de muncă** emise conform legislaţiei specifice (lucrul în mediu exploziv şi/sau ISCIR, ...) – prezentate la accesul pe amplasamente aparţinând S.N.G.N Romgaz S.A.;
☐ **Verificări metrologice** pentru echipamentele utilizate de prestator - vor fi prezentate l momentul accesului în incinta SNGN Romgaz SA;
☐ **Planul de securitate şi sănătate**, conform HG 300/2006 (elaborat de proiectant);
☐ Expertiza tehnică în eventualitatea încadrării în condiţii speciale de muncă a personalului di cadrul Romgaz, pentru activitatea de foraj;
☐ altele NU ESTE CAZUL

1.3 Cerinţe obligatorii la finalul contractului

3.1 Pentru servicii:

☐ Prezentarea **Planului de securitate si sănătate** (actualizat), ca parte integrantă proiectului lucrării, conform HG 300/2006, - ptr. servicii de proiectare lucrări;
☐ altele NU ESTE CAZUL

Director Resurse Umane

ANEXA nr. 9 la Caietul de sarcini nr. 10.898.14.03.2024

Nr. de înregistrare: 11.778/20.03.2024

Către: **Serviciul Telecomunicații**

CERINȚE DE PROTECȚIA MEDIULUI PENTRU ACHIZIȚIA DE:
„Servicii de audit informatic pentru identificarea și evaluarea vulnerabilităților și riscurilor informatice în conformitate cu Legea 362/2018 (NIS)"

1. **Documente obligatorii în faza de adjudecare:**

- NU ESTE CAZUL

2. **Documente obligatorii a fi prezentate de către ofertantul declarat câștigător, în termen de 10 zile lucrătoare de la data comunicării rezultatului procedurii:**

- NU ESTE CAZUL

3. **Cerinţe de protecţia mediului asociate aspectelor de mediu potenţiale:**

- NU ESTE CAZUL

Data: 20.03.2024

ANEXA 3 la Caietele de sarcini transmise prin adresa nr.: Nr. de înregistrare 11101/15.03.2024

Nr. de înregistrare 12053/21.03.2024

Catre:

S.N.G.N. Romgaz S.A. - Sediu

Serviciul Telecomunicatii

Cerințe privind situațiile de urgență la achiziția de:

„Servicii de audit informatic pentru identificarea si evaluarea vulnerabilităților si riscurilor informatice in conformitate cu legea 362/2018 (NIS''

- **Nu este cazul**