Cerințe funcționale și tehnice pentru achiziția unei soluții de administrare, audit și monitorizare a infrastructurii Active Directory

1. Context și obiectiv

Instituția urmărește achiziția unei soluții software integrate pentru administrarea, auditarea și monitorizarea infrastructurii de tip Active Directory, cu scopul creșterii nivelului de securitate, automatizării proceselor administrative și asigurării trasabilității operațiunilor efectuate asupra conturilor, grupurilor, politicilor și resurselor IT.

Soluția propusă trebuie să permită administrarea centralizată a mediilor multi-domeniu, monitorizarea modificărilor critice asupra infrastructurii și realizarea de audituri periodice privind drepturile de acces și utilizarea conturilor privilegiate sau nenominale.

2. Cerințe generale

Soluția ofertată trebuie să fie compatibilă cu infrastructuri Microsoft Active Directory și să permită integrarea facilă în mediul existent al instituției.

Se solicită ca aplicația să fie disponibilă în arhitectură web și să permită accesul securizat prin autentificare bazată pe roluri și politici de control al accesului.

Soluția trebuie să permită:

- administrarea centralizată a utilizatorilor, grupurilor și unităților organizaționale;
- generarea de rapoarte detaliate și exportabile;
- configurarea de alerte automate;
- păstrarea jurnalelor de audit pe termen lung;
- delegarea granulară a drepturilor administrative;
- integrarea cu mecanisme de autentificare enterprise.

2.1 Cantități și licențiere

Pentru toate produsele licențierea propusă trebuie să includă toate componentele necesare funcționării complete a soluției/ componentei.

A. Software de administrare, audit și monitorizare a infrastructurii Active Directory

- licențiere în regim perpetuu (Perpetual Licensing Model)
- 200 utilizatori domeniu;
- 2 domenii Active Directory;
- minimum 5000 obiecte utilizator monitorizate și administrate.

B. Audit și monitorizare Active Directory

- licență perpetuă pentru auditarea a 5 Domain Controllers principale și 2 DC secundare;
- drept permanent de utilizare;
- monitorizare și audit centralizat al activităților și evenimentelor.

C. File Integrity Monitoring

- licență perpetuă pentru auditarea a 5 File Servers;
- monitorizarea accesului și modificărilor asupra fișierelor și directoarelor;
- funcționalități de File Integrity Monitoring.

D. Windows Servers

- licență perpetuă pentru auditarea și monitorizarea a 100 Windows Servers;
- cantitate solicitată: 2 bucăți;
- drept permanent de utilizare.

3. Cerințe tehnice și funcționale

3.1 Cerințe privind administrarea infrastructurii Active Directory

Soluția trebuie să ofere funcționalități complete pentru administrarea infrastructurii Active Directory, inclusiv:

3.1.1 Administrare multi-domeniu

Soluția trebuie să permită administrarea centralizată a mai multor domenii Active Directory din aceeași interfață, fără necesitatea conectării separate pe fiecare domeniu.

Se solicit ca soluția să permită:

- administrare simultană a obiectelor din mai multe domenii;
- suport pentru relații de trust între domenii;
- administrare unificată a utilizatorilor și grupurilor;
- posibilitatea aplicării de politici și operațiuni în mod centralizat;
- vizualizare consolidată asupra infrastructurii.

3.1.2 Automatizarea operațiunilor administrative

Soluția trebuie să permită automatizarea activităților repetitive, minim:

- creare/modificare/dezactivare conturi;
- resetare parole;
- mutare utilizatori între unități organizaționale;
- gestionare grupuri de securitate;
- activarea/dezactivarea conturilor inactive.

Trebuie să existe posibilitatea programării de task-uri automate și utilizarea de șabloane operaționale.

3.1.3 Delegarea controlată a drepturilor

Soluția trebuie să permită delegarea granulară a drepturilor administrative fără acordarea de privilegii excesive la nivel de domeniu.

Se solicita ca soluția să permită:

- definirea de roluri administrative;
- limitarea accesului pe obiecte și operațiuni;
- trasabilitatea activităților efectuate de administratori;
- jurnalizarea tuturor operațiunilor efectuate.

3.2 Cerințe privind auditul și monitorizarea infrastructurii

3.2.1 Audit și monitorizare Active Directory

Soluția trebuie să permită monitorizarea și auditarea în timp real a modificărilor efectuate asupra infrastructurii Active Directory.

Soluția trebuie să permit monitorizarea cel puțin a următoarele tipuri de evenimente:

- creare, modificare și ștergere utilizatori;
- modificări asupra grupurilor și apartenențelor;
- modificări de politici și permisiuni;
- modificări asupra obiectelor critice;
- activități privilegiate;
- tentative de acces neautorizat.

De asemenea soluția trebuie să permită:

- generarea de alerte în timp real;
- definirea de praguri și reguli personalizate;
- păstrarea istoricului modificărilor;
- generarea de rapoarte pentru audit intern și conformitate.

3.2.2 File Integrity Monitoring (FIM)

Soluția trebuie să includă funcționalități de monitorizare a integrității fișierelor (File Integrity Monitoring), prin care să poată fi detectate modificările neautorizate asupra fișierelor și directoarelor critice.

Se solicită ca soluția să permită:

- monitorizarea fișierelor și folderelor critice;
- detectarea modificărilor, ștergerilor și redenumirilor;
- identificarea utilizatorului care a efectuat modificarea;
- alertare în timp real;
- păstrarea istoricului modificărilor;
- posibilitatea definirii unor politici personalizate de monitorizare.

Soluția trebuie să permită auditarea fișierelor cu relevanță operațională și de securitate, inclusiv fișiere de configurare, politici și documente sensibile.

3.2.3 User Access Review – conturi nenominale

Soluția trebuie să permită realizarea de procese periodice de revizuire a drepturilor de acces (User Access Review), cu accent pe conturile nenominale și conturile cu privilegii ridicate.

Se solicită ca soluția să permită:

- identificarea conturilor nenominale;
- identificarea conturilor inactive sau neutilizate;
- evidențierea conturilor privilegiate;
- raportarea accesului acordat utilizatorilor și grupurilor;
- posibilitatea certificării periodice a drepturilor de acces;
- exportul rapoartelor în formate standard.

Soluția trebuie să permită implementarea unui proces formal de recertificare a accesului și să contribuie la reducerea riscurilor asociate conturilor generice sau partajate.

3.3. Cerințe privind raportarea și conformitatea

Soluția trebuie să includă un modul avansat de raportare și conformitate, capabil să genereze:

- rapoarte predefinite;
- rapoarte personalizabile;
- export în format PDF, CSV și XLSX;
- rapoarte programate automat;
- dashboard-uri centralizate.

Se solicită suport pentru cerințe de audit și conformitate privind securitatea informației și trasabilitatea accesului.

3.4 Modul Governance, Risk and Compliance (GRC)

Soluția trebuie să inlcudă un modul dedicat GRC care să asigure minim:

- guvernanță IT;
- analiză și control al drepturilor de acces;
- audit și conformitate;
- procese de recertificare a accesului;
- identificarea conturilor nenominale și privilegiate.

3.5. Cerințe privind securitatea

Soluția trebuie să respecte bunele practici de securitate și să permită:

- autentificare securizată;
- comunicare criptată;
- jurnalizare completă a operațiunilor;
- segregarea drepturilor administrative;

- integrare cu infrastructura existentă de securitate.

4. Cerințe privind suportul și implementarea

Livrarea soluției va include:

- instalarea soluției;
- configurarea componentelor software;
- integrarea cu infrastructura Active Directory existentă;
- configurarea monitorizării și auditului;
- configurarea alertelor și notificărilor;
- configurarea politicilor de acces și delegare;
- testarea funcționalităților;
- punerea în producție.

4.1 Servicii de instruire

Cerințe minime:

- sesiune online/fizic de instruire;
- durată minimă: (administrare, provisioning, automatizări, rapoarte) - 8 ore
- durată minimă: (auditare AD, file servers, alerte, compliance) - 8 ore
- durată minimă: Pentru un workshop intensiv cu laboratoare practice și scenarii reale de producție, 3 zile (24 ore)
- maximum 5 participanți;
- instruire în limba română;
- documentația de curs și materialele suport vor fi furnizate în limba română.

Tematicile minime vor include:

- administrarea soluției;
- configurarea alertelor și rapoartelor;
- administrarea drepturilor de acces;
- monitorizarea și auditarea infrastructurii;
- operațiuni de mentenanță și troubleshooting.

4.2. Livrabile

Materialele livrabile vor include minim:

- licențelor software;
- documentației tehnice;
- ghidurilor de administrare;
- procedurilor de backup și restaurare;
- documentelor de configurare și punere în funcțiune.

- documentația de curs și materialele suport în limba română

4.3 Garanție și suport

Toate produsele vor beneficia de garanție, mentenanță și suport pentru 60 de luni de la livrare, pentru toate componentele soluției.

Servicii disponibile în perioada de garanție, mentenanță și suport:

- actualizări software, suport și mentenanță
- suport remote
- suport pentru optimizare și ajustări de configurare;
- suport pentru incidente operaționale;
- recomandări privind bune practici de administrare și securitate.