Caiet de Sarcini pentru

Servicii de consultanță privind sistemele informatice - Servicii de consultanță pentru implementare NIS
Cod CPV 72220000-3

LEGEA nr. 362 / 2018 (Legea NIS) stabilește cadrul juridic și instituțional, măsurile și mecanismele necesare în vederea asigurării unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice. Printre articolele esențiale ale legii, operatorilor de servicii esențiale le revin anumite obligații în scopul asigurării securității rețelelor și sistemelor informatice.

Astfel, conform reglementărilor legale, Romgaz trebuie să implementeze măsuri tehnice și organizatorice adecvate și proporționale pentru îndeplinirea cerințelor minime de securitate în domenii precum: Guvernanța de securitate, Protecția rețelelor și sistemelor informatice, apărarea cibernetică și reziliența serviciilor.

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

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 Esențiale (ROSE).

În aceste condiții, pentru a asigura conformitatea cu cerințele Legii NIS, este necesară achiziția de servicii de specialitate de securitate cibernetică pentru atingerea următoarelor obiective:

- implementarea cerințelor minime de asigurare a securității rețelelor și sistemelor informatice aplicabile operatorilor de servicii esențiale așa cum au fost definite în Normele Tehnice aprobate prin Ordinul nr. 1323 / 2020 de către Secretariatul General al Guvernului și
- efectuarea unei evaluări preliminare a conformității (preaudit)
- efectuarea auditului de Securitate de către un auditor de securitate cibernetică atestat de Directoratul Național de Securitate Cibernetică (DNSC)

În cadrul prezentei proceduri de achiziție sunt considerate serviciile necesare pentru asigurarea primelor 2 obiective.

Reglementările care completează LEGEA nr. 362 / 2018 sunt:

- REGULAMENT din 22 martie 2021 pentru atestarea și verificarea auditorilor de securitate cibernetică, emis de Secretariatul General al Guvernului.
- Ordinul nr. 1323/2020 pentru aprobarea Normelor tehnice privind cerințele minime de asigurare a securității rețelelor și sistemelor informatice aplicabile operatorilor de servicii esențiale, emis de Secretariatul General al Guvernului.

1. SERVICIILE SOLICITATE

Serviciile de consultanță vor fi axate pe următoarele direcții majore:

1.1. Analiza de gap pentru cerințele legii 362 și definirea nivelului existent de maturitate al managementului securității informației.

În acestă etapă, va fi furnizat un serviciu de preaudit al nivelului de conformare cu directiva NIS care va fi executat în următoarele direcții:

1.1.1. Preaudit NIS.

În această etapa, echipa formata din auditori atestați NIS va efectua o evaluare a nivelului de securitate existent în conformitate cu cerințele de metodă de audit ale legii NIS.

1.1.2. Aria de aplicabilitate

Aria de aplicabilitate a activităților va cuprinde **Analiza securității organizației [AS5] Analiza arhitecturii [AS1], cât și existența controalelor de securitate pentru partea de managementul configurației și a security baselines.**

Obiectivele principale ale acestei etape sunt:

- evaluarea riscurilor, identificarea și clasificarea sistemelor de informații și / sau a activelor organizației;
- evaluarea generală a eficacității controalelor operaționale ale organizației în toate straturile, procedurale și sistemice;
- conformitatea tuturor sistemelor și proceselor organizației cu:
    - cadrul de reglementare existent (legislația europeană și națională); și
    - politicile și standardele legate de IT.

1.1.3. Metodologia serviciului de preaudit general

Scopul acestui serviciu este de a determina riscurile de securitate și conformitatea cu cerințele minime de securitate impuse de legislația națională și europeană, cât și de standardele de securitate în domeniu.

În vederea creării unei opinii obiective și a unui raport de audit cuprinzător, echipa de audit va realiza următoarele activități:

1.1.3.1. Etapa de planificare:

Informațiile necesare pentru executarea evaluării securității sunt colectate în această fază (de exemplu, activele care urmează să fie evaluate, principalele amenințări împotriva activelor, controalele de securitate care trebuie utilizate pentru a atenua aceste amenințări etc.). Evaluarea securității este alcătuită dintr-un plan de management al proiectului, obiective generale și obiective specifice, sfera de aplicare, cerințe, roluri și responsabilități ale echipei, limitări, ipoteze, provocări, interval de timp necesitat, etc. Toate cele de mai sus trebuie să fie convenite în timpul fazei de planificare.

1.1.3.2. Etapa de execuție:

Faza de execuție este faza principală, în timpul căreia trebuie implementată metodologia și tehnica de evaluare aplicabila. La finalizarea fazei de execuție, evaluatorii vor identifica vulnerabilitățile sistemului, rețelei și proceselor organizaționale.

1.1.3.3. Etapa post-execuție

Următoarele activități au loc în această fază:

- analiza vulnerabilităților identificate;
- se realizează identificarea cauzei principale a apariției vulnerabilităților;
- recomandări pentru măsuri de reducere a riscului; și
- redactarea raportului final.

1.1.3.4. Activități esențiale:

Înțelegerea organizației - strângerea de informații relevante despre Romgaz pentru utilizarea în cadrul etapelor următoare. Aceste informații includ: detalii despre organizarea internă, detalii despre organizarea IT, despre tehnologiile și sistemele folosite, modul de funcționare al sistemelor din cadrul domeniului de audit.

Vor fi organizate interviuri cu persoanele responsabile pentru procesele Romgaz, sau, după caz, se vor utiliza chestionare pentru fiecare secțiune în parte. Tot în această etapă se va realiza o listă cu rolurile și responsabilitățile personalului Romgaz în administrarea și operarea sistemelor.

Analiza documentației relevante - evaluarea conformității reglementărilor interne și documentațiile de referință din Romgaz cu cerințele specificate de standardele în domeniu.

Analiza de risc - definirea expunerii pe care o au sistemul și informațiile gestionate la riscuri privind securitatea informațiilor;

În vederea realizării acestei analize de risc, se realizează următoarele:

- Identificarea elementelor analizate: sisteme, aplicații, procese, oameni;
- Identificarea vulnerabilităților și a amenințărilor;
- Cuantificarea și măsurarea scenariilor de risc;
- Identificarea controalelor aplicabile;
- Stabilirea registrului de riscuri și identificarea riscurilor reziduale sau a scenariilor necontrolate.
- Definirea planului de acțiune - definirea de obiective de control și de verificări care vor fi folosite în verificările la fața locului;
- Evaluarea sistemului - echipa de consultanți va întreprinde evaluările și testele prevăzute în planul de acțiune, cu scopul de a verifica atingerea obiectivelor de control stabilite;

1.1.3.5. Aria de aplicabilitate

Lista domeniilor de securitate și a activităților solicitate:

Domenii de securitate	Categorii de activități de securitate	Măsuri de securitate	Activități
GUVERNANȚĂ	Managementul securității informației	Analizarea și evaluarea riscurilor	x
		Realizarea planurilor de securitate. Politica de securitate	x
		Acreditarea de securitate	x
		Indicatori de securitate	x
		Verificarea conformității cu privire la securitatea informației. Audit de securitate	x
		Testarea și evaluarea securității rețelelor și sistemelor informatice	
		Asigurarea securității personalului	x
		Conștientizarea și instruirea utilizatorilor	x
		Gestionarea activelor	x
	Managementul ecosistemului	Cartografierea ecosistemului	x
		Relațiile ecosistemului	x
PROTECȚIE	Managementul arhitecturii	Managementul configurației rețelelor și sistemelor informatice	x
		Managementul suporților de memorie externă	x

		Segregarea și segmentarea rețelelor și sistemelor informatice	x
		Filtrarea traficului	x
		Asigurarea protecției produselor și serviciilor aferente rețelelor și sistemelor informatice	x
		Protecția împotriva malware	x
	Managementul administrării	Administrarea conturilor	x
		Administrarea rețelelor și sistemelor informatice	x
		Managementul accesului de la distanță	x
	Managementul identității și accesului	Managementul identificării și autentificării utilizatorilor	x
		Managementul drepturilor de acces	x
	Managementul mentenanței	Mentenanța rețelelor și sistemelor informatice	x
		Sisteme control industrial. SCADA - monitorizare, control și achiziții de date	x
	Managementul securității fizice	Asigurarea protecției fizice a rețelelor și sistemelor informatice	x
APĂRARE CIBERNETICĂ	Managementul detecției	Managementul vulnerabilităților și alertelor de securitate	x
		Înregistrarea evenimentelor	x
		Jurnalizarea și asigurarea trasabilității activităților în cadrul rețelelor și sistemelor informatice	x
	Managementul incidentelor de securitate	Răspuns la incidente de securitate	x
		Raport incidente	x
		Comunicarea cu Autoritatea competentă la nivel național pentru securitatea rețelelor și sistemelor informatice (ANSRSI) și CSIRT național	x
REZILIENȚĂ	Managementul continuității afacerii	Asigurarea disponibilității serviciului esențial și a funcționării rețelelor și sistemelor informatice	x
		Managementul recuperării datelor în caz de dezastre	x
	Managementul crizelor	Organizarea gestionării crizelor	x
		Procesul de gestionare a crizelor	x

1.1.4. Descrierea detaliata a activităților de evaluare

1.1.4.1. Activități specifice referitoare la arhitectura sistemelor

- Adoptarea unei viziuni globale a rețelelor și sistemelor informatice pentru a identifica:
  - vulnerabilitățile și orice cale de atac asociată;
  - elementele/componentele relevante care urmează a fi auditate.
- Identificarea și colectarea elementelor de arhitectură și echipamentelor de rețea care urmează să fie auditate.
- Auditarea configurației echipamentelor de rețea alese anterior.
- Realizarea de interviuri cu administratorii de rețea.
- Identificarea vulnerabilităților prezente în arhitectură și în configurația echipamentului auditat.
- Formularea de recomandări adecvate pentru remedierea riscurilor care decurg din vulnerabilitățile descoperite.

- Elaborarea și prezentarea unui raport de evaluare.

Consultanții vor evalua următoarele elemente:

- diagramele arhitecturale;
- matricea fluxurilor;
- regulile de filtrare;
- configurarea echipamentelor;
- interconectări cu rețele terțe sau Internet;
- documentele de arhitectură tehnică.

1.1.4.2. Activități specifice în ceea ce privește securitatea informației

- Adoptarea unei viziuni globale a organizației pentru a identifica:
  - politicile și procesele relevante care urmează să fie auditate,
  - locurile relevante care urmează să fie auditate,
  - vulnerabilitățile și orice cale de atac fizică asociată.
- Colectarea documentelor asociate proceselor care urmează să fie auditate.
- Auditarea proceselor și locațiilor alese anterior.
- Desfășurarea de interviuri cu managerii de proces și responsabilii de securitate, inclusiv responsabilii NIS.
- Identificarea vulnerabilităților prezente în procesele și arhitectura fizică a locurilor auditate.
- Formularea de recomandări adecvate pentru remedierea riscurilor care decurg din vulnerabilitățile descoperite.
- Valorificarea cunoștințelor dobândite, oferirea de feedback și răspunsuri către echipa Romgaz, precum și elaborarea și prezentarea unui raport de evaluare.

Consultanții vor:

- analiza organizarea securității rețelelor și sistemelor informatice pe baza standardelor tehnice și de reglementare stabilite de lege, în conformitate cu cerințele minime de securitate aplicabile ROMGAZ;
- respecta regulile specifice de audit, respectiv trebuie să:
  - determine conformitate rețelelor și sistemelor informatice auditate cu privire la parametrii de referință și identificarea abaterilor care prezintă vulnerabilități majore ale acestora;
  - integreze analiza elementelor legate de securitatea aspectelor fizice ale rețelelor și sistemelor informatice, în special, protecția spațiilor care găzduiesc componente ale rețelelor și sistemelor informatice și a datelor/informațiilor auditate sau controlul accesului la aceste componente;

1.1.4.3. Cerințe Suplimentare

Adițional serviciilor solicitate mai sus, se vor lua în considerare și serviciile de mai jos așa cum sunt descrise în Ordinul Nr. 1323 din 9 noiembrie 2020 pentru aprobarea **Normelor tehnice privind cerințele minime de asigurare a securității rețelelor și sistemelor informatice** aplicabile operatorilor de servicii esențiale.

Astfel sunt solicitate următoarele:

- Evaluarea gradului de conformitate în ceea ce privește modul de implementare al guvernanței securității informatice la nivelul ROMGAZ;
- Evaluare gradului de conformitate în ceea ce privește modul de implementare al protecției cibernetice implementate la nivelul ROMGAZ;
- Evaluare gradului de conformitate în ceea ce privește modul de implementare al apărării cibernetice implementate la nivelul ROMGAZ;
- Evaluare gradului de conformitate în ceea ce privește modul de implementare al rezilienței cibernetice implementate la nivelul ROMGAZ;

Detalierea serviciilor solicitate se regăsește mai jos:

Guvernanță	
Managementul securității	• Analizarea și evaluarea riscurilor [A11];

informației	• Realizarea planurilor de securitate. Politica de securitate [A12]; • Acreditarea de securitate [A13]; • Indicatori de securitate [A14]; • Verificarea conformității cu privire la securitatea informației; Audit de securitate [A15]; • Testarea și evaluarea securității rețelelor și sistemelor informatice [A16]; • Asigurarea securității personalului [A17]; • Conștientizarea și instruirea utilizatorilor [A18]; • Gestionarea activelor [A19];
Managementul ecosistemului	• Cartografierea ecosistemului [A21]; • Relațiile ecosistemului [A22];
Protecție	
Managementul arhitecturii	• Managementul configurației rețelelor și sistemelor informatice [B11]; • Managementul suporturilor de memorie externă [B12]; • Segregarea și segmentarea rețelelor și sistemelor informatice [B13]; • Filtrarea traficului [B14]; • Asigurarea protecției produselor și serviciilor aferente rețelelor și sistemelor informatice [B15]; • Protecția împotriva malware [B16];
Managementul administrării	• Administrarea conturilor [B21]; • Administrarea rețelelor și sistemelor informatice [B22]; • Managementul accesului de la distanță [B23];
Managementul identității și accesului	• Managementul identificării și autentificării utilizatorilor [B31]; • Managementul drepturilor de acces [B32];
Managementul mentenanței	• Mentenanța rețelelor și sistemelor informatice [B41]; • Sisteme de control industrial. SCADA - Monitorizare, control și achiziții de date [B42];
Managementul securității fizice	• Asigurarea protecției fizice a rețelelor și sistemelor informatice [B51];
Apărare cibernetică	
Managementul detecției	• Managementul vulnerabilităților și alertelor de securitate [C11]; • Înregistrarea evenimentelor [C12]; • Jurnalizarea și asigurarea trasabilității activităților în cadrul rețelelor și sistemelor informatice [C13];
Managementul incidentelor de securitate	• Răspuns la incidente de securitate [C21]; • Raport incidente [C22]; • Comunicarea cu ANSRSI și CSIRT Național [C23];
Reziliență	
Managementul continuității afacerii	• Asigurarea disponibilității serviciului esențial și a funcționarii rețelelor și sistemelor informatice [D11]; • Managementul recuperării datelor în caz de dezastre [D12];
Managementul crizelor	• Organizarea gestionarii crizelor [D21]; • Procesul de gestionare a crizelor [D22].

1.1.5. Livrabile

- **Raport de evaluare a conformității NIS,** în care sunt documentate neconformitățile, observațiile și recomandările pentru îmbunătățire.

1.2. Definirea Elementelor de Guvernanță a Securității Informației

În cadrul acestei etape, obiectivul principal este să se verifice implementarea unor structuri de guvernanță eficiente, să se clarifice rolurile și responsabilitățile și să se îmbunătățească procesele de raportare și evaluare.

Vor fi considerate următoarele activități:

- Verificarea rolului Responsabil NIS.
- Definirea canalelor de raportare și feedback: Aceasta implică revizuirea și actualizarea canalelor de raportare și feedback pentru a asigura că informațiile privind securitatea cibernetică sunt comunicate eficient și în mod oportun între diferitele părți interesate din organizație.
- Stabilirea procesului de acreditare: În conformitate cu Politica de securitate, trebuie stabilit un proces prin care Organizația acreditează sistemele NIS utilizate în furnizarea serviciilor esențiale.
- Definirea indicatorilor de evaluare: Acești indicatori vor fi baza pe care ROMGAZ își va evalua conformitatea cu Politica de securitate a rețelelor și sistemelor informatice. Indicatorii ar trebui să fie relevanți, măsurabili și să reflecte aspectele importante ale securității informației. De asemenea va fi stabilita atât modalitatea de raportare a nivelului de performanta a securității, dar și se vor trasa care sunt acei indicatori care sunt cei mai relevanți pentru conducerea ROMGAZ.
- Metode de evaluare a indicatorilor de conformitate.
- Procedură privind evaluarea conformității NIS și efectuarea auditului de securitate.

Rezultatele și livrabilele acestei etape sunt:

- RAIPOD - model de Raport privind implementarea politicii de securitate a rețelelor și sistemelor informatice care asigură furnizarea serviciilor esențiale și a documentelor de aplicare a acesteia
- PEANIS - model de procedura pentru Procesul de acreditare stabilit în PONIS prin care ROMGAZ acreditează NIS utilizate în furnizarea serviciilor esențiale, inclusiv componentele de administrare
- MANIS - model ajustat pentru Mapa de acreditare de securitate; document în baza căruia se emite Decizia de acreditare
- DANIS - Decizia de acreditare; decizie formală luată de managementul de nivel înalt al ROMGAZ
- SMSI Sistemul de management a securității informației
- IEC Indicatori de evaluare, pe baza cărora ROMGAZ își evaluează conformitatea cu Politica de securitate a rețelelor și sistemelor informatice
- RAEC Raport de evaluare a conformității
- MEIEC Metoda de evaluare a indicatorilor de conformitate
- PRECAS - procedură privind evaluarea conformității NIS și efectuarea auditului de securitate a rețelelor și sistemelor informatice.
- Documentele specifice pentru obtinerea angajamentului angajatilor pentru respectarea cerintelor de securitate informationala. Acestea se pot materializa în ajustări ale Fișelor de post / ROF / Regulament de ordine interioara.
- Program complet de educatie a angajatilor in materie de securitate cibernetica care include
    - Sustinerea a două sesiuni de training în materie de securitate informatica
    - Recomandări pentru implementarea mecanismelor de educare și constientizarea angajatilor (emailuri, constructia unui portal sau sectiuni dedicate pentru comunicarea catre angajati, constructia sau utilizarea de unelte digitale pentru verificarea cunostintelor)

1.3. Analiza de Impact asupra Afacerii.

Faza de Analiză de Impact asupra Afacerii va asigura fundamentul remedierii problemei și coordonarea optimizată a eforturilor de asigurare a continuității serviciilor esențiale.

Activitățile de bază includ următoarele:

- Identificarea funcțiilor critice de afaceri: Implică înțelegerea diverselor funcții și procese care sunt vitale pentru operațiunile de afaceri.
- Evaluarea impactului: Se va evalua impactul potențial al unei întreruperi. Acest lucru implică evaluarea costurilor directe și indirecte asociate cu întreruperea acestor funcții.
- Identificarea dependențelor dintre procesele de business.

- Stabilirea priorităților de recuperare.
- Instrumentarea integrării Analizei de Impact asupra Afacerii în planurile de continuitate și de recuperare în caz de dezastru.

Rezultatele și livrabilele acestei etape sunt:

- Raportul Analizei de Impact asupra Afacerii: Un document detaliat care prezintă rezultatele analizei de impact asupra afacerii. Acesta va include o descriere a funcțiilor critice de afaceri, evaluarea impactului unei întreruperi asupra acestora, și identificarea dependențelor dintre diferitele procese de afaceri.
- Lista de procese critice de afaceri.
- Matricea de impact: Un tabel sau o matrice care arată efectele diferitelor scenarii de întrerupere asupra funcțiilor critice de afaceri, inclusiv impactul financiar și operațional.
- Raport cu Timpul de Recuperare (RTO) și Punctul de Recuperare (RPO): Acestea sunt măsurători care descriu timpul maxim admisibil în care un proces sau sistem poate fi nefuncțional (RTO), respectiv vechimea maximă a datelor care pot fi pierdute în caz de întrerupere majoră (RPO).
- Enumerarea proceselor operaționale și alocarea de nivele de criticitate, a cerințelor țintă pentru RTO și RPO
- Enumerarea departamentelor care susțin direct serviciile esențiale in contextul Legii NIS, dar și a departamentelor suport, fără de care furnizarea serviciului esențial depind direct.
- Enumerarea sistemelor și aplicațiilor care susțin procesele de afacere
- Alocarea cerințelor de RTO și RPO asupra elementelor de infrastructură și aplicații, precum și definirea nivelelor de criticitate.
- Identificarea sistemelor care susțin accesul și disponibilitatea sistemelor critice, sau a căror securitate și disponibilitate impacteaza sistemic procesele de afaceri critice dar și sistemele și aplicațiile critice
- Planul de prioritizare a recuperării: Acest plan identifică ordinea în care procesele critice de afaceri ar trebui să fie recuperate în caz de întrerupere.
- Diagrama de dependențe: Aceasta prezintă relațiile dintre diferitele procese de afaceri și modul în care sunt interconectate.
- Raport cu Recomandări pentru planificarea continuității afacerii și a recuperării în caz de dezastru: Acestea se bazează pe rezultatele BIA și oferă orientări despre cum să se pregătească pentru și să gestioneze potențiale întreruperi.

1.4. Analiza de risc.

Analiza de risc este destinată să faciliteze identificarea și evaluarea potențialelor amenințări și vulnerabilități ale sistemelor informaționale. Aceasta include următoarele etape:

- Asistență în construcția listelor de inventar IT și ICS Scada cât și implementarea acestora în CMDB.
- Analiza arhitecturii sistemului informațional, se va analiza atât modelul fizic, cât și cel logic al arhitecturii sistemelor informaționale care susține serviciilor esențiale. De asemenea, vor fi inventariate configurațiile detaliilor sistemelor informatice, inclusiv componentele și interacțiunile între elemente.
- Analiza fluxurilor de circulație a informațiilor în sistemul informațional, identificarea posibilelor puncte slabe sau vulnerabilități care ar putea fi exploatate de actori rău intenționați.
- Analiza configurării tehnice și a arhitecturii de securitate ale sistemelor informatice relevante.
- Analiza vulnerabilităților.
- Modelarea amenințărilor, elaborarea scenariilor de risc, calculul probabilității și impactului.
- Asistență în construcția registrului de riscuri pentru departamentele implicate în furnizarea serviciilor esențiale.
- Asistență în implementarea procedurii de management al riscurilor existente în societate cât și în implementarea cerințelor de proces

1.5. Analiza Contractelor Furnizorilor Terți (vendor risk assesment)

Se vor evalua relațiile cu furnizorii terți în vederea evidențierii riscurilor asociate cu acestea. Această etapă implică analiza detaliată a contractelor cu acești furnizori, precum și a responsabilităților lor tehnice în

furnizarea serviciilor externalizate sau de suport. Principalele elemente care vor fi considerate sunt următoarele:

- Analiza contractelor cu furnizorii terți: Vor fi examinate fiecare contract în parte pentru a înțelege clar serviciile oferite, nivelurile de serviciu convenite, obligațiile de securitate cibernetică ale furnizorilor și posibilele sancțiuni pentru nerespectarea obligațiilor contractuale.
- Evaluarea responsabilităților tehnice ale furnizorilor: Aceasta include o revizuire a obligațiilor tehnice ale furnizorilor, verificarea competențelor lor tehnice, evaluarea mecanismelor de securitate pe care le au în vigoare și înțelegerea modului în care acestea contribuie la securitatea generală a organizației.
- Raportul de riscuri asociate cu furnizorii externi: La finalizarea acestei etape, va fi livrat un raport detaliat care identifică și evaluează riscurile asociate cu fiecare furnizor terț. Acesta va include o listă a riscurilor potențiale identificate și o evaluare a impactului și a probabilității acestora în furnizarea serviciilor esențiale.
- Analiza relațiilor cu părțile interesate ale ecosistemului: Vor fi analizate și riscurile reprezentate de relațiile cu alte părți interesate ale ecosistemului, inclusiv parteneri, clienți, reglementatori și alte entități cu care organizația interacționează.
- Lista cu acorduri la nivel de serviciu și/sau mecanisme de audit a rețelelor și sistemelor informatice: Va fi elaborată o listă cu toate acordurile la nivel de serviciu (SLAs) cu furnizorii terți și vor fi examinate mecanismele de audit existente pentru rețelele și sistemele informatice.

Rezultatele și livrabilele acestei etape sunt:

- LASPO Lista activelor, sistemelor și proceselor organizației
- Listele de inventar IT si ICS Scada implementate in CMDB pe nivele de criticitate
- Scheme de arhitectura IT și Scada refăcute
- Raport de audit asupra configurațiilor tehnice și a arhitecturii de securitate ale sistemelor informatice relevante
- Registrul de riscuri
- Planul pentru implementarea măsurilor de control a riscurilor
- Raport privind monitorizarea performanțelor
- Raport privind desfășurarea procesului de gestionare a riscurilor
- Informare privind monitorizarea performanțelor și gestionarea riscurilor
- LASMA - Listă cu acorduri la nivel de serviciu și/sau mecanisme de audit a rețelelor și sistemelor informatice
- PROSRE - Procedură de stabilire a relațiilor ecosistemului; documentul include interconexiunile (relațiile externe) între rețelele și sistemele informatice și terți
- LIRIE - Lista riscurilor potențiale identificate și evaluarea acestora în furnizarea serviciilor esențiale. Riscurile sunt reprezentate de relațiile cu părțile interesate ale ecosistemului
- Analize de risc distincte pentru fiecare furnizor de servicii externe
- SICAE - Situația cartografică a ecosistemului; document prin care se realizează stabilirea și identificarea ecosistemului care stă la baza furnizării serviciului esențial atât NIS, cât și alte componente

1.6. Clasificarea Informației

În această etapă se vor urmări elementele specifice necesare asigurării că toate informațiile sensibile sunt identificate și protejate în mod adecvat. Aceasta implică următoarele etape:

- Inventarierea informațiilor indiferent de formatul lor (digital sau analog), pentru toate domeniile și departamentele organizației.
- Alocarea nivelului de secretizare: După ce a fost efectuat inventarul, fiecărei informații i se va aloca un nivel de secretizare conform procedurii de clasificare a informației. Acest nivel va determina măsurile de protecție care trebuie aplicate informației respective.
- Implementarea măsurilor tehnice și organizatorice pentru etichetare: Următorul pas este implementarea măsurilor necesare pentru a aplica etichetele de clasificare la fiecare informație. Aceasta poate include utilizarea unor sisteme de gestionare a informațiilor care permit etichetarea automată a informațiilor în funcție de criteriile stabilite.

- Protecția suportului informațional: Se vor furniza ghidaje pentru a implementa măsuri de securitate adecvate pentru a proteja suporturile informaționale împotriva divulgării neautorizate. Acestea pot include criptarea datelor, controlul accesului și alte măsuri de securitate fizică și cibernetică.
- Colectarea informațiilor: În acest stadiu, vor fi realizate interviuri cu fiecare șef de direcție și de departament pentru a colecta informații despre tipurile de informații pe care le dețin și modul în care sunt utilizate.
- Furnizarea situației centralizate a tipurilor de informații pe nivelele de secretizare: La finalizarea procesului de colectare a informațiilor, va fi furnizată o situație centralizată a tuturor tipurilor de informații din organizație, împreună cu nivelurile lor de secretizare.
- Emiterea de recomandări pentru implementarea de măsuri tehnice și organizatorice: În funcție de rezultatele analizei, vor rezulta recomandări pentru implementarea de măsuri tehnice și organizatorice pentru protecția informațiilor. Aceasta poate include recomandări pentru implementarea unui sistem de prevenire a pierderii datelor (DLP), îmbunătățirea politicii de acces sau implementarea altor tehnologii de securitate.
- Analiza a nivelului de conformare cu GDPR pe următoarele componente:
    - Analiza Registrului Procesărilor de date cu caracter personal;
    - Analiza identificării în mod corect "proprietarilor" de sisteme și de informații;
    - Analiza identificării și descrierii în mod relevant a proceselor de business prin care se prelucrează date cu caracter personal
    - Analiza identificării calității în care organizația prelucrează date cu caracter personal (operator asociat, împuternicit)
    - Analiza identificării datelor cu caracter personal prelucrate în fiecare proces de business, temeiul legal al prelucrării, cât și categoriile de date prelucrate în fiecare proces
    - Analiza evaluării interesului legitim, unde e cazul.

Rezultatele și livrabilele acestei etape sunt:

- PRECDI - Procedură privind etichetarea și clasificarea datelor și informațiilor
- Anexa PRECDI cu clasificarea informației pe categorii de suport informațional și categorii de informații structurate pe nivelele de secretizare.
- Raport de evaluare tehnica pentru implementarea unei soluții software pentru Identificarea și protecția informațiilor personale identificabile (PII) cât și ale informațiilor în general și pentru implementarea de măsuri tehnice și organizatorice pentru protecția informațiilor.
- Analiza implementării GDPR

1.7. Managementul identității și al accesului.

Serviciile vor include:

- **Consultanță pentru Inventarierea tuturor identităților în toate sistemele informatice:** Va fi efectuată o revizuire completă a tuturor identităților digitale din organizație.
- **Consultanță pentru Regulile de acces la sisteme:** Vor fi definite și implementate politici de acces care reglementează cine poate accesa ce resurse în cadrul organizației. Aceste politici vor fi concepute pentru a se asigura că utilizatorii au acces doar la resursele de care au nevoie pentru a-și efectua sarcinile lor.
- **Consultanță pentru Accesul de la distanță:** În contextul muncii la distanță la sistemele critice, vor fi analizate modalități pentru ca inginerii de sistem să se conecteze sigur la serverele de proces.
- **Consultanță pentru Conturile privilegiate și verificarea acestora.**
- Consultanță pentru selecția tehnologiilor care să ajute la digitalizarea operațiunilor care rezultă din procedurile operaționale.

Rezultatele și livrabilele acestei etape sunt:

- Rapoarte de analiză pentru selecția măsurilor tehnice pentru Managementul identității și al accesului.
- Un registru centralizat al tuturor identităților și al acceselor la resurse.
- PPSIA Plicul cu parole utilizate pentru sisteme informatice de administrare a rețelelor și sistemelor informatice
- PROLD Procedură privind lucrul la distanță
- ECUPA Evidența conturilor pentru utilizatori și pentru procesele automatizate

- LICPA Lista conturilor privilegiate pe nivele de acces și funcționalități accesabile
- LICA Lista conturilor de administrare
- MEAUP Mecanism de autentificare pentru utilizatori și procese automatizate la resursele rețelelor și sistemelor informatice
- SIVMOC Sistem de verificare a potențialelor modificări ale unui cont privilegiat
- PRASI Procedură privind accesul și securitatea resurselor și informațiilor

1.8. Managementul Sistemelor

Va fi analizată arhitectura de rețea pentru segregare optimă, setările firewall-urilor, implementarea unui management eficient al cheilor de criptare și propunerea standardelor de securitate. Va fi creat un baseline de securitate, aliniat la standardele internaționale. Serviciile vor include:

- Definirea arhitecturii de rețea: Definirea și implementarea unei arhitecturi de rețea care asigură o segmentare eficientă și segregarea rețelelor și sistemelor informatice pentru a limita riscul de expunere la amenințări și a minimiza impactul potențial al unui incident de securitate. Acest proces include identificarea resurselor critice, proiectarea rețelei pentru a separa aceste resurse de restul rețelei și implementarea controalelor necesare pentru a asigura această segregare.
- Evaluarea modalităților de implementare a segregării rețelei: va fi analizată conformitatea modalităților actuale de segregare a rețelei. Se vor la în considerare metodele actuale de segregare a rețelei, eficacitatea acestora și posibilele îmbunătățiri.
- Analiza setărilor de firewall: Aceasta implică o revizuire a setărilor actuale de firewall pentru a asigura că acestea sunt configurate corect și că oferă nivelul necesar de protecție pentru rețelele și sistemele informatice.
- Implementarea efectivă a managementului cheilor de criptare: Acest proces implică implementarea procedurilor pentru generarea, utilizarea și urmărirea cheilor de criptare, inclusiv gestionarea ciclului de viață al cheilor și protejarea acestora împotriva divulgării neautorizate.
- Definirea standardelor de securitate (baselining) pentru toate elemente IT care susțin procesele critice, managementul excepțiilor de la acestea cât și definirea și implementarea unui flux operațional. În această direcție se va evalua un model de maturitate versus standardele internationale aplicabile și se va crea un roadmap de aliniere la acest standard din punctul de vedere operațional dar mai ales tehnic. Se vor crea referințe arhitecturale de baza, se va asigura consultanta pentru selecția de tehnologii aplicabile, dar și consultanță pentru ajustarea arhitecturii și consultanță pentru implementarea efectiva a soluțiilor tehnice.
- Consultanta pentru selecția tehnologiilor care sa ajute la digitalizarea operațiunilor care rezulta din procedurile operaționale.

Rezultatele și livrabilele acestei etape sunt:

- Raport de recomandări de optimizare al regulilor de firewall
- Fluxuri de lucru pentru managementul cheilor de criptare, aplicarea de baselines de securitate, pentru managementul exceptiilor
- Baselines de securitate create pentru fiecare dintre tipurile de dispozitive critice de rețea
- Raport de evaluare al arhitecturii Scada si arhitectura actualizata al acesteia
- PROMNIS - Procedură pentru menținerea securității rețelelor și sistemelor informatice
- PRAPMA- Procedură pentru asigurarea protecției malware
- PRUSIA- Procedură privind utilizarea sistemelor informatice de administrare
- JIERU- Jurnalele de înregistrare a evenimentelor produse de resursele utilizate pentru administrare. Jurnalele sunt constituite și ținute sub formă electronică sau pe hârtie.
- PRUSME- Procedură privind utilizarea suporților de memorie externă
- RESME Registre de evidență a suporților de memorie externă
- PROSES - Procedură privind segregarea și segmentarea rețelelor și sistemelor informatice utilizate pentru furnizarea serviciilor esențiale

1.9. Managementul vulnerabilitatilor

Această etapă este orientată spre implementarea unui management al excepțiilor de securitate, cât și mecanisme de verificare a activităților de aplicare de patching. Serviciile vor include:

- Consultanță pentru definirea fluxurilor de lucru operaționale pentru scanarea și detectarea vulnerabilităților: Această activitate implică evaluarea infrastructurii IT și SCADA existente ale organizației și utilizarea unor instrumente de scanare avansate pentru a identifica vulnerabilitățile potențiale. Consultanții vor formula recomandări pentru configurarea și rularea scanărilor, analiza rezultatelor și identificarea punctelor slabe în sistemele de securitate.
- Consultanță pentru prioritizarea vulnerabilităților.
- Consultanță pentru tratarea excepțiilor.

Rezultatele și livrabilele acestei etape sunt:

- Fluxuri operaționale pentru managementul vulnerabilităților.
- PRORUVI Procedură pentru reducea riscurilor legate de utilizarea unei versiuni învechite
- PEIREV proces de identificare, clasificare, remediere și eliminare a vulnerabilităților, în special în software și firmware, la nivelul rețelelor și sistemelor informatice
- Consultanță pentru selecția tehnologiilor care să ajute la detecția de vulnerabilități, digitalizarea operațiunilor care rezulta din procedurile operaționale.

1.10. Managementul detecției.

Vor fi incluse activități de consultanță care să optimizeze modalitatea prin care se realizează managementul detecției și răspunsul la incidentele de securitate. Activitățile cele mai importante sunt:

- Evaluarea capabilităților prezente în ROMGAZ.
- Definirea proceselor operaționale de tip SOC.

Rezultatele și livrabilele acestei etape sunt:

- Raport de maturitate a operațiunilor de tip SOC (Security Operations Center)
- Alocarea de echipe de SOC. SLA și alte metrice operaționale
- Procesele operaționale de SOC documentate
- Testarea operațională a echipei de SOC. Table Top exercise.
- Executive Brief (Interacțiunea participanților cu planul de răspuns la incident (IRP), Planul de comunicare și procedurile de escaladare, Lecții învățate, Recomandări strategice)
- PRORAI - procedură pentru gestionarea, răspunsul și analiza incidentelor care afectează funcționarea sau securitatea rețelelor și sistemelor informatice
- PRORIS - procedură pentru raportarea incidentelor de securitate
- PISAC procedură de interconectare la serviciul de alertare și cooperare al CERT-RO.
- LIRNIS lista responsabililor NIS
- PRIMSA procedură pentru gestionarea informațiilor primite și, după caz, a măsurilor de securitate adoptate pentru protejarea NIS
- Consultanta pentru selecția tehnologiilor care să susțină următorii indicatori de control
- SIEM managementul monitorizării, cercetării și identificării rapide a principalelor cauze de afectare a securității, precum și ale încălcării politicilor de securitate
- SMMEIS sistem de monitorizare și management al evenimentelor și incidentelor de securitate
- SIDGI sistem informatic dedicat pentru gestionarea incidentelor

1.11. Managementul continuității

Vor fi urmărite următoarele domenii:

- Revizuirea Planului de Recuperare în Caz de Dezastru (DRP). Activitățile de consultanță pentru definirea unui DRP vor include următoarele etape:
    - In baza primei etape (Evaluarea Riscului și Analiza Impactului Asupra Afacerii (BIA) - în care vor fi identificate și evaluate potențialele amenințări sau riscuri pentru operațiunile organizației, impactul potențial pe care aceste evenimente îl pot avea asupra operațiunilor de afaceri, identificarea și prioritizarea Funcțiilor Esențiale ale Afacerii.
    - Stabilirea Strategiilor de Recuperare: Aceasta implică identificarea și dezvoltarea strategiilor și soluțiilor tehnice pentru restaurarea funcțiilor și operațiunilor critice ale afacerii în urma unui dezastru.

- Definirea unii Plan de implementare: Acesta este un set detaliat de instrucțiuni și proceduri care descrie exact ce trebuie făcut, când și de către cine, în cazul unui incident. Ar trebui să fie suficient de detaliat încât oricine cu cunoștințe de bază să fie capabil să implementeze planul.
- Evaluarea definirii Roluri și responsabilități: Această secțiune detaliază cine are responsabilitatea pentru ce anume în timpul și după un incident. Aceasta ar trebui să includă contactele de urgență, precum și o listă a responsabilităților fiecărei persoane.
- Planuri de testare și actualizare: Aceasta arată când și cum va fi testat planul pentru a asigura eficacitatea sa, și când și cum va fi revizuit și actualizat.
- Instruire și sensibilizare: Detaliază programele de instruire și sensibilizare menite să asigure că personalul este conștient de plan și este capabil să își execute responsabilitățile în cazul unui incident.
- Definirea de Anexe operaționale: Acestea vor include orice alte informații relevante, cum ar fi planuri de evacuare, liste de echipamente, copii ale contractelor importante, scheme de rețea, liste de verificare etc.

Rezultatele și livrabilele acestei etape sunt:

- Planul de continuitate a afacerii.

2. Considerente de natură tehnica și organizatorică cu privire la desfășurarea activităților

- În ofertă va fi prezentat un plan de proiect cu alocarea personalului prestatorului pe activitățile considerate.
- Serviciile vor fi prestate la punctele ROMGAZ de lucru și de la distanță.
- Interacțiunea cu personalul Romgaz va avea loc în timpul programului de lucrul orelor normale de lucru, de la 8 a.m. pana la 4 p.m. de Luni pana Vineri.
- Va fi asigurată participarea tuturor factorilor cheie de decizie relevanți pentru procesele evaluate.
- Personalul intern va acorda timp suficient pentru derularea proiectului în conformitate cu termenele;
- Va fi acordat accesul necesar membrilor echipei de proiect pentru a analiza, documenta și cartografia informațiile necesare în fiecare etapa a proiectului,
- Documentele vor fi livrate în format electronic.

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

4. Echipa de proiect

Echipa de consultanți va deține, în mod cumulativ, următoarele competențe:

- Auditare sisteme IT, demonstrată prin deținerea cel puțin unei certificări de tip:
  - CISA - Certified Information Systems Auditor ,
  - ECSA - EC-Council/ Certified Security Analyst,
  - OPSE - OSSTMM Professional Security Expert,
  - CISSP - Certified Information Systems Security Professional,
- Guvernanță sisteme IT și securitate, demonstrată prin deținerea cel puțin unei certificări de tip: CGEIT - Certified in the Governance of Enterprise IT , CISM - Certified Information Security Manager , CRISC - Certified in Risk and Information Systems Control, COBIT5 - COBIT 5 Certification sau similar,

- Organizare și coordonare de SOC, demonstrată prin deținerea cel puțin unei certificări de tip: GRID - GIAC Response and Industrial Defense, GSOM - GIAC Security Operations Manager, sau similar,
- Securizare medii ICS Scada, demonstrată prin deținerea cel puțin unei certificări de tip: Global Industrial Cyber Security Professional Certification (GICSP) de la GIAC, sau Certified SCADA Security Architect (CSSA) de la IACRB, sau oricare certificare similare.

În ofertă vor fi prezentați membrii echipei de consultanță și CV-urile acestora.

5. Cerințe minime privind Prestatorul

Prestatorul ce va realiza serviciile de consultanță prezentate mai sus trebuie să îndeplinească minim următoarele condiții:

- Prestatorul este înregistrat în Registrul național al auditorilor de Securitate cibernetică gestionat de Directoratul National de Securitate Cibernetică,
- Deține certificări ISO 9001 și ISO 27001.

6. Experiența similară

Prestatorul va demonstra realizarea a cel puțin unui proiect similar care să aibă ca obiect servicii de consultanta de securitate cibernetică similare celor solicitate, care să fie din același domeniu de activitate sau similar Romgaz sau de complexitate similara Romgaz,

De asemenea, prestatorul va demonstra realizarea a cel puțin unui Audit a rețelelor și sistemelor informatice ce susțin servicii esențiale ori furnizează servicii digitale în condițiile Legii nr. 362/2018.

Pentru demonstrarea experienței similare, se vor prezenta recomandări din partea beneficiarilor.

7. Termen de prestare a serviciilor

Serviciile vor fi demarate în cel mult o lună de la semnarea contractului, iar prestarea se va întinde pe o perioadă de cel mult 6 luni. Contractul aferent acestor servicii va avea durata de 7 luni.

Întocmit

Dan MORARIU

Șef serv. Telecomunicații

S.N.G.N. ROMGAZ S.A.
VIZAT PENTRU
02. AUG. 2024
REALITATEA, REGULARITATEA ȘI LEGALITATEA OPERAȚIUNILOR
Nr.59

ROMGAZ	CERINȚE DE SECURITATE ȘI SĂNĂTATE ÎN MUNCĂ PENTRU ACHIZIȚIA DE *Servicii de consultanță privind sistemele informatice - Servicii de consultanță pentru implementare NIS*	Cod: 02F-07-Act.3.2
		Pag. 1 / 1

ANEXA nr. 1 la Caietul de sarcini nr. .....

Nr. 32.731 / 02.08.2024

Confidențial

Serviciul Telecomunicații
CPV: 72220000-3

1. **Documente obligatorii în faza de adjudecare și ulterior, la livrarea produselor sau prestarea serviciilor/lucrărilor**
   Toate documentele vor fi prezentate în limba română. Documentele emise în altă limbă vor fi însoțite de traduceri autorizate.

1.1 Pentru serviciile desfășurate pe amplasamente aparținând S.N.G.N. Romgaz S.A.

X Lista cu persoanele care prestează serviciile (actualizată);

2. **Cerințe obligatorii la finalul contractului**

2.1 Pentru servicii:

Nu este cazul.

Notă:
Prezentele reglementări nu sunt limitative. Pe toată perioada derulării contractului, contractorul va respecta legislația din domeniul securității și sănătății în muncă, în vigoare, aplicabilă activităților pe care le desfășoară.

ROMGAZ	CERINȚE DE PROTECȚIA MEDIULUI PENTRU ACHIZIȚIA DE: „SERVICII DE CONSULTANȚĂ PRIVIND SISTEMELE INFORMATICE-SERVICII DE CONSULTANȚĂ PENTRU IMPLEMENTARE NIS”	Cod: 02F-08-Act.3.1
		Pag. 1/1

ANEXA nr. 2 la Caietul de sarcini nr. ..... înregistrare solicitare nr. FN

Nr.32.669/02.08.2024
Confidențial

Către:
SERVICIUL TELECOMUNICAȚII

1. Documente obligatorii în faza de adjudecare

1.1 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

2.1 Documente care să ofere informații cu privire la amprenta de carbon a produselor care fac obiectul achiziției.

3. CERINȚE DE PROTECȚIA MEDIULUI ASOCIATE ASPECTELOR DE MEDIU POTENȚIALE

3.1 Nu este cazul.

Data: 02.08.2024