APROBAT:

Președinte Consiliului de Administrație SA "Moldovagaz"

_____Vadim CEBAN

CAIET DE SARCINI

Licitației "Analiza riscurilor a proceselor în sistemele și infrastructura informațională IT"

Elaborat:

Șef Direcție Tehnologii Informaționale **Vitalie Burcovschi**

1. **Descrierea serviciilor și a livrabilelor care urmează a fi realizate**

Obiectivul general este acela de a identifica si evalua riscurile la adresa securității informației in cadrul infrastructurii IT a SA Moldovagaz, dar nelimitând-se numai la aceasta. În vederea realizării acestei analize de risc, este necesar de a realiza următoarele:

- **Identificarea elementelor analizate: sisteme, aplicaţii, procese, oameni;**
- **Identificarea vulnerabilităţilor şi a ameninţărilor din interior cât exterior;**
- **Cuantificarea şi măsurarea scenarilor de risc;**
- **Identificarea controalelor aplicabile;**
- **Stabilirea registrului de riscuri şi identificarea riscurilor reziduale sau a scenariilor necotrolate.**

Analiza de risc urmează să cuprindă cel puțin următoarele etape:

Etapa de pre-audit / planificare

Informațiile necesare pentru executarea evaluării securității vor fi 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 va fi 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.

Etapa de audit efectiv / execuție

Faza de execuție este faza principală de audit, 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.

Etapa post-execuție

Următoarele sarcini vor fi executate în această fază:

- analiza vulnerabilităților sau neconformitatilor identificate;
- se realizează identificarea cauzei principale (root cause) a aparitiei lor;
- analiza riscurilor in baza:
    - ISO 31000:2018 "Risk Management—Principles and Guidelines";
    - ISO 27001:2018 "Information Technology—Security techniques—Information Security Management Systems—Requirements";
    - ISO 27002:2013 "Information Technology–Security techniques–Code of practice for Information Security management";
    - ISO 27005:2011 "Information Technology–Security techniques–Information Security Risk Management".
- elaborarea recomandărilor pentru măsuri de reducere a riscului;
- elaborarea raportului final.

Lista domeniilor de audit si a controalelor ce necesită de fi efectuate:

	Domeniu
1	**Managementul securitatii informatiei**
1.1	Organigrama si rolul securitatii in organizatie
1.2	Politica de securitate
1.3	Gestiunea riscului datelor cu caracter personal
2	**Managementul continuitatii afacerii**
2.1	Organizarea BCM
2.2	Definirea cerințelor cu privire la continuitate
2.3	Planurile de continuitate
2.4	Testarea planurilor de continuitate, proceduri de backup
2.5	Recuperarea in caz de dezastru
2.6	Răspunsul la incidente
3	**Securitatea informațiilor in cadrul resurselor umane**
3.1	Proceduri de angajare
3.2	Proceduri in timpul perioadei de angajare
3.3	Instruirea angajaților privind conștientizarea rolului securității în organizație
3.4	Proceduri la finalizarea contractului de munca
4	**Securitatea Operațiunilor**
4.1	Proceduri si responsabilități privind securitatea operațiunilor
4.2	Managementul livrării de servicii din partea unei terțe părți
4.3	Protejarea mediilor de stocare
4.4	Protecția împotriva scurgerilor de informație
4.5	Schimbul de informație
4.6	Distrugerea informației
5	**Securitatea Sistemelor IT**
5.1	Arhitectura infrastructurii IT
5.2	Securitatea serverelor si stațiilor de lucru
5.3	Securitatea comunicațiilor
5.3	Securitatea dispozitivelor portabile
5.4	Securitatea echipamentelor de retea
5.5	Securitatea rețelei (acces extern, WiFi, VPN)
5.6	Monitorizare, detectare si răspuns la incidente
6	**Achiziția, dezvoltarea si mentenanța sistemelor IT**
6.1	Definirea cerințelor de securitate
6.2	Securitatea in cadrul procesului de dezvoltare
6.3	Managementul vulnerabilităților
7	**Managementul accesului**

7.1	Politica privind controlul accesului
7.2	Definirea rolurilor si drepturilor de acces ale utilizatorilor
7.3	Autentificare, autorizare si trasabilitate in cadrul sistemelor si aplicațiilor
7.4	Echipamente mobile si acces de la distanta
8	**Managementul resurselor**
8.1	Definirea proprietarilor de informație
8.2	Responsabilitatea pentru resurse
8.3	Clasificarea informațiilor
9	**Securitatea fizica**
9.1	Concept de securitate fizica in cadrul organizației
9.2	Zonele de securitate pe nivele de risc
9.3	Securitatea perimetrala a clădirii
9.4	Sistemul control acces
9.5	Sistemul de supraveghere video
9.6	Sistemul de detecție si stingere a incendiilor
9.7	Centru de date; Camere tehnice; camera serverelor

LIVRABILE

Rapoartele furnizate de prestator vor fi prezentate direct Beneficiarului si vor fi structurate în două părți distincte: **partea executiva** si **partea tehnica**. Acestea au ca obiectiv de a identifica si evalua riscurile la adresa securității informației in cadrul infrastructurii IT a Moldovagaz. **Partea executiva** va conține descrierea pe scurt a neconformităților si riscurilor identificate si va utiliza metode grafice (cel puțin diagrame, grafice sau hărți).

- **Partea tehnica** va detalia din punct de vedere tehnic neconformitățile si riscurile identificate. Partea tehnica va conține cel puțin următoarele capitole:
    - Sumar executiv;
    - Obiectivele si scopul evaluării;
    - Prezentare succinta a metodologiei utilizate in cadrul auditului;
    - Descrierea contextului in care s-a desfășurat auditul;
    - Prezentarea individuala a riscurilor descoperite, după cum urmează:
        - Descrierea riscului;
        - Catalogarea riscului;
        - Descrierea tehnica;
        - Analiza severității si probabilității;
        - Calcularea riscului;
        - Masuri recomandate pentru reducerea riscului.
        - Alte detalii si recomandări;
        - Anexa cu lista controalelor de securitate efectuate.

2. **Cerințe față de ofertant**
   La concurs vor fi admise doar ofertele operatorilor economici care întrunesc următoarele criterii:
   - să dețină actele permisive necesare (licențele, de acreditare, de atestare etc.) pentru practicarea acestui tip de activitate
   - dotare tehnică și personal calificat în vederea executării prevederilor contractului;
   - operatorul economic nu trebuie să fie inclus în listele neadmisibile la procedurile de achiziții a Beneficiarului sau Agenției pe Achiziții Publice;
   - nu este în incapacitate de plată sau insolvabilitate, să nu se afle în proces de lichidare, bunurile nu trebuie să fie sechestrate, activitatea economică nu trebuie să fie suspendată;
   - Experiență similară și competență în domeniu
     - Cel puțin un contract realizat în Republica Moldova, de o valoare nu mai mică decât valoarea ofertei depuse (complexitate similară).
     - Cel puțin o scrisoare de recomandare de la entitățile în care au fost livrate soluții similare.
   - să nu înregistreze datorii față de Buget de Stat sau alte fonduri guvernamentale;

3. **Cerinte fata de echipa ofertantului:**
   Membrii echipei de proiect trebuie să fi compus din cel puțin 2 persoane care cumulativ dețin următoarele certificări
   - Certificat Auditor Intern Securitate Informațională ISO 27001:2022;
   - Offensive Security Certified Professional (OSCP)
   - Licensed Penetration Tester (LPT)
   - Global Industrial Cyber Security Professional (GICSP)
   - Offensive Security Wireless Professional (OSWP)
   - Certified Ethical Hacker
   - Certified Information Systems Auditor (CISA)
   - Certified Information Security Manager (CISM)
   - Offensive Security Certified Professional
   - Offensive Security Wireless Professional