CAIET DE SARCINI
Sistem Informatic Managerial ”e-ANFP”
Întărirea capacităţii instituţionale a ANFP în vederea asigurării unui management performant al funcţiei publice şi funcţionarilor publici la nivelul administraţiei publice centrale şi al serviciilor publice din subordinea/coordonarea autorităţilor publice centrale şi locale prin implementarea de instrumente inovatoare”

AXA PRIORITARĂ

Axa prioritară 2 - ”Îmbunătăţirea calităţii şi eficienţei furnizării serviciilor publice, cu accentul pus pe procesul de descentralizare”

DOMENIUL DE INTERVENŢIE

Domeniul major de intervenţie 2.2 – ”Îmbunătăţirea calităţii şi eficienţei furnizării serviciilor”

OPERAŢIUNEA

Implementarea iniţiativelor de reducere a duratei de livrare a serviciilor publice prin folosirea sistemelor informatice de management, respectiv semnătură electronică, arhivare electronică şi flux informatic unitar de raportare şi monitorizare

NOTĂ:
Caietul de sarcini, respectiv prezentul document, face parte integrantă din documentaţia pentru atribuirea contractului şi constituie ansamblul cerinţelor pe baza cărora se elaborează de către fiecare ofertant, propunerea tehnică.
Cerinţele impuse sunt considerate ca fiind minimale. Ofertarea de servicii inferioare celor prevăzute în Caietul de sarcini sau care nu satisfac cerinţele Caietului de sarcini va avea drept consecinţă declararea ofertei ca fiind neconformă.

Specificaţiile tehnice care indică o anumită origine, sursă, producţie, un procedeu special, o marcă de fabrică sau de comerţ, un brevet de invenţie, o licenţă de fabricaţie, sunt menţionate doar pentru identificarea cu uşurinţă a tipului de produs şi NU au ca efect favorizarea sau eliminarea anumitor operatori economici sau a anumitor produse. Aceste specificaţii vor fi întotdeauna considerate ca având menţiunea «sau echivalent».

CUPRINS

1. Informaţii generale

1.1 Instituţia Achizitoare

Instituţia Achizitoare a prezentului proiect - Agenţia Naţională a Funcţionarilor Publici (ANFP) - a fost înfiinţată prin Legea nr. 188/1999 privind Statutul funcţionarilor publici, cu scopul de a asigura managementul funcţiilor publice şi cel al funcţionarilor publici.

ANFP funcţionează în subordinea Ministerului Dezvoltării Regionale şi Administraţiei Publice, conform Hotărârii Guvernului privind organizarea şi funcţionarea Ministerului Dezvoltării Regionale şi Administraţiei Publice.

Atribuţiile principale ale ANFP se regăsesc în Legea nr. 188/1999 privind Statutul funcţionarilor publici (r2) cu modificările şi completările ulterioare, iar activitatea ANFP este reglementată de prevederile Hotărârii de Guvern nr. 1000/2006 cu modificările şi completările ulterioare.
Conducerea Agenţiei este asigurată de un preşedinte, cu rang de secretar de stat, ajutat de un vicepreşedinte cu rang de subsecretar de stat, numiţi prin decizia primului ministru, la propunerea ministrului Dezvoltării Regionale şi Administraţiei Publice.

Atribuţiile principale ale Agenţiei Naţionale a Funcţionarilor Publici sunt:

- elaborarea cadrului legislativ privind funcţia si funcţionarii publici;
- monitorizarea si controlul aplicării reglementarilor in domeniu;
- gestionarea programelor privind funcţia publică, prin intermediul cărora se realizează managementul funcţiei şi funcţionarilor publici;
- colaborarea cu alte instituţii din ţară şi din străinătate, în vederea perfecţionării pregătirii profesionale a funcţionarilor publici;
- centralizarea nevoilor de instruire ale funcţionarilor publici;
- furnizarea programelor de formare şi perfecţionare profesională pentru personalul din administraţia publică;
- administrarea bazei de date cuprinzând evidenţa naţională a funcţiilor publice şi a funcţionarilor publici.

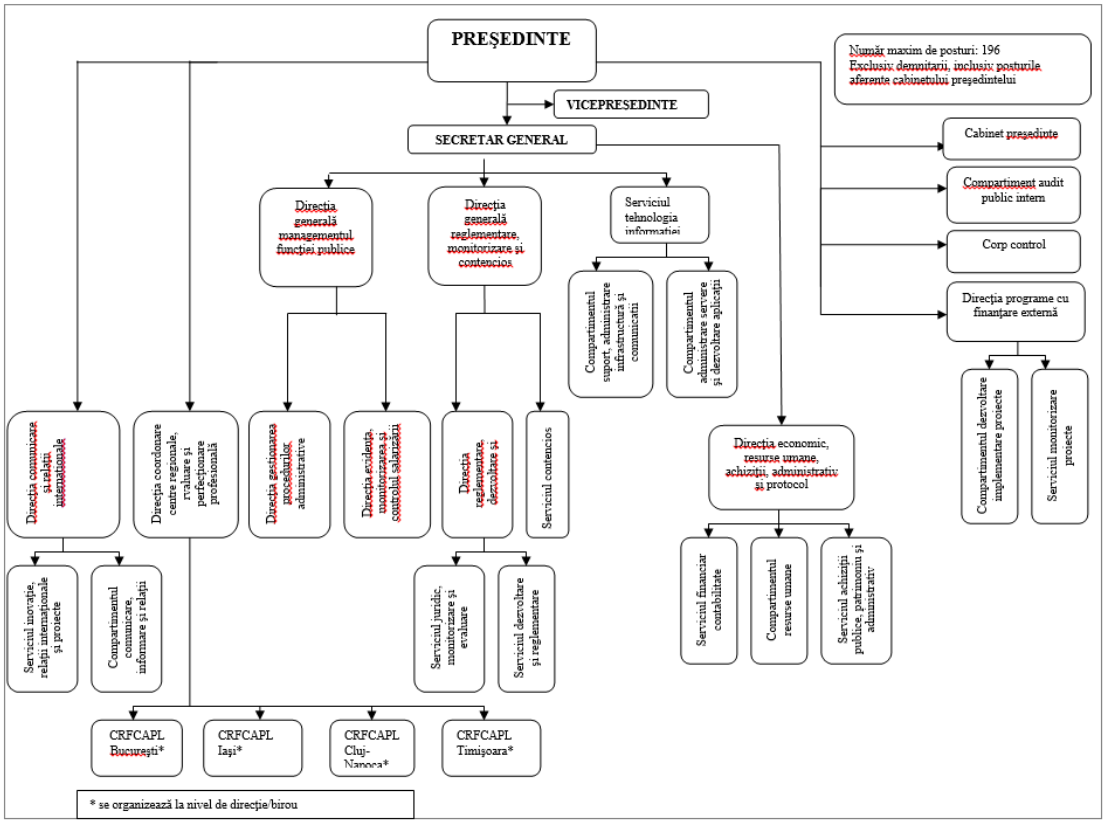
Beneficiarii activităţii Agenţiei Naţionale a Funcţionarilor Publici sunt următorii:

- funcţionarii publici, prin:
  - monitorizarea eficientă a aplicării Legii nr. 188/1999 (r2) cu modificările şi completările ulterioare, precum si a legislaţiei secundare, astfel încât să fie respectat principiul transparenţei în organizarea şi dezvoltarea carierei în funcţia publică;
  - planificarea carierei în funcţia publică prin elaborarea planului de ocupare a funcţiilor publice, cu respectarea principiilor egalităţii de şanse, competenţei, competiţiei, profesionalismului şi motivării;
  - crearea unor mecanisme de recompensare a performantelor personale individuale;
  - asigurarea unui sistem unitar de salarizare a funcţionarilor publici, transparent, motivant, predictibil;
  - perfecţionarea pregătirii profesionale a funcţionarilor publici.
- cetăţenii, prin:
  - instituirea unui serviciu public stabil, profesionist, transparent, eficient şi imparţial în interesul cetăţenilor;
  - eficientizarea managementului funcţiei publice şi funcţionarilor publici, pentru asigurarea continuităţii şi celerităţii serviciului public;
  - stabilirea unor norme deontologice în raporturile dintre funcţionarii publici şi cetăţeni.
- autorităţile şi instituţiile publice ale administraţiei publice centrale şi locale, prin:
  - aplicarea coerentă şi unitară a reglementărilor legale în domeniul funcţiei publice şi funcţionarilor publici;
  - instituirea unor mecanisme de comunicare inter-instituţională eficientă;
  - coordonarea metodologică a compartimentelor de resurse umane din cadrul autorităţilor si instituţiilor publice.

1.2 Structura organizaţională

Organigrama ANFP este prezentată mai jos:

STRUCTURA ORGANIZATORICĂ A AGENŢIEI NAŢIONALE A FUNCŢIONARILOR PUBLICI



1.3 Descrierea situaţiei actuale

Descrierea situaţiei actuale este structurată pe 4 zone funcţionale - zone adresate direct de către cele 4 obiective ale prezentului proiect, şi anume:

- Arhiva instituţională;
- Sisteme Informatice utilizate;
- Semnătură electronică calificată;
- Camera serverelor;

În plus faţă de zonele de mai sus, descrierea va evidenţia şi alte aspecte din domeniul (tehnologiei) informaţional(e), precum:

- Monitorizare şi administrare sisteme şi utilizatori;
- Salvare şi restaurare a datelor;
- Audit informatic.

Notă: Detalii suplimentare faţă de conţinutul acestui capitol vor fi subiectul exclusiv al activităţii de analiză din cadrul implementării proiectului Sistem e-ANFP.

1.3.1 Arhiva instituţională

ANFP posedă la ora actuală o arhivă fizică conţinând documentele (organizate de cele mai multe ori sub formă de dosare) de uz intern în format tipărit, fără a avea implementată o soluţie informatică de tip arhivă electronică. Din punct de vedere volumetric, arhiva ANFP se compune din:

- Documente deja arhivate şi stocate în camere amenajate ca şi arhive fizice totalizând :

    - 5.6 milioane pagini A4;
    - 0.5 milioane pagini format < A4;
    - 0.4 milioane pagini A3.
- Documente arhivate sau în curs de arhivare şi stocate în birourile utilizatorilor totalizând:
    - 4.8 milioane pagini format A4.

Principalele neajunsuri evidenţiate în zona de arhivare fizică sunt:

- Beneficiarii direcţi sau indirecţi au acces greoi la informaţiile din cadrul dosarelor procesate de ANFP din cauza timpilor mari datoraţi operării arhivei fizice;
- Birocraţia aferentă operaţiunilor cu caracter repetitiv de solicitare de acces la informaţii, acordare de acces, căutare efectivă în arhivă, punerea la dispoziţia solicitantului a informaţiilor cerute, etc.;
- Efort suplimentar din partea angajaţilor ANFP de încărcare manuală a informaţiilor aferente arhivei fizice în cadrul oricărui sistem informatic care ar solicita acest gen de informaţii;
- Lipsa posibilităţii de furnizare electronică în regim automatizat a documentelor sau informaţiilor deţinute către alte sisteme informatice prin intermediul interconectivităţii;
- Îngreunarea constantă a timpilor de acces la informaţii precum şi de adaptare la schimbări din cauza creşterii continue a volumului arhivei fizice;
- Eforturi mari şi cu caracter repetitiv de administrare a arhivei (aranjare, rearanjare, indexare, transport, etc.);
- Lipsa unei forme de automatizare electronică în lucrul cu documentele arhivei ce menţine riscul de greşală umană la cote înalte;
- Lipsa unui suport adecvat pentru raportare privind arhiva (ex.: imposibilitatea oferirii unor informaţii aferente statusului dosarelor, imposibilitatea calculului unor indicatori de performanţă ai arhivei, etc.);
- Imposibilitatea menţinerii caracterului centralizat pe care trebuie să-l deţină o arhivă;
- Imposibilitatea asigurării unui nivel de securitate optim pentru o arhivă de documente;
- Riscurile asociate deteriorării sau pierderii accidentale de documente.

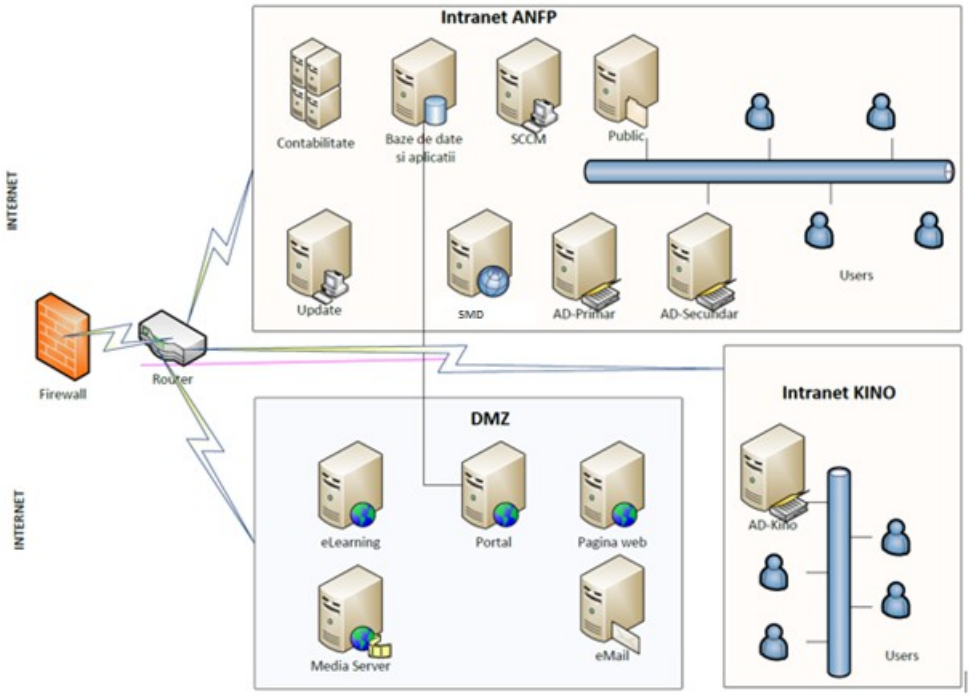
1.3.2 Sisteme informatice utilizate

1.3.2.1 Componenta software

Sistemele (sau aplicaţiile) informatice utilizate în prezent de către ANFP sunt:

- Sistem tip ”Portal” de management a funcţiilor publice şi al funcţionarilor publici;
- Site (web) ANFP;
- Sistem tip e-Learning;
- Sistem tip DMS;
- Sistem Informaţional Integrat privind Funcţia Publică şi Funcţionarii Publici (”MIGBOOK”);
- Sistem de gestiune cursuri şi cursanţi;
- Sistem de solicitare intervenţie IT (suport utilizatori);
- Sistem de legislaţie;
- Sistem de evidenţă a salariaţilor;
- Sistem de Contabilitate, Salarizare şi Gestiune Mijloace Fixe;
- Sistem de email.

În figura de mai jos sunt evidenţiate principalele sisteme din lista de mai sus:



Principalele neajunsuri evidenţiate în urma serviciilor de audit informatic sunt:

- TEHNOLOGIE/APLICAŢII/OPERAŢIONAL:
  - Utilizarea unor tehnologii învechite (ex.: Microsoft Windows Server 2003, Microsoft SQL Server 2005, etc.);
  - Utilizarea pe alocuri a unor componente (sau aplicaţii) informatice nepotrivite cu cerinţele utilizatorilor şi/sau capabilităţile tehnologice modern (ex.: Microsoft Excel);
  - Lipsa suportului oficial (în cazul unora dintre sisteme);
  - Lipsa unui contract între ANFP şi Furnizor (în cazul sistemului tip DMS);
  - Lipsa mediilor de dezvoltare şi/sau testare (în cazul unora dintre sisteme);
  - Lipsa integrării unora dintre sistemele de mai sus cu componenta Microsoft Active Directory, componentă implementată la ANFP;
  - Lipsa unor capabilităţi reale de integrare între sistemele de mai sus, acolo unde s-ar impune;
  - Lipsa posibilităţii de lucru în regim de flux(, din cauza lipsei unei componente specifice tip BPM), care să implice paşi predefiniţi, actori şi activităţi asociate, niveluri de aprobare şi/sau escalare;
  - Lipsa posibilităţilor de procesare (ex.: captură, indexare, arhivare) a documentelor în format tipărit;
  - Lipsa certificatelor (tip semnătură electronica calificată) pentru utilizatorii portalului ANFP, din teritoriu;

- Lipsa unor echipamente dedicate de scanare pentru captură;
- Lipsa unor echipamente de lucru pentru personalul administrative IT cu suport pentru mobilitate;

- ADMINISTRARE/SECURITATE:
  - Lipsa unui acces granular al utilizatorilor la funcţiilor sistemelor informatice(, din cauza lipsei unor componente avansate de management a accesului şi a identităţii utilizatorilor);
  - Lipsa mobilităţii în privinţa efectuării operaţiunilor zilnice pentru administratorii sistemelor informatice;
  - Lipsa unor capabilităţi moderne de management a activelor (”assets”) IT;
  - Lipsa unor instrumente moderne de management a performanţelor aplicaţiilor pentru ca administratorii ANFP să poată monitoriza gradul de utilizare a infrastructurii şi să poată măsura nivelul de experienţă al utilizatorilor;
  - Lipsa unei componente moderne de salvare şi restaurare a Serviciului Director.
- SUPORT UTILIZATORI:
  - Lipsa unei componente moderne de tip ”Help-Desk”.
- SALVARE/RESTAURARE:
  - Lipsa unor scheme de salvare şi recuperare a datelor adecvate (pentru unele sisteme);
  - Lipsa unui sistem funcţional centralizat de salvare şi restaurare a datelor la nivelul ANFP.
- ”BUSINESS CONTINUITY”:
  - Utilizarea unei camere a serverelor dotată şi/sau amenajată necorespunzător standardelor IT modern;
  - Lipsa unei camere (secundare) a serverelor pentru backup (centralizat) ca şi suport pentru ”Disaster Recovery”.

1.3.2.2 Componenta hardware:

ANFP are în uz multiple echipamente hardware de clasă server precum servere de procesare, servere de baze de date, servere de stocare în reţea, echipamente de reţea şi/sau securitate, precum şi posturi de lucru client (laptop sau desktop) (Notă: Detalii privind tipul şi numărul de bucăţi din fiecare fac obiectul etapei de analiză din cadrul implementării proiectului).
Principalele neajunsuri evidenţiate în urma serviciilor de audit informatic sunt:

- Existenţa unor ”Single Point of Failure” la nivelul conecticii şi securităţii reţelei;
- Imposibilitatea (actuală a) implementării unei arhitecturi superioare la nivel de reţea cauzată de lipsa unor echipamente dedicate.

1.3.3 Semnătura electronică calificată

În prezent ANFP utilizează semnătura electronică calificată pentru utilizatorii interni (de la Sediul Central din Bucureşti). Neajunsul aici este lipsa acestei capabilităţi pentru utilizatorii din autorităţile şi instituţiile publice din România.

1.3.4 Camera serverelor

În prezent ANFP utilizează o camera a serverelor la Sediul Central din Bucureşti. Serviciile de audit informatic au scos la iveală o serie de neajunsuri, precum:

- Spaţiu util insuficient faţă de nevoile ANFP (astfel că anumite echipamente sunt locate la alte sedii);
- Risc ridicat în privinţa protecţiei seismice;

- Existenţa unor sisteme neadecvate (sau lipsa unor sisteme) de:
  - Securitate perimetrală;
  - Detectare şi stingere incendii;
  - Climatizare;
  - Alimentare cu energie electrică;
  - Podea/tavan tehnic;
  - Cablaj structurat.

ANFP va pune la dispoziţie un spaţiu la aprox. 400 km de Bucureşti, spaţiu actualmente neutilat şi care se doreşte a fi o camera a serverelor pentru asigurarea capabilităţilor (viitoare) de ”Disaster Recovery”.

1.3.5 Alte considerente

În plus faţă de aspectele evidenţiate în subcapitolele de mai sus, serviciile de audit informatic au identificat şi alte neajunsuri, precum:

- Lipsa unor instrumente specializate de detecţie a vulnerabilităţilor sistemelor informatice, precum şi de asigurare a conformităţii cu regulile de securitate interne ANFP si standardele in domeniu;
- Nevoia de colectare si stocarea securizată a fişierelor tip log, raportare şi alertare de conformitate precum şi investigarea asupra neconformităţilor de securitate în ANFP;
- Lipsa unui management unificat al securităţii organizaţionale;
- Nevoia de instruire a personalului administrativ în vederea utilizării detecţiei şi remedierii vulnerabilităţilor de securitate informatică.

2. Prezentarea generală a proiectului

2.1 Obiective

Obiectivul general al prezentului proiect *este îmbunătăţirea calităţii şi eficienţei serviciilor furnizate de către Agenţia Naţională a Funcţionarilor Publici în vederea modernizării capacităţii administrative a instituţiilor publice şi de a contribui la reforma sistemului administraţiei publice din România*.

Scopul prezentului proiect este dezvoltarea de instrumente inovatoare specifice pentru îndeplinirea eficientă a rolului şi atribuţiilor pe care ANFP le exercită în domeniul funcţiei publice şi al funcţionarilor publici referitoare la utilizarea semnăturii electronice la nivelul administraţiei centrale şi locale precum şi arhivarea electronică (scanarea) a documentaţiei existente în arhiva ANFP. Astfel, aceste elemente vor contribui la dezvoltarea capacităţii de management a Achizitorului şi îmbunătăţirea comunicării /relaţionării instituţiilor publice cu ANFP – ca agenţie centrală ce realizează managementul integrat al funcţiei publice şi al funcţionarilor publici.

Prin implementarea sa, proiectul va ajuta la întărirea capacităţii ANFP de a-şi îndeplini atribuţiile ce îi revin şi de a veni în sprijinul beneficiarilor direcţi ai serviciilor furnizate de către aceasta, în conformitate cu cerinţele standardelor europene.

Prezentul proiect îşi propune să furnizeze utilizatorilor instrumente informatice în scopul eficientizării şi scăderii timpilor de transmitere a documentelor financiare şi non-financiare cât şi de procesare a datelor, evitării întreruperilor ce pot apărea în fluxurile informaţionale între compartimentelor din cadrul ANFP, reducând astfel întârzierile în procesul decizional cu impact asupra activităţilor operative.

Utilizând instrumentele puse la dispoziţie de proiect se va putea cunoaşte în timp real situaţia funcţionarilor publici din administraţia publică din România, atât de la nivel central cât şi local, se vor preveni, în timp real, situaţiile de nerespectare a prevederilor în domeniul funcţiei publice

şi a funcţionarilor publici precum şi situaţia autorităţilor şi instituţiilor publice cu privire la managementul resurselor umane.
Din obiectivul general rezidă următoarele obiective specifice ale proiectului:

- Digitizare arhivă (fizică) a ANFP;
- Livrare şi implementare Sistem (Informatic Managerial – e-ANFP) de suport a lucrului în regim de fluxuri colaborative;
- Amenajare Cameră a Serverelor;
- Audit de securitate informatică;
- Implementare semnătură electronică (calificată) pentru grupul ţintă (conform 2.2 Grupuri ţintă);
- Implementarea arhivei electronice la nivelul ANFP.

2.2 Grupuri ţintă

Proiectul se adresează unui grup ţintă format din 1.930 de autorităţi şi instituţii publice din cadrul administraţiei publice centrale şi locale din România, repartizat şi din punct de vedere geografic, pe întreg spaţiul administrativ teritorial al României, după cum urmează :

- 14 ministere de linie (cu excepţia Ministerul Afacerilor Externe) şi Secretariatul General al Guvernului;
- 542 de autorităţi şi instituţii publice aflate în subordinea/coordonarea ministerelor şi a Secretariatul General al Guvernului;
- 10 autorităţii centrale autonome;
- 41 de Consilii Judeţene;
- 123 de servicii publice la nivel judeţean în subordinea Consiliului Judeţean;
- 103 Consilii Locale ale Municipiilor;
- 415 de servicii publice la nivel local în subordinea Consiliilor Locale ale Municipiilor;
- 217 Consilii Locale ale Oraşelor;
- 434 de servicii publice la nivel local în subordinea Consiliilor Locale ale Oraşelor;
- 6 Consilii Locale ale sectoarelor Municipiului Bucureşti;
- 24 de servicii publice în subordinea Consiliilor Locale ale sectoarelor Municipiului Bucureşti.

Proiectul se adresează unui grup ţintă format din 3.860 de funcţionari, câte 2 reprezentanţi din cadrul fiecărei autorităţi şi instituţii publice de la nivelul administraţiei publice centrale şi locale din România şi 140 de funcţionari publici şi personal contractual din cadrul ANFP, cu următoarea structură :

- 1.930 de responsabili, la nivel de management superior, cu coordonarea resurselor umane din cadrul fiecărei autorităţi şi instituţii publice de la nivel central şi local (secretari generali, secretari generali adjuncţi, prefect, subprefect, secretari de unităţi administrativ-teritoriale, secretari de subunităţi administrativ-teritoriale, conducători de instituţii publice – director general, director sau director executiv);
- 1.930 de responsabili, la nivel de execuţie, de resurse umane din cadrul fiecărei autorităţi şi instituţii publice de la nivel central şi local;
- 140 de funcţionari din cadrul ANFP - Sediul Central, astfel :
    a) 54 de funcţionari publici cu atribuţii în gestionarea funcţiei publice (avizare documentaţie de structură şi avize) ;
    b) 86 de funcţionari publici şi personal contractual în vederea utilizării arhivei electronice plus cei 54 de funcţionari publici de la pct. a).

Beneficiarii indirecţi vor fi: personalul din instituţiile şi autorităţile publice implicate în proiect, cetăţenii care vin în contact cu instituţiile respective, instituţiile administraţiei publice centrale şi

locale şi serviciilor publice deconcentrate ale ministerelor la nivel judeţean care vor beneficia de rezultatele proiectului.
În mod indirect, proiectul se adresează întregii administraţii publice prin efectul de cascadă generat ca urmare a diseminării experienţei dobândite de către cei 4000 de funcţionari publici participanţi la seminarii regionale de instruire către ceilalţi funcţionari ai instituţiilor apartenente.

2.3 Obiectul achiziţiei

Obiectul achiziţiei vine ca răspuns la obiectivele specifice ale proiectului şi este compus din:

- Servicii;
- Echipamente;
- Pachete licenţiere.

Notă : Toate amenajările spaţiilor puse la dispoziţie de Achizitor pentru camera serverelor (Data Center) inclusiv sistemele de reţelistică, echipamentele de protecţie şi de mediu, echipamente şi dotări etc. necesare asigurării funcţionalităţii sistemelor, executate, respectiv livrate în cadrul contractului, rămân în proprietatea Achizitorului.

2.3.1 Servicii

Serviciile incluse în obiectul achiziţiei sunt:

- **Digitizare arhivă (fizică) a ANFP:**
  - Analiză (specifică); se va aloca o perioadă minima de 15 zile de la data ordinului de începere a contractului;
  - Transport arhivă (fizică) de la ANFP către locaţia destinată prestării serviciilor de digitizare;
  - Digitizare (efectivă) a documentelor şi punerea (în regim continuu pe toată durata de realizare) la dispoziţia ANFP a noilor documente (electronice) procesate;
  - Returnare arhivă fizică (către ANFP) în locaţia/spaţiile indicate de către Achizitor;
  - Livrabil: documentaţie de analiză aprobată de ANFP, document ce conţine proceduri/fluxuri de lucru utilizate în prestarea acestor servicii în cadrul proiectului, document ce conţine recomandări către ANFP privind organizarea arhivei fizice după returul de la Prestator, document de utilizare a componentei de captură a Sistemului, document tip opis conţinând situaţia centralizată a documentelor digitizate (aprobat de ANFP).
- **Constituire de către Furnizor a arhivei electronice (în sensul Legii nr. 135/2007) pentru ANFP din cele 60.000 de documente semnate electronic de către Achizitor:**
  - Livrabil: arhiva electronică (la finalizarea serviciilor).

- **Implementare Sistem (Informatic Managerial – e-ANFP) de suport a lucrului** în regim de fluxuri colaborative:
  - Analiză: se va aloca o perioadă minimă de 60 zile de la data ordinului de începere a contractului;
  - Proiectare;
  - Dezvoltare/configurare inclusiv testare internă:
    - Dezvoltare/configurare în cadrul componentelor Sistemului e-ANFP (pentru livrarea licenţelor se va aloca o perioadă de maxim 120 de zile de la începerea de la data ordinului de începere a contractului);
    - Testare internă (per componentă a Sistemului e-ANFP).

- Implementare (deployment) în mediul de Producţie;
- Testare şi teste de acceptanţă:
    - Crearea şi agrearea cu ANFP a scenariilor de utilizare (încă din faza de analiză din cadrul implementării proiectului);
    - Testare Integrată (în vederea acceptanţei din partea ANFP).
- Intrarea în producţie:
    - Încărcare cu informaţii de lucru necesare (ex.: date şi documente rezultate în urma digitizării arhivei);
    - Asistenţă (acordată ANFP pe perioada) Go-live (a proiectului);
- Livrabil - un document care să conţină următoarele capitole:
    - specificaţii de analiză aprobată de ANFP,
    - procedurile de utilizare a Sistemului (manual de instruire), proceduri de administrare per componentă/echipament,
    - procedurile de utilizare per Sistem (manual de administrare),
    - scenariile de testare aprobate de ANFP,
    - specificaţiile tehnice de arhitectură macro şi micro a Sistemului,
    - specificaţiile tehnice de integrare/interfaţare cu alte sisteme/aplicaţii ANFP,
    - specificaţiile tehnice de configurare (şi acolo unde e cazul şi de dezvoltare) a componentelor Sistemului,
    - specificaţiile de raportare aprobate de ANFP,
    - specificaţiile de securitate a Sistemului,
    - recomandările de scalabilitate a Sistemului.

- **Amenajare Cameră a Serverelor:**
    - Livrare echipamente dedicate;
    - Instalare şi testare echipamente (dedicate);
    - Alte servicii de amenajare propriu-zisă precum cablarea în camera serverelor;
    - Livrabil - un document care să conţină următoarele capitole:
        - specificaţiile de analiză aprobată de ANFP,
        - procedurile de utilizare, administrare (şi întreţinere acolo unde e cazul) a echipamentelor,
        - scenariile de testare aprobate de ANFP,
        - specificaţiile tehnice de integrare,
        - specificaţiile tehnice de configurare.
- **Implementare semnătură electronica (calificată) pentru grupul ţintă:**
    - Livrare componente dedicate;
    - Servicii de suport a integrării semnăturii electronice cu sistemul tip ”Portal” de management a funcţiilor publice şi al funcţionarilor publici;
    - Livrabil document: documentaţie de analiză aprobată de ANFP, documentaţie de utilizare, administrare a componentelor aferente semnăturii electronice, document ce va conţine scenariile de testare aprobate de ANFP, specificaţii tehnice de integrare, specificaţii tehnice de configurare, Manual de utilizare a semnăturii electronice.

- **Audit de securitate informatică:**
    - Livrare componente dedicate;
    - Efectuarea propriu-zisă a serviciilor de auditare a Sistemului e-ANFP la finalul implementării acestuia;
    - Livrabil - un document care să conţină următoarele capitole:
        - specificaţiile de analiză aprobată de ANFP,

- scenariile de testare tip ”White-box” aprobate de ANFP,
- raport ce va conţine informaţii privind starea/nivelul de securitate al (componentelor) Sistemului evaluat în urma sesiunilor tip ”white-box testing”,
- propunerile de adresare/remediere a vulnerabilităţilor de securitate IT descoperite (dacă va fi cazul),
- recomandările bazate pe cele mai bune practici în domeniu şi/sau tendinţe moderne de securitate pentru sporirea securităţii Sistemului.

În plus faţă de categoriile de servicii prezentate mai sus se vor include următoarele categorii de servicii:

- **Instruire personal ANFP** (pentru detalii se va vedea în prezentul document la capitolul 6 – ”Instruirea în cadrul proiectului”):
  - Utilizatori (finali) ANFP de la Sediul Central:
    - Aferentă serviciilor de digitizare şi arhivare electronică;
    - Aferentă utilizării Sistemului Informatic Integrat e-ANFP;
    - Livrabile document: material de instruire în format tipărit şi electronic.
  - Utilizatorii (finali) ANFP din teritoriu:
    - Aferentă utilizării semnăturii electronice (calificate);
    - Livrabile document: material de instruire în format tipărit şi electronic.
  - Personal IT ANFP (de la Sediul central):
    - Aferentă amenajării camerei serverelor;
    - Aferentă administrării echipamentelor şi produselor software;
    - Aferentă serviciilor de audit de securitate (informatică);
    - Livrabil document: material (de la producători oficiali – acolo unde e cazul) de instruire în format tipărit şi electronic.
- Management al Contractului (pentru detalii se va vedea în prezentul document la capitolul 5 – ”Managementul Contractului, Organizare şi Metodologie”).

2.3.2 Echipamente

Echipamentele incluse în obiectul achiziţiei sunt:

- Livrare echipamente aferente Sistem (Informatic Managerial – e-ANFP):
  - Servere de:
    - Aplicaţii;
    - Baze de date.
  - Server de stocare unificată;
  - Cabinete metalice;
  - Echipamente tip ”UPS”;
  - Switch-uri cu conectivitate ”Fibre Channel”;
  - Switch-uri cu conectivitate ”Ethernet”;
  - Echipamente de securitate (tip ”Firewall/VPN”);
  - Scanere;
  - Echipamente pentru administratori (tehnici) ANFP:
    - Laptop-uri tip ”Rugged”;
    - Echipamente tip ”Thin Client”.

Detalii privind numărul de echipamente din fiecare tip (precum şi caracteristicile tehnice) se regăsesc în cadrul prezentului document în capitolul 4.5 – ”Infrastructura hardware”.

2.3.3 Pachete licenţiere

Pachetele de licenţe incluse în obiectul achiziţiei sunt evidenţiate (punctual) în cadrul prezentului document în capitolele:

- 4.2 – ”Infrastructură de susţinere a Lucrului cu Fluxuri Informatice”;
- 4.3 – ”Infrastructură de susţinere a Activităţii Administrative IT”;
- 4.4 – ”Infrastructură software de bază”.

3. Arhitectura Sistem Informatic Managerial

3.1 Arhitectura Funcţională

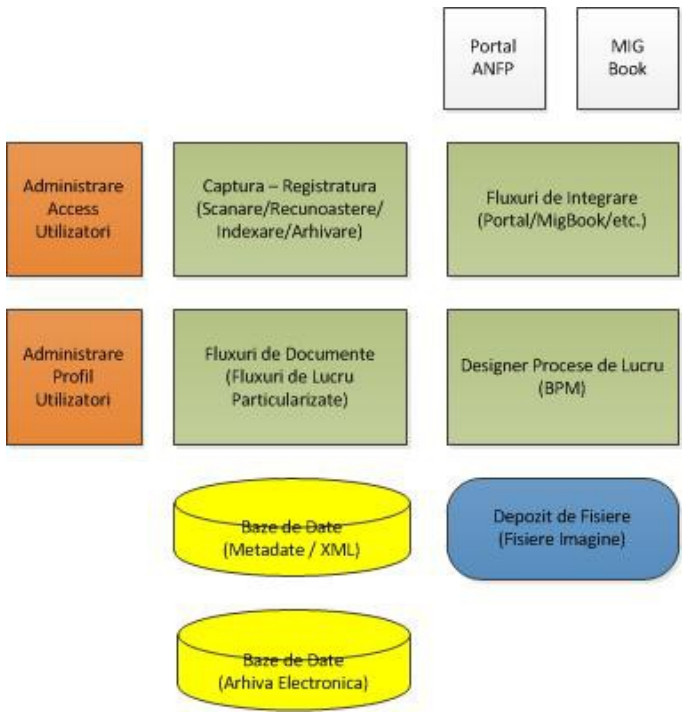
Din punct de vedere funcţional, componentele software ale Sistemului Informatic Integrat e-ANFP pot fi împărţite în două domenii majore, şi anume:

- Domeniu de susţinere a Lucrului cu Fluxuri informatice;
- Domeniu de susţinere a Activităţii Administrative IT.

Domeniile vor fi susţinute prin intermediul unor infrastructuri complexe, descrise detaliat în prezentul document în capitolul 3.3 – ”Infrastructură de susţinere a Lucrului cu Fluxuri Informatice” şi capitolul 3.4 – ”Infrastructură de susţinere a Activităţii de Administrare”. În plus faţă de aceste domenii, Sistemul e-ANFP include şi suportul pentru folosirea semnăturii electronice calificate de către utilizatorii ANFP din teritoriu (a se vedea cap. 2.1 – ”Obiective” şi cap. 2.3 – ”Obiectul achiziţiei” din prezentul document).

3.1.1 Lucrul cu Fluxuri Informatice

Arhitectura aferenta domeniului de Lucru cu Fluxuri Informatice este prezentată schematic in figura de mai jos:



Se identifică astfel următoarele componente:

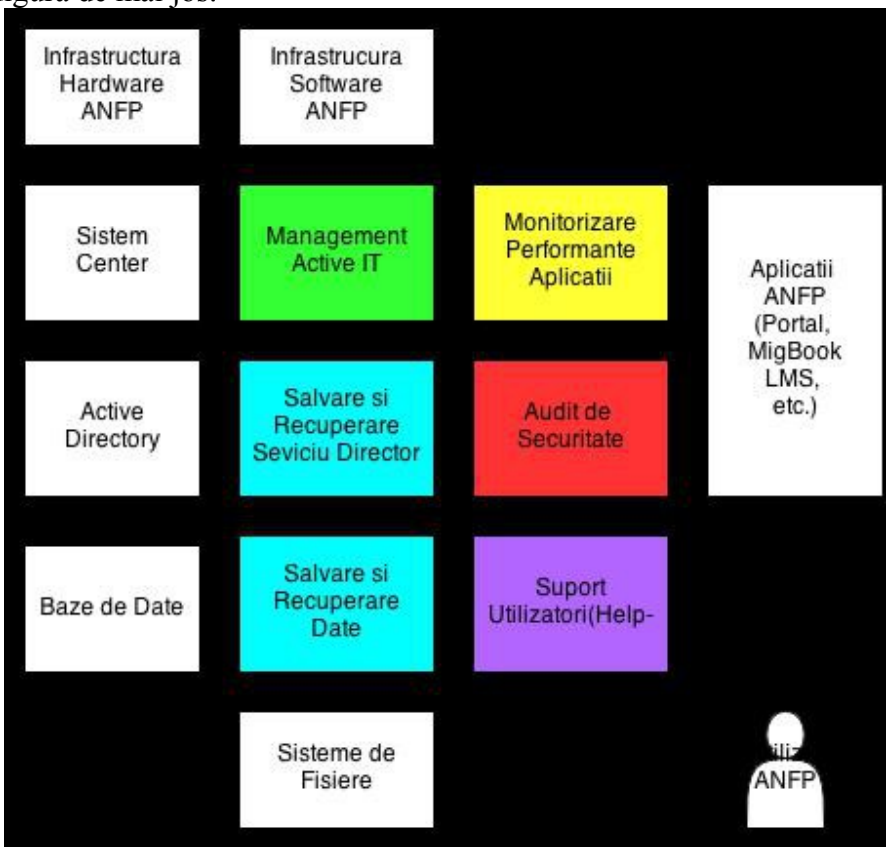
- Fluxuri Documente (pe bază de fluxuri de lucru personalizate);

- Captură – Registratură (conţinând totalitatea operaţiunilor de scanare/recunoaştere/indexare/arhivare) ;
- Fluxuri de Integrare (cu componente informatice precum Portalul ANFP sau Sistemul ”MigBook”);
- Designer Procese de Lucru (utilizând componentă dedicată tip ”BPM”);
- Componente de securitate(a accesului utilizatorilor în lucrul cu fluxurile informatice) precum:
  - Administrare acces utilizatori;
  - Administrare profil/identitate utilizator.
- Baze de Date (utilizând o componenta dedicata tip Sistem Relaţional de Baze de Date pentru stocarea metadate-lor şi a altor informaţii necesare);
- Componenta tip ”File Repository” pentru stocarea fişierelor imagine rezultate în urma digitizării documentelor (fizice).

Notă: componentele aflate în uz la Achizitor, respectiv Portalul ANFP şi Sistemul ”MigBook”, au fost evidenţiate pentru claritatea expunerii.

3.1.2 Susţinerea Activităţii Administrative IT

Arhitectura aferentă domeniului de susţinere a Activităţii Administrative IT este prezentată schematic în figura de mai jos:



Se identifică astfel următoarele componente:

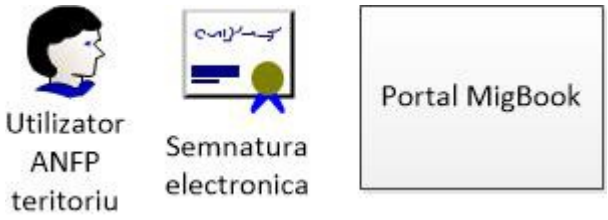
- Management Active IT;
- Monitorizare Performanţe Aplicaţii (informatice);
- Salvare şi Restaurare Centralizată a Datelor;
- Salvare şi Restaurare Centralizată a Serviciului Director;
- Suport Utilizatori (prin intermediul unei componente specifice de ”Help-Desk”);

- Suport pentru efectuarea Auditului de Securitate.

Notă: componentele aflate în uz la Achizitor, respectiv Infrastructura HW-SW, Aplicaţii ANFP, Serviciu Director, Sistem de Management tip "System Center" şi Sistem de Baze de Date, au fost evidenţiate pentru claritatea expunerii.

3.1.3 Semnătura electronica (calificată)

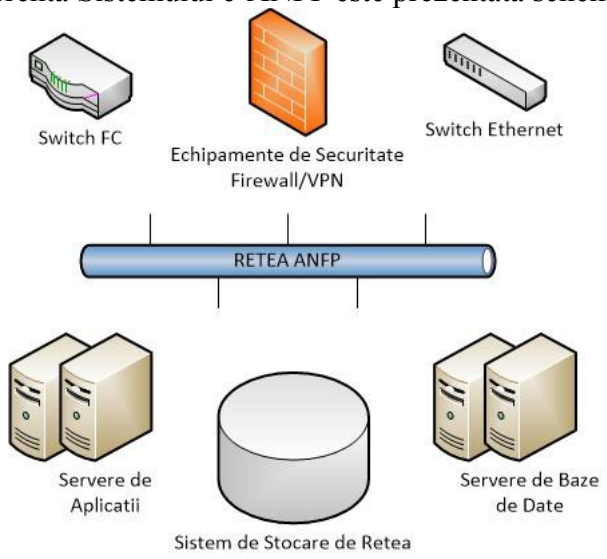
Arhitectura aferenta este prezentata schematic in figura de mai jos:



Se identifică componenta de susţinere a semnăturii electronica calificate.
Nota: componenta aflată în uz la Achizitor, respectiv Portalul MigBook a fost evidenţiate pentru claritatea expunerii.

3.2 Arhitectura Hardware

Arhitectura hardware aferenta Sistemului e-ANFP este prezentata schematic in figura de mai jos:



Se identifică următoarele componente:

- Servere de:
  - Aplicaţii;
  - Baze de date.
- Server de stocare în reţea;
- Switch-uri cu conectivitate "Fibre Channel";
- Switch-uri cu conectivitate "Ethernet";
- Echipamente de securitate (tip "Firewall/VPN");

Notă: Pentru claritatea expunerii alte echipamente hardware incluse în obiectul achiziţiei (a se vedea cap. 2.3.2 – "Echipamente" din prezentul document) nu au fost evidenţiate în figura de mai sus.

4. Descriere Sistem Informatic

4.1 Servicii

4.1.1 Digitizare arhivă ANFP

În efectuarea serviciilor de digitizare (a arhivei fizice ANFP) se vor îndeplini următoarele cerinţe:

- Arhivarea fizică a documentelor va respecta aspectele legale în materie, respectiv Legea nr. 16/1996 (r1) a Arhivelor Naţionale şi va îndeplinii normele de siguranţă la foc a construcţiilor pentru stocarea de documente.
- In efectuarea serviciilor de digitizare se vor respecta prevederile Legii nr. 677/2001 privind protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date, ANFP fiind operator de date cu caracter personal potrivit notificărilor nr. 5129, nr. 19986, nr. 20097, respectiv nr. 23269. Pentru vizualizarea categoriilor de date cu caracter personal prelucrate de către ANFP se poate consulta Registrul on line al notificărilor, disponibil pe pagina web a Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal, la adresa http://www.dataprotection.ro/notificare/cautari.do
- Pentru regăsirea cu uşurinţă a dosarelor în sistemul electronic şi pentru a asigura o legătura strânsă între dosarele fizice şi înregistrările electronice din sistemul electronic de arhivare se va utiliza un sistem de coduri de bare aplicate pe cutii şi rafturi, care împreună cu cititoarele de coduri de bare şi infrastructura de fluxuri informatice vor alcătui un sistem eficient de management al intrărilor-ieşirilor din şi în arhivă.
- Se va menţine integritatea documentelor gestionate asigurându-le împotriva distrugerii sau sustragerii precum şi accesul securizat la acestea.
- De asemenea, se va asigura suport pentru actualizarea/modificarea/completarea nomenclatorului arhivistic al ANFP.

4.1.1.1 Procesul Operaţional

În figura de mai jos este evidenţiată imaginea de ansamblu a activităţii propriu-zise de digitizare a documentelor (proces operaţional) din arhiva ANFP care se va presta în cadrul proiectului:

Acest proces operaţional se constituie din următoarele cinci etape:

- ETAPA 1 – Pregătirea Dosarelor in vederea digitizarii;
- ETAPA2 – Detectarea codurilor de bare şi generarea documentelor electronice PDF (care formează baza de date a cutiei);
- ETAPA 3 – Scanarea, indexarea şi verificarea metadatelor
- ETAPA 4 – Importarea documentelor electronice în sistemul electronic de management al documentelor.

Mai jos sunt detaliate activităţile specifice fiecărei etape.

ETAPA 1 – Pregătirea Dosarelor în vederea digitizării:

Aceasta etapă se va efectua cu respectarea prevederilor Legii Arhivelor Naţionale nr. 16/1996 republicată şi ale Instrucţiunilor privind activitatea de arhivă la creatorii şi deţinătorii de documente, aprobate de conducerea Arhivelor Naţionale prin Ordinul de zi nr. 217 din 23 mai 1996.

Etapa 1 va cuprinde următoarele activităţi:

Activitatea 1. Preluarea documentelor de la Beneficiar

Documentele, organizate in bibliorafturi/dosare/pachete, vor fi preluate de la sediul autorităţii contractante pe bază de procese verbale de predare-primire.
Această etapă consta în livrarea dosarelor de către Achizitor către Furnizor care va organiza arhiva/ dosarele în cutiile puse de către acesta la dispoziţia Achizitorului, etichetarea cutiilor cu cod de bare şi transferul arhivei la centrul de arhivă în vederea scanării, astfel:

- O echipa formată din specialişti în arhivistică (experţii dedicaţi ai Furnizorului pentru serviciile de digitizare) se va deplasa la sediul Achizitorului şi va organiza totul în cutii pentru arhivă.
- Organizarea arhivei în cutii (pentru arhivă) se efectuează după criterii bine stabilite precum(, cel puţin):
  - Departamentul creator;
  - Datele extreme.
- După introducerea documentelor în cutiile de arhivă şi semnarea PV-ului de predare primire a documentelor se procedează la încărcarea arhivei în maşinile pentru transport arhivă. Transportul se va realiza de către Furnizor prin flota proprie (minim 2 maşini) cu maşini monitorizate GPS, cu sistem de înregistrare a traseului.
- Prestatorul va transporta documentele, în spatiile special amenajate din locatiile acestuia.

În procesele verbale se va consemna, impreuna cu Beneficiarul, data preluării, tipul si numarul de bibliorafturi/dosare/pachete, alte eventuale observaţii.

Activitatea 2. Ordonarea documentelor

Dosarele cu documente preluate de către Furnizor vor fi ordonate pe structurile organizatorice ale Achizitorului, cronologic, pe probleme şi termene de păstrare. Documentele aferente proiectelor vor fi ordonate pe activităţi, constituindu-se dosarul unic al proiectului.

Activitatea 3. Constituirea unităţilor arhivistice (dosarelor)

Se scot documentele din bibliorafturi, se elimină părtile metalice (acele, agrafele capsele), filele nescrise, ciornele. Documentele ordonate se vor introduce în coperţi de carton pentru a se constitui unităţile arhivistice. Un dosar nu va avea un număr mai mare de 250 file. În cazul depăşirii acestui număr de file se vor constitui mai multe volume ale aceluiaşi dosar.

Pe copertă se vor înscrie elementele de identificare ale unităţii arhivistice:

- denumirea unitătii,
- denumirea compartimentului
- termenul de păstrare
- numărul dosarului (cota provizorie) si anul
- continutul pe scurt al unitătii arhivistice
- numărul volumului (dacă este cazul)
- datele extreme

În cazul dosarului unic al proiectului, pe copertă , în spaţiul destinat conţinutului unităţii arhivistice, se vor specifica în mod obligatoriu, pe lângă elementele menţionate mai sus, următoarele:

- denumirea programului operational
- Domeniul Major de Interventie (DMI)
- tipul de proiect (strategic/grant/asistentă tehnică)
- codul proiectului

Pe cotor se vor înscrie numărul dosarului, anul, indicativul, termenul de păstrare, număr volum (după caz).

Activitatea 4. Numerotarea filelor dosarelor

Se verifică corectitudinea numerotării filelor (daca exista). În cazul constatării existenţei unor greşeli, se renumerotează filele, iar în situaţia absenţei numerotării, operaţiunea va fi executată integral de către personalul Prestatorului.
La sfârşitul dosarului unic al proiectului, pe ultima pagină nescrisă (sau pe o foaie adaugată), se face certificarea unităţii arhivistice: „ Prezentul dosar conţine....file”, în cifre şi între paranteze în litere, după care semnează şi trece data certificării.

Activitatea 5. Operatiunea de scanare a documentelor

Scanarea documentelor aflate în fiecare dosar se va face înainte de legarea dosarelor.

Activitatea 6. Legarea unităţilor arhivistice

Înainte de legare, unităţile arhivistice vor fi verificate, astfel încât conţinutul dosarului să corespundă înscrisului de pe copertă iar ordinea documentelor în cadrul dosarului să fie cea iniţială. Se verifică, de asemenea, ordinea dosarelor în cutii (după cota definitivă a unităţii arhivistice).

Dosarele vor fi legate conform Instrucţiunilor de aplicare a Legii nr. 16/1996 republicată, în coperţi de carton, astfel încât să se asigure citirea completă a textului, datelor şi rezoluţiilor.
Operatorul economic va asigura coperţile de carton şi celelalte furnituri (sfoară, aracet şi markere specifice) necesare legării documentelor şi înscrierii datelor de identificare ale dosarului pe copertă.

Activitatea 7. Inventarierea documentelor

Inventarele întocmite vor cuprinde toate dosarele cu aceleaşi termene de păstrare create în cursul unui an de către un compartiment de muncă. La rubrica „Conţinutul pe scurt al dosarului" vor fi precizate genurile de documente pe care le conţine respectivul dosar. În cazul dosarelor formate din mai multe volume, în inventar, fiecărui volum îi va fi atribuit un număr curent distinct. Dosarele care cuprind acte din mai mulţi ani vor fi inventariate la anul de început, menţionându-se în inventar datele extreme.

La sfârşitul inventarului se va menţiona: „Acest inventar conţine .... file şi ..... unităţi arhivistice", urmate de data întocmirii şi de numele/semnătura persoanei care a întocmit inventarul.

În cazul dosarelor unice de proiect, pentru fiecare proiect se va întocmi un inventar propriu. Ordinea documentelor inventariate va respecta ordinea activitatilor derulate in cadrul proiectului.

Activitatea 8. Organizarea fondului arhivistic prelucrat şi scanat

Cutiile cu dosare vor fi numerotate în cadrul fondului şi vor fi ordonate conform criteriului de ordonare stabilit iniţial.

Activitatea 9. Predarea fondului arhivistic prelucrat si digitizat

Predarea fondului arhivistic prelucrat si digitizat catre reprezentantii Achizitorului se va face pe bază de Proces Verbal de receptie. Recepţia cantitativă şi calitativă se va efectua de către o comisie de recepţie constituită din reprezentanţi ai achizitorului şi ai furnizorului şi se va finaliza prin semnarea unui proces verbal de recepţie cantitativă-calitativă.

ETAPA 2 - Detectarea codurilor de bare şi generarea documentelor electronice PDF

În aceasta etapă se efectuează următoarele activităţi:

- Scanarea unui volum total de 10 milioane de pagini, rezultând transformarea acestora în format electronic PDF.
- Scanarea se va realiza la o rezoluţie de 200 dpi.
- Fişierele aferente documentelor se vor indexa folosindu-se cel puţin 3 metadate puse la dispoziţie de Achizitor (şi cel mult 6 metadate) per document.
- Numărul exact de metadata per tip de document precum şi atributele documentelor care se vor regăsi în metadate se va stabili împreună cu ANFP în perioada de analiză (specifică serviciilor de digitizare).
- Metadatele vor fi stocate în fişiere tip XML care vor fi importate de Furnizor în infrastructura de suport a lucrului cu fluxuri informatice (din cadrul Sistemului e-ANFP).
- Structura volumului de documente ce se vor digitiza, în funcţie de formatul acestora, este:
  - 2 % (din volumul total) sunt planşe în format > A3;
  - 98% (din volumul total) sunt documente în format <= A3, dintre care:
    - 63% pentru scanare ADF în format A4;
    - 20% pentru scanare ADF în format A3;
    - 15% pentru scanare manuală.
  - Baza de date rezultata în urma procesului de digitizare va fi realizata de către specialiştii în arhivistică; procesul presupune copierea fidela a informaţiilor de pe coperta dosarelor în sistemul de management, coroborarea cu departamentul, codul de bare al cutiei şi data estimată pentru distrugerea cutiei – dacă va fi cazul.
- Pe toată perioada procesului de scanare, cutiile vor fi depozitate într-un centru logistic special construit pentru arhivă sau într-un spaţiu special amenajat, avizat tehnic de către Arhivele Naţionale şi avizat PSI, monitorizat permanent cu camere de filmat, care

posedă sisteme de control acces, este încălzit, iar temperatura şi umiditate sunt controlate electronic.

În cazul în care pe perioada scanării sunt solicitate dosare cărora nu le-a venit încă rândul să fie scanate, se va proceda astfel:

- Solicitările pentru consultări vor fi transmise (de ANFP, în calitate de Achizitor, către Furnizor), prin intermediul unei aplicaţii on-line (implementate de către Furnizor) folosind user name şi parola alocate Achizitorului;
- Documentele fizice vor fi livrate Achizitorului la punctul de lucru indicat în ziua lucrătoare următoare solicitării la nivel de cutie sau dosar.
- Livrarea se va face cu mijloace proprii ale Furnizorului.

ETAPA 3 - Indexarea şi verificarea metadatelor
Această etapă presupune următoarele activităţi specifice:

- Constituirea indexului documentelor (pe baza metadatelor extrase sau introduce);
- Verificarea metadatelor de către o echipă de specialişti de la Furnizor compusă din minim 12 persoane.

Notă: În cazul în care şase metadata sunt insuficiente pentru un tip de document - fie că acestea nu pot asigura unicitatea unui document, fie că ANFP doreşte asignarea mai multora – revine în sarcina ANFP ca, prin forte proprii, să genereze şi să asigneze metadatele suplimentare. Furnizorul va trebui să acorde sprijin ANFP prin stabilirea procedurii de lucru şi punerea la dispoziţie a instrumentelor software necesare automatizării pe cât posibil a acestui proces.

ETAPA 4 - Importul documentelor electronice în sistemul electronic de management al documentelor
Această etapă presupune următoarele activităţi specifice:

- După finalizarea procesului de scanare, cutiile cu dosarele scanate se vor expedia la Achizitor şi se vor aşeza pe rafturile pregătite în avans.
- Predarea tuturor cutiilor trebuie să poată fi efectuată în maxim 15 zile lucrătoare, şi, din aceste considerente, Furnizorul trebuie să deţină competenţe specializate de organizarea a arhivei proprii, adică echipamente specializate tip ”order picker” şi personal calificat în exploatarea acestora. Oder picker-ul este un echipament specializat pentru operaţiuni de picking (luat de pe raft si pus pe raft unităţi mici de produse, respectiv cutii de arhiva sau dosare). Funcţionează cu operator uman, este controlat prin fir magnetic intre rafturi si un scanner heavy-duty care asigură conexiunea wireless permanentă a operatorului cu sistemul de management al înregistrărilor, permiţându-i să localizeze cutiile pe raft (rafturile si cutiile având etichete cod de bare), să extragă cutii sau dosare, să aşeze cutii noi pe raft sau să pună la loc retururi.
- Se vor eticheta toate rafturile cu coduri de bare şi se va face legătura conţinut cutie - cod de bare cutie – adresa raft. Acest mod de organizare va permite accesarea foarte facilă a dosarelor necesare din arhiva fizica doar consultând o baza de date electronică. Tot în această etapă se realizează de către furnizor şi exportul fişierelor scanate şi a metadatelor indexate în repository.

4.1.1.2 Procesul de Scanare

Etapele fluxului procesului de scanare utilizat în cadrul serviciilor de digitizare sunt evidenţiate în figura de mai jos:

LEGENDA:

Transport
Manipularea internă a documentelor
Procese informaţionale (procesare digitala)

Mai jos sunt detaliate activităţile specifice de etapă:

Etapa 1 – Pregătirea documentelor

- Scoaterea din cutii, bibliorafturi, dosare, etc.;
- Eliminarea capselor, boldurilor, etc.;
- Verificarea colilor pentru îndreptarea colţurilor îndoite;
- Inserarea unor pagini interne cu barcode-uri (documentele vor rămâne în forma iniţială, nici un barcode nu va fi aplicat pe documentele ANFP), cu rol de delimitare a dosarelor.

Etapa 2 – Scanarea documentelor

- Scanarea documentelor la rezoluţia solicitată, în formatul solicitat şi cu compresia stabilită;
- Scanarea se face folosind scannere industriale ce folosesc senzori cu infrasunet pentru a elimina tragerea multipla a colilor în procesul de scanare.

Etapa 3 – Detectarea barcode-urilor

- Toate paginile scanate sunt procesate pentru identificarea barcode-urilor;
- Pentru acest pas este recomandată folosirea a doua componente software independente de recunoaştere a barcode-urilor pentru reducerea numărului paginilor nedetectate;

- Toate paginile de garda cu barcode-uri vor avea mai multe barcode-uri de format 1D si 2D pentru minimizarea la 0,001% a procentului paginilor nedetectate.

Etapa 4 – Generarea fişierelor tip PDF

- Cu informaţiile provenite din valorile barcode-urilor din faza 4 se vor genera documentele tip PDF;
- Toate informaţiile de care e nevoie pentru a genera numele fişierelor provenite din faza 4 sunt stocate pentru utilizarea ulterioara;

Etapa 5 – Indexarea nr. 1 a metadatelor

- In aplicaţii dedicate, fiecărui document electronic generat i se atribuie metadatele cerute de către client.

Etapa 6 – Indexarea nr. 2 a metadatelor

- Reatribuirea metadatelor pentru fiecare document in parte pentru a minimiza erorile de introducere.

Etapa 7 – Verificarea metadatelor

- Pentru documentele la care diferă metadatele introduse la paşii 6 si 7, acestea se vor verifica manual de către operatori pentru a micşora spre 0% erorile de introducere a metadatelor.

Etapa 8 – Generarea numelor fişierelor

- Folosind metadatele, se vor genera numele fişierelor.

Etapa 9 – Backup documente

- O copie de siguranţă a documentelor procesate se va păstra în permanenţă pe un hard-disk extern sistemului pe care se face procesarea documentelor; această copie se va transmite periodic Achizitorului prin intermediul unui serviciu ftp securizat.

Etapa 10 – exportul documentelor şi metadatelor

- Toate documentele împreună cu metadatele de identificare sunt importate în infrastructura de suport a lucrului cu fluxuri informatice.

4.1.1.3 Securitatea Informaţiei

Furnizorul serviciilor de digitizare va îndeplini următoarele cerinţe de securitate a informaţiei:

- Întreaga reţea de curent a echipamentelor implicate în derularea procesului de scanare a documentelor (staţiile de lucru, scannerele, echipamentele active de reţea, servere, etc.) trebuie să asigure continuitatea în funcţionalitatea sistemului în caz de avarii majore la reţeaua electrică.
- Procedurile interne pentru toate procesele tipice activităţii de scanare a documentelor (pregătirea documentelor, scanarea documentelor, procesarea imaginilor, indexarea şi verificarea imaginilor şi criteriilor de căutare, reconstituirea documentelor) nu trebuie să permită pierderea sau rătăcirea documentelor fizice şi electronice.
- Preluarea şi predarea documentelor de la şi către Achizitor se va face pe bază de procese verbale în care se specifică întreaga cantitate de documente preluată/predată asigurând integritatea arhivei scanate.
- Pentru procesul de scanare se va folosi un sistem electronic client-server. Serverul trebuie să aibă disk-urile instalate în sistem RAID-1 sau compliant, pentru asigurarea

integrităţii documentelor electronice în cazul în care unul dintre ele cedează, cât şi un "spare disk" pentru regenerarea în mod automat a matricelor RAID-1.

- Reţeaua internă a staţiilor de lucru care efectuează procesul de scanare trebuie să aibă acces la reţeaua Internet. De asemenea, trebuie ca porturile USB să fie dezactivate, să nu aibă unităţi optice instalate şi să fie prevăzute cu software de audit (înregistrarea tuturor activităţilor ce se desfăşoară pe acestea).

4.1.1.4 Alte Cerinţe

Furnizorul serviciilor de digitizare va trebui să posede următoarele certificări:

- Certificări ISO deţinute: ISO 9001, 14001, 27001, 20000-1 sau echivalent;
- Certificări pentru experţii în arhivistică conform fişei de date;
- Certificări pentru sistemul informatic necesar procesului de digitizare a documentelor.

Totodată, Furnizorul serviciilor de digitizare va trebui să posede următoarele echipamente, menite să asigure nivelele de protecţie împotriva incendiilor şi securitate, conform legislaţiei în vigoare, precum şi depozitare in centrul logistic special construit pentru arhiva sau în spaţiu special amenajat în conformitate cu legislaţia în vigoare. :

- mijloace, instalaţii şi sisteme de prevenire şi stingere a incendiilor conform prevederilor legale în domeniu;
- Termohigrometru pentru conformitatea temperaturii şi umidităţii măsurate în cel puţin 2 puncte din depozit;
- Spaţiu minim necesar depozit de cel puţin 7000 de cutii de arhivare
- Sistem supraveghere video cu circuit închis cu vizualizarea tuturor spatiilor de acces si a spaţiilor dimprejurul clădirii;
- Senzori de mişcare si de contact pe toate uşile de acces;
- Sistem de control acces cu carduri de acces pe toate uşile exterioare sau cele spre depozit;
- Servere de procesare şi de stocare a datelor în reţea locate într-un data center pentru protecţia informaţiilor ş i capabilităţi de "Disaster Recovery".

4.1.2 Implementare Sistem Informatic Managerial e-ANFP

Etape

Implementarea Sistemului Informatic Managerial e-ANFP presupune următoarele etape:

- Analiză (se va prevede în calendarul de proiect al ofertei o perioadă de minim 15 zile pentru obţinerea acceptanţei de etapă din partea Achizitorului);
- Proiectare;
- Dezvoltare (în cadrul componentelor Sistemului e-ANFP);
- Instruire (utilizatori şi personal administrative ANFP);
- Testare:
  - Unitară;
  - Integrată (în vederea acceptanţei din partea ANFP – se va prevede în calendarul de proiect al ofertei o perioadă de cel puţin 30 zile aferentă activităţii de testare efectuată de utilizatorii Achizitorului).
- Instalare (în mediul de producţie);
- Încărcare cu informaţii de lucru necesare (ex.: date şi documente rezultate în urma digitizării arhivei);
- Perioadă de pilotare
  Asistenţă tehnică acordată în timp real pe toată durata proiectului, timpul de raspuns fiind de maxim 1 ora

Volumetrie

Aşa cum reiese din descrierile din cap. 2.1 – ”Obiective” şi cap. 3.1.1 – ”Lucrul cu fluxuri Informatice”, Sistemul e-ANFP include o Infrastructură de susţinere a lucrului pe bază de fluxuri utilizând documente (cerinţe detaliate regăsindu-se în cap. 4.2 – ”Infrastructură de susţinere a Lucrului cu Fluxuri Informatice” din prezentul document). Pentru dimensionarea corectă a serviciilor de implementare aferente acestei Infrastructuri de Fluxuri Informatice se vor avea în vedere următoarele considerente:

- Număr actual de Direcţii/Departamente din ANFP: 13.
- Număr (maximal) de tipuri de documente (distincte la nivel ANFP): 175.
- Număr (maximal) de fluxuri de lucru (distincte la nivel ANFP): 125.
- Număr (mediu) de actori pe fluxurile de lucru (la nivel ANFP): 10.

În tabelul de mai jos sunt evidenţiate următorii indicatori volumetrici (per Direcţie/Departament):

Nr.	**Nume Direcţie / Departament**	**Număr (total) de tipuri de documente**	**Număr (total) de fluxuri**	**Număr de actori (per flux)**	**Număr de paşi (per flux)**	**Număr de documente procesate lunar**	**Număr mediu de pagini (per document procesat)**
1	Direcţia generală managementul funcţiei publice	30	20	12	16	2500	45
2	Direcţia gestionarea procedurilor administrative						
3	Direcţia evidenţa, monitorizarea şi controlul salarizării						
4	Direcţia generală reglementare, monitorizare şi contencios	47	41	19	34	603	93
5	Direcţia comunicare şi relaţii internaţionale	45	15	5	10	150	2
6	Direcţia coordonare centre regionale, evaluare şi perfecţionare profesională	30	15	4	6	100	30
7	Direcţia economic, resurse umane, achiziţii, administrativ şi protocol	100	80	20	10	10.000	10
8	Direcţia programe cu finanţare	20	8	5	3	1000	10

Nr.	Nume Direcţie / Departament	Număr (total) de tipuri de documente	Număr (total) de fluxuri	Număr de actori (per flux)	Număr de paşi (per flux)	Număr de documente procesate lunar	Număr mediu de pagini (per document procesat)
	externă						
9	Compartiment audit public intern	21	3	3	3	11	4
10	Corp control	20	12	6	10	25	5
11	Serviciul Tehnologia Informaţiei	20	10	5	7	30	2

Notă: Tipurile de documente, precum şi fluxurile/numărul de actori/numărul de paşi asociate prezente în tabelul de mai sus nu sunt distincte la nivel organizaţional (ANFP), ci indică participarea/implicarea fiecărei Direcţii/Departament la volumetria (tipuri documente/fluxuri/etc.) totală a Instituţiei (Achizitore). Practic, se evidenţiază astfel în cate din fluxurile distincte la nivel ANFP e prezentă o Direcţie/Departament.

Raportare
Se va avea în vedere crearea şi implementarea (activităţi ce se vor reflecta în calendarul de proiect al ofertei) unui număr (maximal) de 75 de rapoarte (la nivel ANFP) - respectiv 60 pentru utilizatori şi 15 pentru personalul de management - aferente Infrastructurii de Fluxuri Informatice.

Notă: Detalii suplimentare informaţiilor volumetrice din acest sub-capitol fac obiectul etapei de analiză din cadrul implementării proiectului.

4.1.3 Amenajare cameră pentru servere

4.1.3.1 Considerente generale
Ţinând cont de echipamentele existente şi a celor ce vor fi instalate prin implementarea Sistemului e-ANFP, Furnizorul va efectua întâi evaluarea spaţiului, a necesarului răcire şi de alimentare cu energie precum şi infrastructura de cablare pentru efectuarea serviciilor de amenajare a camerei serverelor ANFP (locaţia acestuia se va comunica Ofertantului câştigător în timpul implementării proiectului, la o data la care nu va afecta buna desfăşurare a activităţilor proiectului).
Suprafaţa utila a camerei serverelor este de 50 mp.
Serviciile de amenajare a camerei serverelor se vor desfăşura începând cu **luna a 3 a** contractului şi va face obiectul în Ofertă a unui calendar de implementare separat şi nu va depăşi **luna a 6 a contractului**. Aceste servicii constau în livrarea şi implementarea (instalarea, configurarea, testarea) tuturor echipamentelor (şi componentelor software aferente) descrise în sub-capitolele următoare.
Serviciile de amenajare a camerei serverelor vor fi realizate cu respectarea specificaţiilor şi standardelor din Legea nr. 135/2007 (r1) privind arhivarea documentelor în formă electronică şi din Ordinul nr. 489/2009 privind normele metodologice de autorizare a centrelor de date.
După finalizarea serviciilor de amenajare a camerei pentru servere este nevoie ca echipamentele tip server din actuala camera a serverelor a ANFP (Sediul Central şi cel secundar) - respectiv servere de procesare şi/sau baze de date, soluţii de stocare externă, echipamente de reţelistică, cabinete (rack-uri), echipamente UPS, alte echipamente – să fie mutate (transportate) la noua

locaţie (notă: în total este vorba de 6 cabinete integral echipate). Astfel, oferta va conţine toate costurile asociate lor de tip server.

4.1.3.2 Finisaje interioare

Finisajele interioare trebuie să aibă un design tehnic aspectuos, să nu fie generator de praf şi să fie uşor de întreţinut şi curăţat.

Termoizolaţia

Termoizolaţia pereţilor trebuie să îndeplinească următoarele condiţii:

- coeficientul de conductivitate termica mai mic sau egal cu 0,022 W/mK.
- clasa de combustibilitate este minim C1.

Pardoseala

Finisarea şi tratarea podelei se va face cu vopsea sau şapă autonivelantă, ambele pe bază de răşini epoxidice. După efectuarea lucrărilor, pardoseala trebuie să aibă următoarele proprietăţi:

- trebuie să fie rezistentă la acţiunea substanţelor chimice – acizi diluaţi, substanţe alcaline, săruri, uleiuri, carburanţi;
- să aibă proprietăţi antistatice, sor de întreţinut;
- rezistenta la compresiune de minim 95 N/mm^2;
- rezistenta la rupere de minim 40 N/mm^2.

Iluminatul

Se va implementa un sistem de iluminare care sa ofere condiţii de lucru, conforme cu normele in vigoare, pentru spatii tehnice unde sunt executate sarcini vizuale impuse (tehnica de calcul, măsurători precise, etc.), în limita a 500-1000 lucşi măsuraţi în orice punct al încăperii aflat într-un plan orizontal la aproximativ 1500 mm înălţime de la podea. Se vor instala minim 8 lămpi 2x36 W cu tuburi fluorescente.

Spaţiu Rack-uri

Camera serverelor va permite instalarea a 8 rack-uri ce vor avea următoarele dimensiuni maximale:

- Înălţime: 42U;
- Lăţime: 800mm;
- Adâncime 1200mm.

Rack-urile vor fi instalate folosindu-se si o soluţie de protecţie antiseismică:

- Fixarea rackurilor in beton se va face cu bolţuri sau tije filetate de minim 10 mm.
- Fixarea mecanica a rackurilor intre ele pentru reducerea problemelor în caz de seism.

Alte Considerente

- se va prevede o soluţie de aşezare a rackurilor care sa ofere spaţiu de lucru de minim 1000 mm atât in fata cat si in spatele rackurilor;
- uşa de acces la camera serverelor va avea dimensiuni minime de 900 x 2000 mm şi va avea rezistenţă la foc de minim 60 minute;
- se va prevede o soluţie de poziţionare a echipamentelor, trasee electrice şi de date şi direcţionare a fluxurilor de aer fără podea supraînălţată;
- cablurile de date si cele electrice vor fi protejate in jgheaburi metalice orizontale etajate pe verticala, astfel încât cablurile electrice, de date/cupru si de date/Fibră Optică sa fie complet separate fizic unele de altele;

- suporturile cablurilor de date vor fi dimensionate astfel încât să permită cablarea orizontală a minim 500 cabluri UTP şi a minim 2000 patch-corduri de Fibră Optică de 2 mm.

4.1.3.3 Climatizare (Răcire)

Caracteristici generale

O soluţie de răcire adecvată devine imperativă în cazul creşterii densităţii echipamentelor din camera serverelor, astfel ca se va prevede un sistem de climatizare care va îndeplini următoarele cerinţe:

- Sistemul de climatizare trebuie să realizeze în mod continuu răcirea tuturor echipamentelor din camera serverelor furnizând un flux de aer cu temperatura menţinută în intervalul 17-25 grade Celsius înainte de admisia în rackuri, pentru sarcina IT, sau în celelalte echipamente care necesită răcire, cum ar fi: echipamente UPS şi baterii, sisteme de securitate, etc.
- Sistemul de climatizare va fi proiectat cu o redundanta minima de N+1 în configuraţie 3x30 KVA.
- Puterea de răcire nominală a unităţilor interioare de climatizare va fi de maxim 15 KW.
- Puterea de răcire nominala furnizata de sistemul de climatizare trebuie sa fie de minim 1 KW răcire per 1 KVA IT si maxim 1,2 KW răcire per 1 KVA IT.

Caracteristici specifice echipamente climatizare

- Debitul de aer furnizat pentru răcirea echipamentelor IT:
  - minim185 cfm/KVA IT în funcţionare normal - cu redundanta N+1;
  - minim 140 cfm/KVA IT în avarie - fără redundanta.
- Indice EER de minim 3 KVA putere IT per KW electric de răcire.
- Tip compresor: INVERTER DC SCROLL sau echivalent.
- Interval de temperaturi pentru funcţionarea normală a unităţii exterioare de climatizare: intre -15 si +45 grade Celsius.
- Refrigerant – de tip R410A.

Separare fluxuri de aer

Se va prevede un sistem de containerizare a fluxurilor de aer rece, respectiv cald, în vederea eficientizării consumului de energie electrica a întregii camera a serverelor. Containerizarea se va face in sistemul insula caldă/insulă rece avându-se în vedere un coeficient de conductivitate termică al separaţiei de maxim 0,022 W/mK.

Evacuare apa condens

Unităţile interioare de climatizare vor fi prevăzute cu un sistem de protecţie suplimentar împotriva scurgerilor accidentale de apă de condens şi cu sistem de evacuare automată a apei de condens în afara incintei camerei serverelor. Se va indica sistemul de protecţie propus.

4.1.3.4 Alimentarea cu energie electrică

Alimentarea cu energie electrică este una dintre cele mai importante componente ale unei camere pentru servere, astfel că se doreşte o soluţie pentru asigurarea electroalimentării camerei serverelor a ANFP. Se vor avea în vedere toate echipamentele electrice, materialele auxiliare şi consumabilele necesare efectuării lucrărilor - prezentate mai jos - pentru această componentă.

Echipamentul tip UPS :

Se va prevede un echipament UPS care să îndeplinească următoarele cerinţe:

- Alimentarea cu energie electrica a echipamentelor IT se va face prin intermediul UPS-urilor în configuraţie cu redundanta minim N+1.
- Puterea minimă furnizată de sistemul UPS va fi de minim 42 KVA.
- Încărcarea maxima per UPS in regim de avarie - fără redundanta – de 70 la suta.
- Autonomie de minim 7 minute la 100% din puterea nominala IT (minim 42 KVA).
- Intrare/ieşire trifazată, online dublă conversie.
- Distorsiunea curentului de intrare: maxim 3%.
- Factor de putere la intrare: 0,99%.
- Toleranţa frecvenţei de intrare: 40-70 Hz.
- Factor de putere pe ieşire: minim 0,9.
- Tensiune la ieşire: selectabila intre 380-410 V.
- Frecvenţa la ieşire: 50 Hz.
- Stabilitatea frecventei in timpul funcţionării pe baterii: maxim 0,01%.
- Distorsiunea tensiunii la ieşire: maxim 1% pentru sarcini liniare, maxim 3 la sută pentru sarcini neliniare.
- Suprasarcina la factor de putere de 0,8:
  - minim 110% pentru timp nelimitat,
  - minim 150% pentru 1 minut.

Grup electrogen:

Se va prevede un grup electrogen care să îndeplinească următoarele cerinţe:

- Putere variabila PRP: minim 90 KVA.
- Tensiune de ieşire trifazata, 400 V, 50 Hz.
- Motor: diesel.
- Consum maxim de combustibil: 23 l/h la 100% PRP si 18 l/h la 75% PRP.
- Regulator de tensiune electronic: da.
- Suprasarcina admisa: 110% pentru 1 oră la fiecare 14 ore de funcţionare continuă.
- Autonomie: minim 50 de ore la 75% PRP minim impus, fără realimentare cu combustibil.
- Nivel de zgomot, măsurat la 7 m: maxim 75 dbA.
- Panou electronic cu afişaj digital pentru monitorizare, măsurare şi comandă: da.
- Port de comunicaţie în vederea monitorizării de la distanţă: da.

Distribuţie electrică:

Se va prevede un tablou electric care să îndeplinească următoarele cerinţe:

- Tabloul electric general va permite separarea fizică atât pe intrare cât şi pe ieşire pentru fiecare echipament UPS din configuraţia propusă, respectiv operaţiuni de mentenanţă la nivelul echipamentelor UPS fără întreruperea alimentarii sarcinii IT.
- Tabloul electric va furniza alimentarea separata a tuturor echipamentelor de climatizare sau auxiliare (iluminat, prize suplimentare, etc.) din circuite neprotejate de UPS.
- Vor fi furnizate 2 linii de alimentare de joasa tensiune (230 V/16 A) cu cate 3 faze la nivel de rack pe fiecare dintre linii, pentru fiecare din cele 8 rackuri (*Observaţie: suplimentar faţă de rack-ul de tip A inclus în proiect şi care va fi poziţionat în camera serverelor, Furnizorul va reloca aici cele 7 rack-uri cu echipamente aflate în uz la Achizitor*).
- Se vor prevede circuite de alimentare protejate de UPS pentru sarcina IT şi pentru echipamentele de monitorizare şi securitate prevăzute prin proiect.

- Se vor prevede cel puţin doua circuite trifazate de rezerva de 3x32 A protejate de UPS, în afara celor cerute mai sus.
- Se vor prevede cel puţin încă doua circuite trifazate 3 x 32 A neprotejate de UPS, în afara celor prevăzute mai sus.

Se vor prevede *cabluri electrice* care să îndeplinească următoarele cerinţe:

- Branşamentul general (din tabloul general al clădirii) şi cel de rezerva (corespunzător alimentarii de rezerva-grup electrogen) vor fi asigurate cu cablu de Cupru, cu armătura de protecţie
- Cablurile de distribuţie la nivel de rack vor fi din Cupru, conforme cu SR CEI 60228 sau echivalent, vor suporta minim 32 A per faza la 30 grade Celsius, temperatura maxima admisa pe cablu de va fi de minim 70 grade Celsius, cu rezistenta la foc conform SR CEI 60332-3 sau echivalent.

Se vor prevede prize pentru rack care să îndeplinească următoarele cerinţe:

- cele doua linii de alimentare vor fi furnizate prin intermediul unor prize industriale cu 5 poli (3P+N+PE) de 16 A, conform IEC/EN 60309 sau echivalent.

Automatizare cuplare alimentare de rezerva

Se va avea în vedere un sistem de cuplare automata a alimentarii de rezerva care să permită comutarea unei sarcini electrice de 100 KVA în maxim 30 secunde intre branşamentul principal si cel de rezerva, fără riscul cuplării simultane a celor doua branşamente.

4.1.3.5 Sisteme de securitate si monitorizare

În privinţa sistemelor de securitate şi monitorizare se vor îndeplini următoarele cerinţe:

Detecţie şi stingere de incendiu:

Se vor prevede următoarele echipamente de detecţie şi stingere incendiu care să îndeplinească următoarele cerinţe:

- Centrala de incendiu:
  - Se va permite separarea zonelor de avertizare, cel puţin două, corespunzătoare insulei reci respectiv calde.
  - Se vor monitoriza atât numărul minim de senzori de incendiu prevăzuţi prin proiect conform normativelor, cât şi a unui număr de cel puţin 4 senzori de apa care vor fi prevăzuţi pentru detectarea eventualelor scurgeri de apa din camera serverelor.
  - Se vor prevede cel puţin 2 ieşiri de minim 1 A necesare cuplării sirenelor de supraveghere.
  - Se vor prevede ieşiri de alarma si defect prin relee libere de tensiune.
  - Se va prevede port de comunicaţie prin Ethernet.
- Senzori de incendiu:
  - Detectorii de incendiu vor fi de tip dual fum/temperatură.
  - Se vor prevede detectori cu sensibilitatea de detecţie programabilă prin intermediul unei componente software pentru evitarea alarmelor false.
  - Detectorii vor fi prevăzuţi cu indicator luminos (LED) şi sistem antifurt.
- Alte considerente legate de detective:
  - Va exista buton de panică punctual resetabil cu indicator de stare.
  - Va exista sirena adresabilă cu flash, de interior, având minim 80 dbA.
  - Va exista un apelator telefonic GSM care să permită comunicarea alarmelor de incendiu în timp real.
- Sistem de stingere de incendiu:
  - Sistemul de stingere incendiu se va realiza pe baza de INERGEN.

- Sistemul de stingere incendiu va putea fi acţionat automat prin intermediul centralei de detecţie sau manual, în caz de necesitate.
- Instalaţie de desfumare:
  - Se va prevede un sistem de desfumare care să permită evacuarea aerului contaminat şi înlocuirea cu aer proaspăt din întreaga camera în maxim 15 minute.
  - Se vor prevede clapete antifoc necesare izolării automate a compartimentelor contra incendiilor.

Sistem de control acces

Se va prevede un controlor acces (împreună cu reperele adiacente de mai jos) care să îndeplinească următoarele cerinţe:

- Controlor acces:
  - Să permită controlul a cel puţin o uşă în ambele sensuri (intrare/ieşire).
  - Să poată înrola cel puţin 200 de cartele individuale.
  - Să permită înregistrarea a cel puţin 100 programe orare de acces.
  - Să permită memorarea a cel puţin 2000 de evenimente.
  - Să accepte comunicaţie pe standardele RS-232 si RS-485 sau compliante cu acestea.
  - Alimentarea cu energie electrica să fie protejată suplimentar cu baterie reîncărcabilă.
  - Să permită acţionarea dispozitivelor de blocare electromagnetica a uşii.
  - Să dispună de minim 2 porturi pentru cititoare de acces.
  - Să poată funcţiona şi în lipsa comunicaţiei cu componenta software de gestiune.
  - Să accepte module de extensie pentru cel puţin 6 uşi simplu sens.
- Cititoare de proximitate cu cartel:
  - Pentru ieşire se va prevede un cititor de proximitate care sa suporte standarde intre 26 si 128 de biţi WIEGAND în tehnologie 125 kHz RFID sau compliante cu acestea.
  - Pentru ieşire se va instala un buton (acţionabil manual)
  - Distanţa maximă de citire acceptată să fie de minim 10 cm.
  - Se va prevede (şi) un buton de evacuare în caz de urgenţă.
- Dispozitiv blocare uşă:
  - Se va prevede un dispozitiv de blocare a uşii electromagnetic, cu suport pentru cel puţin 250 kg forţă.
- Management control acces:
  - Se va prevede un calculator de management al sistemului de control acces care să includă sistem de operare, monitor, mouse, tastatură, componentă software de management.
  - Să permită managementul vizitatorilor, înrolare/blocare cartel şi crearea nivelelor de acces.
  - Să permită înrolarea a minim 500 cartele individuale.
  - Să permită controlul a cel puţin 8 uşi simplu sens .
  - Să permită comunicaţia serială şi TCP-IP.
  - Să integreze echipamentul DVR (ofertat).

Detecţie de inundaţie

Se vor prevede sub unităţile interioare de climatizare senzori de inundaţie care să permită alarmarea în caz de scurgeri accidentale de apă şi care să poată fi cuplaţi la centrala de detecţie incendiu.

Monitorizare video

Se va prevede un sistem de monitorizare video tip CCTV sau echivalent care să îndeplinească următoarele cerinţe:

- sistemul trebuie să permită vizionarea atât în timp real, cât şi sub forma de înregistrări atât a interiorului camerei serverelor (rack-uri, UPS-uri, etc.), cât şi a echipamentelor aflate la exterior (grup electrogen, unităţi exterioare de climatizare, etc.).
- Sistemul trebuie să include un echipament DVR (videorecorder) cu următoarele caracteristici minimale:
  - Minim 8 intrări video;
  - Minim 200 FPS afişare/înregistrare;
  - Posibilitate de înregistrare la detecţie mişcare;
  - Posibilitate de orar programabil sau continuu;
  - Rezoluţie de vizionare: minim 704x576 in timp real, 25 FPS per canal;
  - Să permită instalarea unui hard disk de minim 4000 Gb, interfaţa SATA;
  - Posibilitate de zoom digital minim 10x pe înregistrări;
  - Porturi (minim): RS-485 PTZ, 2 x USB, Ethernet;
  - Porturi video (minim) : HDMI, VGA, video complex (active simultan pe 3 monitoare);
  - Protocoale internet/reţea (minim): HTTP, IPv4/IPv6, TCP/IP, UPNP, RTSP, UDP, SMTP, NTP, DHCP, DNS, PPPOE, DDNS, FTP, IP Filter.

Se va prevede camera de interior care să îndeplinească următoarele cerinţe:

- La interior vor fi prevăzute minim 4 camere video, in funcţie de modul de amplasare a echipamentelor, dispunând de următoarele capabilităţi tehnice:
  - Senzor CMOS minim 1/3Rezolutie video de minim 700p;
  - Iluminare minima 0,1 lux IR off, 0 lux IR on;
  - Posibilitate de filmare IR, iluminator IR, comutator automat filmare zi/noapte.

Se vor prevede camere de exterior care îndeplinească următoarele cerinţe:

- Va fi prevăzută minim o cameră care să poată viziona în condiţii de siguranţă echipamentele amplasate la exterior, dispunând de următoarele capabilităţi tehnice:
  - Senzor CMOS minim 1/3Rezolutie video de minim 700p;
  - Iluminare minima 0,1 lux IR off, 0 lux IR on;
  - Posibilitate de filmare IR, iluminator IR, comutator automat filmare zi/noapte;
  - Iluminator IR propriu care să permită filmarea pe timp de noapte până la o distanţă de minim 10 m;
  - Lentila cu reglaj manual extern pentru focalizare şi zoom.

Monitorizare parametrii

În privinţa monitorizării parametrilor de funcţionare a (principalelor) echipamente din camera serverelor se vor avea în vedere următoarele considerente:

- Mărimi electrice:
  - Se va monitoriza funcţionarea UPS-urilor şi a grupului electrogen.
  - De asemenea se va prevede posibilitatea monitorizării de la distanţă a tuturor circuitelor electrice la nivel de faza pentru toate rackurile şi echipamentele de climatizare, urmărindu-se în timp real principalii parametri electrici – tensiune, intensitatea curentului, putere activa, frecvenţa.
  - Monitorizarea parametrilor electrici amintiţi mai sus se va realiza cu ajutorul transformatoarelor de curent splitcore, astfel încât să poată fi înlocuite în caz de defectare fără întreruperea alimentării circuitelor monitorizate

- Climatizare:

    - Va fi implementată monitorizarea de la distanţă şi înregistrarea temperaturilor de intrare respectiv de ieşire in/din fiecare rack şi a temperaturilor de intrare şi de ieşire in/din unităţile interioare de climatizare.
    - Temperaturile de intrare şi ieşire din rack vor fi măsurate la înălţimea de un metru a uşilor din fata si spatele rackurilor, la exterior.
- Securitate:
    - Centralele de detecţie de incendiu si de control acces vor fi prevăzute cu posibilitatea înregistrării si arhivarii evenimentelor.

Serviciile de amenajare a Data Center vor avea în vedere respectarea minim a prevederilor Ordinului Ministrului Comunicaţiilor şi Societăţii Informaţionale nr. 489/2009 privind normele metodologice de autorizare a centrelor de date, cu modificările şi completările ulterioare, astfel încât la finalul lucrărilor Achizitorul să demareze activitatea de autorizare a Data Center-ului în condiţiile legislaţiei în vigoare.

4.1.3.6 Servicii amenajare camera backup (altă locaţie decât locaţia Data Center-ului)

Se vor prevede servicii de amenajare a camerei (serverelor) pentru backup pentru care se va ţine cont de următoarele considerente:

- Locaţie:
    - Maxim 400 km de Bucureşti, la unul din sediile teritoriale ale Achizitorului (adresa se va comunica Ofertantului Câştigător în debutul etapei de analiză a implementării proiectului).
- Suprafaţa:
    - 8 mp.
- Detalii servicii:
    - Livrare si montare senzori de căldura/fum/mişcare + camera IP, corespunzător spaţiului;
    - Servicii de transport, montare şi asigurarea funcţionalităţii sistemului de climatizare corespunzător spaţiului care vor fi puse la dispoziţie de Achizitor;
    - Servicii de transport şi montare echipamentelor IT puse la dispoziţie de Achizitor;
    - Integrare cu sistemul de monitorizare al Camerei pentru Servere.

4.1.4 Implementare semnătură electronică (calificată)

Se vor include servicii de livrare şi implementare a 2000 unităţi de semnare electronica compuse dintr-un dispozitiv criptografic tip token si un certificat digital calificat, unităţi ce vor fi livrate împreună cu componenta software aferentă de semnare a documentelor inclusiv manual de utilizare aferent.
Caracteristicile tehnice minimale pentru unităţi şi componente software sunt următoarele:

- **Certificat Digital Calificat** cu valabilitate de minim 1 an de la data emiterii, conţinând Semnătura Electronică Extinsă, care:
    - Asigură integritatea şi confidenţialitatea documentelor transmise electronic;
    - Permite autentificarea la diverse aplicaţii şi garantează identitatea persoanei în sensul Legii nr. 455/2001 privind semnătura electronica şi a HG nr.1259/2001 privind aprobarea Normelor tehnice şi metodologice de aplicare, cu modificările şi completările ulterioare,
    - Este emis de un furnizor acreditat de servicii de certificare calificată.
- **Dispozitiv Criptografic**, de tip token, după cum urmează:
    - Dispune de protecţie software şi hardware împotriva atacurilor criptografice;
    - Sisteme de operare suportate (minim): Windows Server 2008/2012 , Windows XP/Vista7/8 , Mac OS X, Linux;

- API-uri şi standarde suportate (minim): PKCS # 11 v2.01 , Microsoft CAPI , PC / SC , X.509 v3 depozitare certificat , SSL v3 , IPsec / IKE, ISO 7816-1 / ISO 7816-2 / ISO 7816-3 / ISO 7816-4, X7 IP - IEC 529;
- Memorie internă: minim 72K;
- Algoritmi criptografici suportaţi (minim): RSA 1024 - bit / 2048 - bit , DES , 3DES , SHA1 , ECC p.256/p.394;
- Certificări de securitate suportate (minim): FIPS 140-2 L2 & 3, Common Criteria EAL4/EAL5,
  Common Criteria EAL4 +;
- Conectivitate: USB 1.1 si 2.0;
- Retenţie date in memorie: minim 10 ani;
- Rescriere a celulelor memoriei: minim 500.000 ori.

- **Componenta (software) de semnare** a oricărui tip de documente/aplicaţie pentru semnare electronică.

4.1.5 Implementarea arhivei electronice la nivelul ANFP

Implementarea arhivei electronice în sensul Legii nr. 135/2007 la nivelul ANFP va fi constituită din maxim 60.000 documente existente în ANFP care îndeplinesc condiţiile cerute de legislaţia în domeniu cu privire la arhivarea electronică.

Documentele semnate cu semnătura electronică extinsă începând cu luna octombrie 2010 vor fi predate Prestatorului în vederea gestionării şi constituirii arhivei electronice de către Prestator pe perioada contractului, urmând ca şi arhiva electronică constituită să fie predată către ANFP în ultima lună de contract.

Sistemul va asigura lucrul cu două arhive de documente, prima arhivă fiind aferentă unei zone tampon dedicate stocării documentelor electronice care nu vor fi semnate electronic (în cadrul serviciilor de analiză din implementarea SIM se va evidenţia şi acest caz), iar cea de-a doua fiind dedicată zonei de arhivă electronică (în sensul Legii nr. 135/2007).

Menţionăm că cele 60.000 de documente semnate electronic de către ANFP vor fi transferate – după obţinerea acreditării de către ANFP ca şi procesator de arhivă electronică – prin intermediul unui modul de transfer specializat care se va implementa în cadrul SIM (dezvoltat în prezentul proiect).

Totodată, SIM va asigura posibilitatea exportului documentelor electronice (semnate electronic) în format Word sau .pdf pentru cazul în care este nevoie şi de semnarea fizică a acestora.

Prestatorul va elabora şi livra procedurile prevăzute de legislaţia în domeniu autorizării Data Center şi autorizării ca şi administrator arhivă electronică în nume propriu către Achizitor, cel târziu în luna a 7 de contract.

Prestatorul va elabora şi implementa procedurile aferente pentru arhivarea electronică, inclusiv manual de utilizare, precum şi registrul arhivei electronice conform modelului aprobat prin Ordinul Ministrului Comunicaţiilor şi Societăţii Informaţionale nr. 493/2009.

4.1.6 Audit de securitate

Se vor include următoarele servicii de audit de securitate informatică:

Număr	Denumire	Etapă/Arie de business/Proces
1	Sesiune de audit specific ISO 27001, sau	Opening Meeting Prezentare metodologie de audit, reprezentanţi, prezentare sistem, modificări apărute.

	echivalent	
		Securitatea informaţiei - Sistemul de management al securităţii informaţiei Mod de desfăşurare: interviu, chestionar. Tematica: planuri de acţiune; controale si măsuri compensatorii (noi/existente), planuri de securitate; analiza masuri de securitate; politici si proceduri de securitate pentru sistemul analizat.
		Controlul documentelor; Controlul înregistrărilor Mod de desfăşurare: interviu, chestionar, observaţie. Proceduri documentate; Controalele necesare pentru identificare, depozitare, protecţie, recuperare, timpul de reţinere si eliminare a înregistrărilor; cerinţe relevante legale si reglementate, obligaţii contractuale
		Zona IT Mod de desfăşurare: interviu, chestionar, observaţie. Proceduri/instrucţiuni IT, evaluare securitate, desfăşurarea proceselor, roluri şi responsabilităţi, monitorizare, revizuiri periodice, managementul incidentelor de securitate
		Zona operaţional Mod de desfăşurare: interviu, chestionar, observaţie. Proceduri/instrucţiuni operaţionale, desfăşurarea proceselor, rolurile cheie, monitorizare, revizuiri periodice, managementul incidentelor, acţiuni preventive si corective
		Analiza elemente identificate, prezentare rezultate audit on site.
2	Sesiune tip ”White-box pentesting”	Teste unitare (per componentă hardware-software).
		Teste integrate (per submulţimi de component hardware-software ale Sistemului e-ANFP.

Se vor aloca în calendarul de proiect din ofertă 3 zile pentru sesiunea de audit specific ISO 27001, sau echivalent, şi 3 zile pentru sesiunea de pentest.

Notă: Mai multe detalii privind sesiunea de pentest se vor stabili de comun acord cu Ofertantul câştigător în perioada de analiză din implementarea proiectului.

4.2 Infrastructură de susţinere a lucrului cu Fluxuri Informatice

Infrastructura de fluxuri informatice va susţine dezvoltarea capacităţii de management a ANFP precum şi îmbunătăţirea comunicării (relaţionării) instituţiilor publice cu ANFP, ca agenţie centrală ce realizează managementul integrat al funcţiei publice şi al funcţionarilor publici.
Infrastructura de fluxuri informatice va include soluţii informatice (sau componente) dedicate tip COTS aparţinând aceluiaşi producător, pentru asigurarea suportului avansat de producător şi eliminarea eforturilor de integrare şi testare a (întregii) infrastructuri, pentru asigurarea zonelor de:

- Lucru cu fluxuri de documente şi captură,
- Lucru cu fluxuri de integrare şi procese de lucru,
- Administrare a utilizatorilor şi controlul accesului.

4.2.1 Fluxuri de documente şi captură

Zona de fluxuri de documente şi captură trebuie să asigure transformarea în format electronic, gestionarea şi arhivarea documentelor şi să permită dezvoltarea de aplicaţii suplimentare (pe platforma soluţiei propuse, fără utilizarea de componente tip ”third-party”), fără a impune limitări de funcţionalitate la nivelul acesteia. Această zonă se compune din următoarele soluţii informatice:

- Soluţia de management al documentelor;
- Soluţia de captură.

4.2.1.1 Caracteristici generale

Zona de fluxuri de documente şi captură trebuie să dispună de următoarele caracteristici:

- Să includă licenţele aferente pentru serverul relaţional de baze de date pentru stocarea informaţiilor, precum si a serverului de aplicaţii.
- Licenţierea se va face în funcţie de numărul utilizatorilor sub-sistemului, şi nu în funcţie de tipul şi/sau numărul de servere folosite.

4.2.1.2 Soluţia de management al documentelor

Soluţia de management al documentelor trebuie să dispună de următoarele caracteristici:

- Să ofere suport pentru procesarea electronică a documentelor, astfel încât să se obţină varianta acestora sub formă de text, permiţându-se indexarea conţinutului acestuia.
- Să permită stocarea unei game variate de conţinut în format electronic, de la imagini scanate ale documentelor pe hârtie, la documente create cu editoare de text, foi de calcul tabelar, desene CAD, fişiere video AVI, MPG, fişiere audio MP3, fişiere grafice: BMP, JPG, GIF, fişiere text: PDF, TXT, HTML. Documentele trebuie păstrate independent de sistemul de baze de date utilizat pentru a evita creşterea dimensiunii bazei de date şi îngreunarea timpului de răspuns. Astfel, în baza de date se vor păstra doar legături către documente/fişiere, alături de datele asociate specifice.
- Să pună la dispoziţia utilizatorilor toate funcţiile platformei prin intermediul unor aplicaţii web de tip ”out-of-the box”.
- Să permită adăugarea de documente electronice printr-un mecanism de tip ”drag-and-drop” in browser-ul web.
- Să ofere posibilitatea alocării de numere de înregistrare fiecărui document.
- Să permită crearea de reguli de validare la introducerea datelor.
- Să posede interfaţa în limba română.
- Să permită organizarea documentelor într-o structura ierarhică intuitivă. Această organizare ierarhică va fi prezentată într-o structură arborescentă, similară sistemelor de fişiere comune/obişnuite. Se doreşte ca documentele să poată fi organizate în structuri care să simuleze modalitatea reală de organizare în dosare şi fişete.
- Să ofere posibilitatea de organizare a documentelor pe dosare prin realizarea de legături între documentele relevante pentru un anumit domeniu comun.
- Să ofere posibilitatea stocării documentelor într-un spaţiu centralizat şi organizat şi posibilitatea de a asocia metadate pentru fiecare document în parte, cum ar fi: data creării, autor, problematică. Aceste câmpuri de date trebuie să poată fi definite de către administratorul sistemului folosind doar interfaţa grafică, fără a fi nevoie de intervenţia în codul aplicaţiei.

- Să includă un mecanism de definire la nivel administrativ a metadatelor astfel încât setul de date (administrative) să poată fi personalizat la nivel de tip de document.
- Să permită prelucrarea documentelor pe tipuri de documente şi metadate specifice acestor tipuri
- Să ofere suport pentru ciclul de viaţă al unui document (creare, validare, aprobare, publicare, arhivare).
- Să ofere posibilităţi de arhivare a documentelor.
- Stocarea documentelor trebuie să se facă într-un spaţiu centralizat şi organizat.
- Să ofere posibilitatea stocării documentelor atât intr-o baza de date relaţională, cât şi într-un sistem de fişiere.
- Să poată stoca metadatele în cel puţin următoarele sisteme de baze de date relaţionale: Oracle Database, Microsoft SQL Server, IBM DB2 sau echivalente.
- Să includă un mecanism integrat de management al versiunii documentelor (incluzând versiuni ale diverselor componente ale documentelor) cu posibilitatea revenirii în orice moment la o versiune anterioară.
- Gestiunea istoricului versiunilor să se poată face pentru fiecare document. Identificatorul de versiune al documentelor trebuie sa fie cel puţin pe doua nivele: major si minor.
- Să permită urmărirea şi trasabilitatea modificărilor efectuate pe un document.
- Să permită crearea de versiuni a documentelor la fiecare modificare făcută de către utilizatorii (care au drepturi de modificare).
- Să permită nativ versionarea documentelor prin funcţionalităţi de tip „Check In – Check Out”. Formatul de stocare al documentelor electronice trebuie să fie cel nativ, astfel se exclude păstrarea documentelor în formatul propriu sistemului de arhivare electronică, pentru a asigura recuperarea facilă a datelor în caz de defecţiune.
- Să ofere posibilităţi de căutare complexe a unui document folosind multiple criterii precum şi posibilităţi de rafinare a căutărilor (căutare în rezultatele altei căutări) şi salvarea criteriilor de căutare în vederea reutilizării lor (salvarea va fi inclusă în sistemul de securitate şi drepturi astfel încât fiecare utilizator să aibă acces doar la căutările salvate pe care are dreptul să le utilizeze)
- Să ofere un mecanism intuitiv pentru regasirea documentelor dupa datele asociate introduse de către utilizatori, comentarii ale utilizatorilor sau după cuvinte din conţinutul documentelor. Mecanismul de căutare va deţine facilităţi de rafinare a rezultatelor afişate (oferta va detalia acest aspect).
- Să permită realizarea de template-uri de interogări, în vederea regăsirii documentelor.
- Să permită salvarea rezultatelor interogărilor realizate.
- Să permită afişarea tuturor versiunilor unui document în urma realizării unei căutări.
- Să permită realizarea de căutări în conţinutul documentelor.
- Să ofere un cadru integrat de colaborare.
- Să permită integrarea cu alte sisteme informatice, astfel încât să schimbe informaţii cu acestea sub formă de documente. Aceasta funcţionalitate priveşte (şi) interogarea (la nevoie a) arhivelor de către organizaţii externe.
- Să dispună de integrare nativă cu aplicaţii Microsoft Office (in vederea asigurării compatibilizării cu sistemele utilizate în prezent de Achizitor), astfel încât să permită editarea şi/sau salvarea documentelor direct pe server, fără a părăsi aplicaţiile respective.
- Să permită declararea unui document, ca înregistrare electronica, din interfaţa Microsoft Office (in vederea asigurării compatibilizării cu sistemele utilizate în prezent de Achizitor).
- Să permită integrarea altor aplicaţii (existente sau viitoare ale ANFP, precum Portalul de Management, Aplicaţia de Management - MigBook) ce solicită lucru cu documente sau fluxuri de documente.

- Să deţină un mecanism de extindere a funcţionalităţilor şi integrare cu alte aplicaţii prin dezvoltare de cod.
- Să permită importul şi exportul definiţiilor obiectelor in formatul XML.
- Să permită transmiterea prin email a documentelor sau a unui link către documentele stocate in depozitul de documente al soluţiei (”repository”).
- Să dispună de capabilităţi de integrare cu alte aplicaţii şi/sau sisteme informatice prin intermediul serviciilor web.
- Să permită integrarea cu soluţii dedicate de management a înregistrărilor in vederea extinderii ulterioare a Sistemului Informatic aflat în scopul prezentului proiect, prezentându-se în acest sens documente oficiale de la producător.
- Să permită integrarea cu soluţii dedicate de captură a documentelor, prezentându-se în acest sens documente oficiale de la producător.
- Să permită integrarea cu soluţii de management a proceselor, prezentându-se în acest sens documente oficiale de la producător.
- Să permită accesarea documentelor numai de către utilizatorii autorizaţi.
- Să includă un mecanism de acces la documente bazat pe roluri. Drepturile de acces trebuie să poată fi moştenite de toată structura ierarhică a folderelor şi a documentelor.
- Să utilizeze un sistem centralizat de management a utilizatorilor bazat pe standardul LDAP .
- Să ofere o interfaţă dedicată de administrare a platformei.
- Să ofere posibilitatea creării structurii de date, utilizând atât o interfaţă grafică, precum si o interfaţă API.
- Să pună la dispoziţia utilizatorilor scripturi care să permită modificarea schemei bazei de date utilizata ca repository.
- Să permită posibilitatea aflării numărului de documente gestionat de platforma precum si a dimensiunii acestora, atât dintr-o interfaţa grafică, precum şi utilizând o interfaţă API.
- Să ofere posibilitatea de a monitoriza evenimentele
- Să permită auditarea activităţilor utilizatorilor in aplicaţie prin urmărirea evenimentelor, cum ar fi crearea, modificarea si ştergerea documentelor, adăugarea, ştergerea paginilor, crearea, modificarea, ştergerea informaţiilor index, vizualizarea, tipărirea, exportul sau transmiterea prin email a documentelor din arhiva, crearea, ştergerea, indexarea loturilor de documente, salvarea, ştergerea, executarea, modificarea criteriilor de căutare in arhiva, operaţiile de tip check in si check out.
- Să permită păstrarea istoricului activităţii (log introducere documente, aprobări, printări).
- Să asigurare procesele de salvare şi recuperare pentru întregul sistem de documente.
- Să permită păstrarea unui istoric de funcţionare a serverului pentru a se putea urmări potenţialele probleme ce urmează fi transmise echipei de suport tehnic şi un mecanism avansat de audit cu toate operaţiile efectuate asupra documentelor.
- Să permită utilizatorilor recuperarea documentelor şterse prin punerea la dispoziţia a unor facilităţi de tipul “recycle bin”.
- Să permită realizarea operaţiilor de administrare inclusive de pe dispozitive portabile.
- Să ofere suport pentru modelul DITA sau echivalent
- Să permită criptarea documentelor stocate in interiorul acesteia.
- Să pună la dispoziţie un API ce permite utilizarea protocolului REST sau echivalent
- Să pună la dispoziţia utilizatorilor un instrument ce verifica inconsistentele dintre metadate si obiectele stocate în repository.
- Să fie de tip enterprise si sa poată fi instalată pe o gama variata de sisteme de operare incluzând Linux, Windows şi Unix.
- Sa permită încărcarea de documente semnate electronic (format utilizat de către Achizitor p7s sau p7m)

- Sa permită semnarea electronica a documentelor încărcate fără a fi necesara extragerea si reîncărcarea acestora in sistem
- Să permită semnarea electronică invizibilă a documentelor de tip PDF
- In cadrul interfeţei sistemului sa fie vizibile persoanele semnatare a fiecărui document fără a fi necesara deschiderea documentului

Se vor **include licenţe pentru soluţia de management al documentelor**, dimensionată de către Ofertant conform nevoilor identificate în analiza cerinţelor documentaţiei de atribuire şi corelată cu modul de licenţiere al producătorului propus, care să ofere suport **pentru minim 140 de utilizatori concurenţi**.

4.2.1.3 Soluţia care asigură capabilitatea de captură

Soluţia de captură a documentelor trebuie să dispună de următoarele caracteristici:

- Să permită integrarea cu dispozitivele de tip scanner pentru preluarea documentelor tipărite, care nu sunt accesibile electronic.
- Să permită integrarea cu componenta de gestiune a arhivei electronice în vederea transmiterii către acesta a tuturor documentelor scanate precum şi a informaţiilor de catalogare ale acestora.
- Să ofere suport pentru următoarele operaţii în raport cu documentele format hârtie:
  - Scanarea documentelor format hârtie şi obţinerea de imagini scanate.
  - Integrarea cu dispozitive scanner prin standardele ISIS si TWAIN sau echivalente.
  - Utilizarea de separatori de documente pentru oferirea posibilităţii de automatizare a unor procese de lucru.
  - Îmbunătăţirea calităţii imaginilor scanate (ofertele vor detalia acest aspect).
  - Constituirea imaginilor scanate sub formă de documente electronice.
  - Indexarea documentelor electronice prin completarea metadescriptorilor asociaţi.
  - Recunoaşterea optică a textului, formularelor şi codurilor de bare .
  - Recunoaşterea automata a tipului de document pe baza formatului precum şi învăţarea interactivă de noi formate, in timpul sesiunii de lucru.
  - Validarea metadescriptorilor asociaţi la nivel de document, atât manual cât şi automat, pe bază de reguli sau date din sisteme externe.
  - Definirea de multiple fluxuri de scanare si rutarea pe bază de reguli a documentelor pe fluxuri, fără necesitatea de a scrie cod.
  - Posibilitatea de a folosi atât clienţi desktop, cât şi web in cadrul unui flux de scanare intr-o arhitectură bazată pe server
  - Integrarea cu alte sisteme pe parcursul fluxului de scanare si posibilitatea de a ruta fluxul de scanare în funcţie de date din sisteme externe
  - Exportul documentelor electronice validate către sistemul central integrat de gestiune a arhivei electronice.
- Componenta web de vizualizare va permite următoarele operaţii:
  - Vizualizarea direct din browser a imaginilor si documentelor, fără a fi nevoie de instalarea de viewer-e pe staţia locală.
  - Acoperirea unor părţi din imaginile scanate, pentru ca anumite informaţii să nu poată fi vizualizate, din motive de securitate.
  - Posibilitatea de a aplica adnotări pe documente.

Se vor include licenţe pentru soluţia de captură, dimensionată de către Ofertant conform nevoilor identificate în analiza cerinţelor documentaţiei de atribuire şi corelată cu modul de licenţiere al producătorului propus, care să ofere suport **pentru minim 4 utilizatori concurenţi**.

4.2.2 Fluxuri de integrare şi procese de lucru

Capabilitatea de gestiune a proceselor cu documente va permite circulaţia documentelor pe trasee ierarhice sau definite de autorul documentului, cu posibilitatea aprobării sau respingerii acestora, standardizarea, distribuirea şi circulaţia informaţiilor şi a documentelor interne în cadrul structurii, precum şi a celor generate în relaţia cu autorităţi externe.

Astfel, se vor prevede componente pentru modelarea şi implementarea proceselor intr-un mod colaborativ, in scopul documentării, analizei, optimizării, automatizării şi monitorizării proceselor de lucru şi a fluxurilor de documente.

4.2.2.1 Fluxuri de integrare

Componenta (soluţia) de fluxuri de integrare trebuie să dispună de următoarele caracteristici:

- Să constituie un mediu unitar de definire şi modificare a proceselor şi fluxurilor de integrare (modelare, vizualizare, modificare, executare, simulare, optimizare), bazat pe standardul BPMN, BPEL sau echivalent.
- Să includă componente vizuale, configurabile, fără să necesite dezvoltarea sau codarea diagramelor de procese, a activităţilor, formularelor, logicii de integrare, regulilor de business, evenimentelor sau rapoartelor statistice.
- Să permită autorilor de procese să reprezinte grafic parametrii proceselor, să implementeze activităţile necesare şi să modifice parametrii şi regulile de business
- Să permită autorilor de procese să definească procese şi activităţi reutilizabile.
- Să ofere capabilităţi de generare a formularelor web pe baza obiectelor de business utilizate in procese.
- Să ofere componente out-of-the-box utilizate cu drag and drop pentru generarea cu uşurinţă a interfeţei utilizator.
- Să permită modificarea interfeţelor utilizator fără codare sau restartare a server-ului web.
- Să permită autorilor de procese, modificarea cu uşurinţă a fluxurilor de procese, regulilor şi logicii de rutare fără intervenţia utilizatorilor IT şi fără activităţi de tip IT ca instalarea de noi pachete ale aplicaţiei sau modificări in schema bazei de date.
- Să ofere suport vizual de definire a obiectelor de business suportând obiecte cu structuri complexe.
- Să ofere un mecanism de precompletare la definirea de variabile, tipuri de date, roluri, utilizatori sau grupuri.
- Să ofere posibilitatea revizuirii modificărilor intr-o aplicaţie in derulare, fără compilare sau o nouă instalare.
- Să ofere autorilor de procese posibilitatea să execute rapid doar un singur pas din proces, un subset de activităţi sau un proces, fără a fi nevoiţi să execute tot procesul şi fără a executa activităţi de tip IT ca export sau instalare de noua versiune de o proces.
- Să includă un mecanism de atenţionare pentru modificări care ar putea impacta sau genera erori pentru anumite componente.
- Să permită autorilor de procese să definească reguli de business intr-un limbaj aproape natural sau in tabele de decizie, fără intervenţie IT (exemplu regula: dacă vârsta şoferului este mai mică e 18 ani şi mai mare de 80, setează eligibilitatea pe FALSE).

4.2.2.2 Optimizarea încărcării şi Gestionarea Modificărilor

Componenta pentru optimizarea încărcării şi a gestionării modificărilor trebuie să dispună de următoarele caracteristici:

- Să ofere o instalare uşoară de noi versiuni ale unui proces, fără exportul şi instalarea de arhive aplicaţie.

- Să ofere publicarea cu uşurinţă de modificări majore ale unui proces şi aplicarea lor asupra instanţelor de proces in derulare.
- Să suporte execuţia de simulări pe bază de date istorice sau reale, pentru a analiza impactul adus de modificările in procese.
- Să permită filtrarea datelor de simulare pe baza metadata-lor din proces, (cum ar fi nume_client).
- Să ofere rularea de scenariu de simulare "side by side" pentru a compara impactul modificărilor.
- Să permită analiza rezultatelor simulării pe baza căilor de rulare a procesului sau a segmentelor executate.
- Să ofere un nivel ridicat de colaborare intre business şi IT intr-un mediu unificat ce permite tuturor participanţilor să vadă versiunile curente de procese
- Să permită optimizarea şi analiza unor scenarii ce implică mai multe procese.
- Să ofere recomandări de optimizare a procesului de business pe baza simulărilor executate.
- Să permită autorilor de procese să gestioneze şi guverneze cu uşurinţă modificările in procesele şi resursele asociate proceselor, intr-un singur catalog inclus pentru centralizarea şi instalarea proceselor.
- Să suporte rularea in paralel a mai multor versiuni de procese.
- Să ofere o vizibilitate la nivel administrative, pentru a identifica ce versiuni de procese sunt executate pe diferite medii.
- Să fie scalabilă cu uşurinţă oferind capabilităţi robuste pentru arhitecturi in cluster, pentru disponibilitate înaltă şi fail-over.
- suporte cu uşurinţă instalarea de noi versiuni de procese pe diferite medii, fără generări şi export de arhive.
- Să suporte verificarea consistenţei versiunilor la nivel de configuraţii de proces.

4.2.2.3 Orchestrarea serviciilor şi activităţilor

Componenta pentru orchestrarea serviciilor şi activităţilor trebuie să dispună de următoarele caracteristici:

- Să se integreze cu uşurinţă cu soluţii de control al accesului si al identităţii (minim LDAP, Active Directory).
- Să suporte autorizarea şi controlul acceselor pe bază de roluri, grupuri, permisiuni.
- Să fie implementată/dezvoltată pe arhitectura de tip SOA (Arhitectura Orientata pe Servicii).
- Să ofere toate capabilităţi de integrare ale unui ESB şi capabilităţi de server de aplicaţie J2EE sau echivalent.
- Să implementeze standardul BPEL şi BPEL 4 WS sau compliante.
- Să ofere posibilitatea captării de date în timp real din orice bază de date, coadă de mesaje sau aplicaţie.
- Să suporte implementarea proceselor de tip short running (sincrone) cât si a celor de tip long running (asincrone – care necesită intervenţia utilizatorilor), astfel:
  - să permită implementarea şi rularea proceselor tranzacţionale (commit/rollback) pentru procesele de tip "short running";
  - să ofere mecanisme de compensare a tranzacţiilor pentru procesele de tip "long running". Pentru fiecare pas de execuţie, sau secvenţă de paşi de execuţie, al procesului trebuie să ofere posibilitatea de a defini o acţiune compensatorie-opusă.
- Să ofere mecanisme de tratare a erorilor. Acest mecanism trebuie să fie capabil sa declanşeze şi mecanismele de compensare descrise mai sus.
- Să ofere posibilitatea includerii de in-line java code direct in fluxurile de procese.

- Să permită rularea de procese de integrare cu alte sisteme informatice, de tip service bus şi procese care necesită o execuţie de tip „straight-through” cu performanţă ridicată.
- Să permită patern-uri de mesaje şi protocoale, cum ar fi publish/subscribe, scrion/asincron, şi topics/queues.
- Să ofere suport complet pentru persistenţa mesajelor.
- Să permită integrare la nivel de FTP, fişier şi bază de date, SCA, Web Service-uri sau cu adaptori.
- Să suporte o gamă largă de adaptori de tehnologie şi de aplicaţii (cel puţin SAP, Oracle, PeopleSoft).
- Să ofere un mod centralizat de gestiune a politicilor de securitate (autentificare, autorizare, criptare, decriptare) peste portofoliul de fluxuri electronice instalat.
- Să suporte standardul JCA, sau compliant, pentru conectarea la sisteme externe.
- Să ofere suport pentru modelele de programare bazate pe standardul SDO şi SCA, sau compliante cu acestea.
- Să permită integrare cu un catalog de servicii, pentru gestionare politici si guvernare.
- Să permită selectarea in mod dinamic a End Point WebService dintr-un catalog de servicii.
- Să ofere un mediu integrat de test pentru integrarea cu un catalog de servicii.
- Să ofere securitate bazată pe Single Sign-On (SSO).
- Să ofere balansarea activităţilor pe baza algoritmului Round Robin sau încărcării utilizatorilor, dar şi distribuirea automată pe bază de afinitate utilizator, grupuri, lista de utilizatori sau politici particularizate de rutare.
- Să ofere prioritizarea activităţilor pe baza unor reguli sau condiţii de business
- Să ofere un sistem tip portal out-of-the-box pentru ca utilizatorii de business să rezolve activităţile în lucru
- Să suporte standardele WSRP si JSR168 care permit integrarea cu un Portal Web.
- Să ofere REST API sau echivalent pentru accesarea şi modificarea listei de activităţi
- Să permită utilizatorilor să vizualizeze un istoric al activităţilor fără a rula un anumit proces.
- Să suporte executarea de procese cu calendare şi fusuri orare multiple
- Să suporte delegarea automată a activităţilor umane către alţi utilizatori, pe bază de reguli sau încărcare
- Să permită utilizatorilor să suprascrie manual datele unei instanţe de proces in derulare, iar aceste modificări să poată fi capturare şi raportate
- Să permită crearea automată de tipuri de date direct dintr-un fişier WSDL (sau echivalent) sau un Registru tip UDDI (sau echivalent).

4.2.2.4 Gestionarea Evenimentelor

Componenta pentru gestionarea evenimentelor trebuie să dispună de următoarele caracteristici:

- Să detecteze automat evenimente din alte sisteme, să evalueze aceste evenimente şi să acţioneze corespunzător.
- Să suporte detectarea şi programarea evenimentelor.
- Să suporte invocări asincrone pe bază de evenimente.
- Să suporte definirea şi evaluarea de condiţii şi reguli de evenimente.
- Evenimentele trebuie să poată fi reprezentate şi definite in diagrama de proces.
- Să suporte programarea executării proceselor pe bază de trigeri, alerte, date de exporare, intervale de timp.
- Să garanteze livrarea evenimentelor trimise de alte sisteme.

- Să suporte selectarea de evenimente, prioritizarea şi gruparea acestora pe bază de reguli specifice proceselor de business.
- Să suporte corelarea de evenimente pentru a executa anumite procese de business pe baza regulilor specifice proceselor.
- Să ofere scalabilitatea subsitemului de gestiune a evenimentelor, odată cu creşterea numărului de evenimente şi apariţie a lor.

4.2.2.5 Monitorizarea si Raportarea

Componenta pentru monitorizarea proceselor şi pentru raportare trebuie să dispună de următoarele caracteristici:

- Să ofere definirea de puncte de măsură a performanţei la nivel de fiecare activitate sau proces.
- Să ofere posibilitatea accesului la măsurările performanţei prin API sau tablouri de bord uşor de citit de către utilizatorii de business
- Să permită analiştilor de business construirea de rapoarte personalizate si cu filtrări ad-hoc, utilizând datele măsurate, fără scrierea de cod
- Să permită autorilor de procese să creeze dashboard-uri ce include rapoarte multiple şi date externe
- Să ofere posibilitatea de drill down in rapoarte pe mai multe niveluri.
- Să ofere autorilor de procese posibilitatea analizei proceselor in timp real, dar şi a evoluţiei in timp şi a optimizării.
- Să ofere ”out of the box” diferite scoreboard-uri şi tablouri de bord pentru măsurarea performanţei proceselor, a utilizatorilor participanţi in proces, a echipelor de utilizatori sau a diferitelor KPI-uri. De asemenea trebuie să ofere flexibilitate in creare de noi rapoarte, tablouri de bord, KPI-uri sau scoreboard-uri specifice proceselor.
- Să ofere ”out of the box” capabilităţi de drill-down la nivel de fiecare instanţă de proces completă, in risc sau depăşită.
- Să ofere ”out of the box”, tablouri de bord care să măsoare tendinţele de performanţă ale procesului.

Se vor include licenţe pentru soluţia (incluzând toate componentele) de fluxuri de integrare şi procese de lucru, dimensionată de către Ofertant conform nevoilor identificate în analiza cerinţelor documentaţiei de atribuire şi corelată cu modul de licenţiere al producătorului propus, însă nu mai puţin de: 1 nucleu pentru componenta server de web, 2 nuclee pentru componenta server de proces şi 4 nuclee de server de aplicaţii.

Notă: 1 nucleu = 1 core-processor x86_64.

4.2.3 Administrarea utilizatorilor şi controlul accesului

Prin creşterea numărului de utilizatori informatici în instituţie şi prin creşterea interacţiunii acestora cu mediul extern care au acces la informaţiile instituţiei a apărut problema de gestionare a identităţii utilizatorilor de-a lungul ciclului de viaţă în capabilitatea care asigură infrastructura de fluxuri informatice.

Capabilitatea de administrare a utilizatorilor şi controlul accesului vine în ajutorul instituţiei cu îmbunătăţirea aspectelor de securitate ale sistemelor informatice prin operaţii specifice de management al utilizatorilor .

În acest sens avem nevoie de o soluţie care trebuie să asigure administrarea utilizatorilor şi care adresează problemele principale în acest sens, bazându-se pe politici sigure şi automatizate de control al accesului.

Soluţia pentru administrarea utilizatorilor trebuie să dispună de următoarele caracteristici:

4.2.3.1 Administrarea utilizatorilor

- Să fie compatibilă cu o platformă tip J2EE, .NET sau echivalent
- Să includă interfeţe administrative capabile web.
- Să ruleze ca un site web securizat.
- Să ofere capabilitatea de a detecta în timp real orice schimbare în informaţia referitoare la un utilizator (nume, prenume, parola, alte proprietăţi) care apare în orice sursă care conţine respectiva informaţie si să propage in mod automat acea schimbare către orice alta sursă care conţine informaţii despre acel utilizator. Mecanismul de propagare trebuie să fie configurabil.
- Să poată prelua informaţiile despre utilizator din surse multiple: fişiere neformatate, fişiere XML, baze de date, baze de date, servere de directoare.
- Să fie compatibilă cu surse multiple care stochează informaţiile de identitate (precum un sistem HR, baze de date, fişiere, servere de directoare).
- Să ofere capabilitatea de a aloca / modifica drepturile de utilizator / privilegiile de acces la resursele organizaţiei în funcţie de politicile existente in organizaţie şi de rolul utilizatorului în organizaţie.
- Să ofere capabilitatea de a delega responsabilitatea de administrare către divizii, departamente sau alte unităţi ale organizaţiei.
- Să ofere capabilitatea de a permite utilizatorilor să iţi administreze parolele, incluzând schimbarea şi resetarea parolelor fără intervenţia administratorilor.
- Să permită utilizatorilor să solicite crearea de noi conturi folosind un browser web (user self service).
- Să permită utilizatorilor să îţi actualizeze informaţiile personale (adresă, telefon etc.) şi să propage în mod automat informaţia către toate resursele organizaţiei care conţin total sau parţial acele informaţii.
- Să conţină un motor pentru fluxul de lucru care direcţionează orice cerere către aprobatorul sau aprobatorii corespunzători; notificările trebuie făcute printr-un sistem email.
- Să ofere o interfaţă grafică pentru configurarea fluxului de lucru conform politicilor / procedurilor existente in organizaţie.
- Să poată simula orice schimbare referitoare la informaţiile despre utilizatori, politici înainte de efectuarea schimbării.
- Să ofere capabilitatea de a vizualiza solicitările oricărui utilizator sau cererile care privesc solicitările legate de modificarea informaţiei utilizatorului.

4.2.3.1.1 Administrarea conturilor de utilizator

- Să asigure că fiecare cont de utilizator are un ID unic.
- Să ofere reguli configurabile pentru crearea identificatorilor unici.
- Să permită utilizarea unei date de expirare care poate fi utilizată pentru a urmări înnoirea / ştergerea / modificarea conturilor de utilizator.
- Să suporte expirarea conturilor de utilizator pentru diferite tipuri de utilizatori folosind o dată de expirare a contului sau o dată de terminare a contractului
- Să permită notificarea prin email a proprietarului oricărui cont care a fost inactiv pentru o perioadă configurabilă.
- Să ofere o politică de revocare/ştergere a conturilor inactive în cadrul unei perioade configurabile.
- Să ofere capabilitatea de a exporta/importa utilizatori.
- Să ofere capabilitatea de a aproba în mod automat orice solicitare printr-un set de reguli şi politici.

- Să ofere capabilitatea de a vizualiza o solicitare de cont care a fost trimisă şi datele asociate cu acea solicitare.
- Să permită ca grupurile de utilizatori să fie create dintr-o interfaţă web.

4.2.3.1.2 Crearea de reguli bazate pe rol

- Să suporte crearea de ’roluri’ prin:
  - Suportarea atribuirii utilizatorilor către mai multe roluri;
  - Suportarea atribuirii utilizatorilor către roluri ierarhice;
  - Oferirea capabilităţii de a specifica roluri care exclud alte roluri pentru a preveni atribuirea de roluri care s-ar afla în conflict
  - Atribuirea de proprietăţi pentru contul de utilizator odată cu rolul utilizatorului.
  - Utilizarea sistemelor de informaţii cheie din mediul organizaţiei ca sursă de informaţii de încredere despre informaţii de identitate pentru a genera crearea automată de conturi (de ex detectarea noilor angajaţi adăugaţi şi crearea automată de conturi pentru noii angajaţi in funcţie de rolul lor in organizaţie).
  - Atribuirea de resurse pentru un cont odată cu rolul.
  - Atribuirea de drepturi de acces diferite faţă de cele corespunzătoare rolurilor, pentru utilizatori.
  - Atribuirea de drepturi de acces individuale pe lângă cele definite in cadrul rolului, pentru utilizatori.
  - Schimbarea dinamică şi automată a drepturilor de acces in funcţie de schimbările din rolurile utilizatorilor.
  - Generarea de ID-uri de utilizator unice, în conformitate cu politicile organizaţiei.
  - Suportul noţiunii de ’roluri persistente’ (adică schimbările făcute definiţiei unui rol sunt aplicate tuturor utilizatorilor sub acelaşi rol).
  - Suportul mutării unui utilizator dintr-un rol în altul, impactul fiind modificarea drepturilor de acces corespunzătoare noului rol.
  - Suportul rolurilor ”flexibile”.
  - Suportul introducerii drepturilor de utilizator arbitrare ca parte a procesului de oferire de drepturi.
- Să suporte opţiuni multiple de anulare a drepturilor (precum oprirea dar lăsarea conturilor intacte, ştergerea conturilor dar păstrarea identităţii utilizatorului, sau ştergerea cu totul a utilizatorului).
- Să suporte descoperirea automată şi rezolvarea inadvertenţelor de informaţii de identitate dispersate pe mai multe resurse (de exemplu, sincronizarea datelor între mai multe directoare, baze de date şi fişiere).

4.2.3.1.3 Delegarea administrării

- Să ofere capabilităţi de administrare granulară delegată precum politici de informaţie internă de control al accesului (ACI) care limitează atât accesul utilizatorului cât şi al administratorului la rapoarte, informaţii ale utilizatorilor, şi funcţii operaţionale, cu rubrici specifice ’Permis’ şi ’Nepermis’ pentru toate atributele şi operaţiile de identitate (ştergere, transfer, căutare, recuperare, suspendare, adăugare şi modificare).
- Să ofere abilitatea de a propaga utilizatorii desemnaţi (administratorii delegaţi) în funcţie de rol sau în funcţie de un set de atribute configurabile.
- Să permită sarcini administrative cu ‘n‘ niveluri de profunzime.
- Să ofere capabilităţi de lucru în medii izolate (cel puţin reţele izolate prin firewall-uri).
- Să utilizeze tehnologia internet (cel puţin email şi pagini web) pentru facilitarea aprobării in cadrul fluxurilor de lucru.

4.2.3.1.4 Administrarea parolelor

- Să ofere funcţii de resetări de parole ale conturile pe platformele administrate
- Să sincronizeze parolele pentru utilizatori imediat ce utilizatorul şi-a schimbat parola
- Să includă o notificare de operaţie reuşite/nereuşită pentru administrarea parolei (resetare şi sincronizare).
- Să permită trimiterea unei notificări email către un utilizator într-o manieră configurabilă cu un număr de zile înainte ca parola/contul său să expire.
- Să poată genera în mod aleator parola iniţială a unui cont de utilizator.
- Să aibă abilitatea de generare a unei parole pentru utilizarea în accesul iniţial al sistemului.
- Să poată forţa utilizatorul să schimbe parola resetată după prima folosire.
- Să aibă abilitatea de a impune anumite combinaţii configurabile de caractere alfa şi numerice într-o parolă.
- Să poată impune politica parolei (cel puţin: lungime, număr de caractere alfanumerice, caractere neacceptate) atunci când utilizatorii schimbă sau sincronizează parole.
- Să suporte o listă de parole restricţionate pentru a nu permite utilizatorilor să selecteze cuvinte comune.
- Să poată menţine un istoric al parolelor configurabil pentru a evita reutilizarea parolei.
- Să ofere capabilitatea de a genera parole ca un set aleatoriu de numere şi caractere cu lungime configurabilă.
- Să suporte un număr configurabil de întrebări pentru recuperarea eventualitatea unei parole uitate. Numărul si conţinutul întrebărilor si răspunsurilor trebuie sa poată fi configurat de către fiecare utilizator.

4.2.3.1.5 Flux de lucru automatizat

- Să ofere capabilitatea ca oricărui utilizator să-i fie atribuită o acţiune printr-un proces de flux de lucru.
- Să ofere capabilitatea ca anumiţi utilizatori să aibă privilegii de acces specifice pentru a crea, modifica şi/sau şterge un proces de flux de lucru.
- Să aibă capabilitatea de a iniţia procese de fluxuri de lucru bazate pe declanşatori veniţi din sisteme externe.
- Să aibă capabilitatea de a detecta noii angajaţi adăugaţi într-un sistem HR sau în alte surse şi automatizează procesul de acordare a drepturilor pentru noul utilizator.
- Să aibă capabilitatea să automatizeze procesul de acordare sau luare a drepturilor cu sau fără un flux de lucru.
- Componenta flux de lucru a soluţiei trebuie să fie o funcţionalitate integrată a soluţiei pentru administrarea utilizatorilor.
- Componenta flux de lucru a soluţiei trebuie să ofere abilitatea să ridice nivelul sau să transmită acţiunile/cererile în funcţie de data la care au fost iniţiate.
- Componenta flux de lucru trebuie să suporte cerinţe logice conţinute între diferite etape.
- Componenta flux de lucru a soluţiei trebuie să permită participanţilor la fluxul de lucru să întreprindă acţiuni (aprobare / rejectate) prin intermediul unui browser web.
- Componenta flux de lucru a soluţiei trebuie să suporte transmiterea solicitărilor folosind sisteme de mesagerie (e-mail).
- Componenta flux de lucru a soluţiei trebuie să suporte bifurcaţii şi împreunări ale proceselor.
- Componenta flux de lucru a soluţiei trebuie să suporte crearea unui flux de lucru cu etape multiple şi lansarea unui sub-flux de lucru.
- Componenta flux de lucru a soluţiei trebuie să suporte procesele care pot avea sub-fluxuri de lucru sau fluxuri găzduite.

- Componenta flux de lucru a soluţiei trebuie să suporte modificări ale procesului dinamic, în timp real, pentru procesele care rulează.
- Componenta flux de lucru a soluţiei suportă reutilizarea proceselor/fluxurilor de lucru create.
- Componenta flux de lucru a soluţiei trebuie să suporte transmiterea bazată pe rol către recipienţi.
- Componenta flux de lucru a soluţiei trebuie să suporte roluri alternatoare (delegaţi).
- Componenta flux de lucru a soluţiei trebuie să permită unei interfeţe să invoce aplicaţii externe ca să lege orice date relevante ale fluxului de lucru.
- Componenta flux de lucru a soluţiei trebuie să ofere o interfaţă grafică pentru dezvoltarea proceselor/fluxului de lucru.

4.2.3.1.6 Raportarea

- Să includă (în distribuţia soluţiei) cel puţin următoarele rapoarte standard:
  - Raport de operaţii – Raport ale tranzacţiilor operaţionale de un anumit tip (de ex. Adăugarea unui nou utilizator).
  - Raportul de serviciu – tranzacţiile trimise care afectează oferirea către resurse administrate (ex.: server Unix).
  - Raport de utilizator – tranzacţiile trimise care afectează conturile utilizatorilor.
  - Raport de respingere – conturile respinse de către aprobatori în cadrul procesului fluxului de lucru.
  - Raport de reconciliere – rezultatele din reconcilierile recente ale unei resurse administrare.
  - Raportul conturilor inactive de către Resursa Administrativă (ex.: Conturile in sisteme Unix).
  - Raportul conturilor – listează utilizatorii şi conturile asociate şi dacă contul se conformează politicilor curente sau nu.
- Rapoartele trebuie să fie generate în timp real către utilizator/administrator.
- Rapoartele trebuie redate în format pdf.
- Soluţia trebuie să poată genera rapoarte configurabile.

4.2.3.1.7 Interfaţa cu utilizatorul

Interfaţa cu utilizatorul trebuie să fie configurabilă, permiţând cel puţin specificarea:

- fonturilor,
- culorilor,
- localizarea tastelor de navigare,
- numele de afişare ale câmpurilor,
- amplasamentul siglelor.

4.2.3.1.8 Arhitectura de conectare

- Să ofere conexiune fără agenţi, în afară de agenţii platformei locale către resurse de administrare.
- Să ofere agenţi/conexiuni către următoarele resurse:
  - Sistemul de operare,
  - Servere de aplicaţii,
  - Sisteme de Directoare,
  - Baze de date,
  - Produse de autentificare majore,
  - Produse web SSO,
  - Platforme de mesaje/email,

- Aplicaţii de tip help desk,
- Aplicaţii ERP,
- Aplicaţii HR.

- Să includă un SDK pentru a extinde acoperirea platformelor administrate prin aplicaţii customizate şi proprietare (construite în companie).
- Să permită sistemelor externe să acceseze sau să interogheze date din interiorul produsului (cel puţin LDAP, ODBC, JDBC).
- Să includă un "scheduler" pentru rularea sarcinilor programate.

4.2.3.1.9 Caracteristici de securitate

- Să folosească un mecanism de autentificare LDAP cu nume de utilizator şi parolă pentru toate accesele, inclusiv GUI web şi cereri API
- Să se integreze (folosind plugin-uri sau agenţi) cu suport pentru soluţia de autentificare a utilizatorilor.
- Să poată impune încetarea sesiunii din cauza inactivităţii pe o perioadă de timp configurabilă
- Să permită ca toate parolele să fie mascate la introducere
- Toate sesiunile de comunicare din soluţie trebuie securizate folosindu-se sesiuni de criptare SSL cel puţin 128 bit. Aceasta include toate sesiunile utilizatorilor finali cu browsere web precum şi comunicarea între componentele soluţiei precum serverul şi agenţii săi.
- Să ofere o politică de parolă care se poate aplica global tuturor conturilor ţintă sau care poate fi atribuită unuia sau mai multor servicii ţintă, şi are mai multe aspecte, incluzând:
  - Lungime minimă şi maximă,
  - Numărul maxim de caractere repetabile,
  - Numărul minim de caractere alfa şi/sau numerice,
  - Definirea caracterelor invalide şi/sau a celor cerute,
  - Restricţionarea primului caracter şi/sau a întregii parole la un set de caractere declarat,
  - Numărul de parole precedente să nu fie permis (inclusiv cele scrise invers),
  - Nepermiterea numelui de utilizator şi/sau a IDului de utilizator ca parolă,
  - Nepermiterea parolelor găsite în dicţionare .
- Să permită ca valoarea iniţială a parolei trebuie să fie limitată la prima folosire.
- Să ofere posibilitatea de a genera parole aleatoare.
- Să ofere metodele de suspendare/terminare/modificare a contului în cauză conform politicii organizaţiei dacă statutul unui utilizator se schimbă (schimbarea rolului, schimbarea zonei de responsabilitate, concediu fără plată, terminare etc.) .
- Să ofere metode pentru prevenirea reutilizării identităţilor conturilor după ce acestea au fost retrase.

4.2.3.1.10 Salvare şi restaurare

Toate componentele/soluţiile infrastructurii de fluxuri informatice trebuie să fie compatibile (suportate) de aplicaţia de salvare şi restaurare centralizată a datelor oferită (descrisă în prezentul document la capitolul 4.3.3 – "Salvare şi Restaurare Centralizată a Datelor") , fără ca să fie nevoie de oprirea vreunui serviciu în timpul procesului de salvare a datelor.

4.2.3.2 Controlul accesului

Soluţia pentru controlul accesului utilizatorilor trebuie să dispună de următoarele caracteristici:

- Să ofere capabilităţi de autentificare.
- Să ofere capabilităţi de autorizare prin utilizarea următoarelor mecanisme:

    - Propriul serviciu de autorizare,
    - Liste de control al accesului (ACL), politici de obiect protejat (POP) şi reguli de autorizare pentru control al accesului la nivel scăzut,
    - Autorizarea API bazată pe standarde, folosind un API pentru aplicaţiile de limbaj C, şi Java Auhentication & Authorization Service (JAAS) pentru aplicaţiile Java,
    - Capabilitate pentru serviciu de autorizare externă.
- Să ofere posibilitatea criptării schimbului de informaţii între server şi client.
- Să ofere suport pentru utilizarea combinată a standardelor de criptare şi a algoritmilor de detectare a modificărilor ţinând cont de următoarele considerente:
    - Comunicare prin folosirea protocolului de control al transmisei (TCP) standard (nu oferă protecţie),
    - Integritatea datelor – protejează mesajele (fluxurile de date) împotriva modificărilor din timpul comunicării pe reţea,
    - Secretul datelor – protejează mesajele împotriva modificărilor sau inspecţiilor din timpul comunicării pe reţea).
- Să ofere suport pentru integritatea datelor prin intermediul protocolului de comunicare Secure Sockets Layer (SSL).
- Să ofere suport pentru scalabilitate (a soluţiei).
- Să ofere capabilităţi de logare şi auditare (a informaţiei).
- Să ofere suport pentru administrare centralizată.
- Să permită folosirea browserele web, cel puţin Microsoft Internet Explorer, Mozilla Firefox, Google Chrome.
- Să ofere suport pentru cel puţin următoarele platforme (sisteme de operare), sau echivalent:
    - Microsoft Windows 2008, 2012,
    - Red Hat Enterprise Linux,
    - Sun Solaris,
    - IBM AIX,
    - HP-UX.
- Să fie certificată cel puţin conform Common Criteria Certification EAL3.

În plus, soluţia pentru controlul accesului utilizatorilor trebuie să dispună de următoarele caracteristici:

4.2.3.2.1 Specificaţii funcţionale

- Abstractizarea / Translatarea Adresei de Reţea - Toate adresele interne trebuie să fie abstractizate, translatate sau ascunse utilizatorilor finali care accesează aplicaţii interne.
- Abstractizarea / Translatarea Namespace/URL - Serverul Reverse Proxy trebuie să abstractizeze, translateze si să ascundă numele de sistem şi URL-urile interne. Este necesară capabilitatea de mapare între numele intern şi extern al URL-ului. Maparea trebuie să se aplice URL-ului tuturor cererilor, redirecţionărilor, linkurilor şi conţinutului afişat.
- Suport pentru autentificare globală (SSO) - Mecanismul Reverse Proxy trebuie să ofere mecanisme pentru autentificare globală. Trebuie să ofere posibilitatea de efectuare a mai multor operaţii de autorizare pentru resurse sau aplicaţii diferite fără să fie necesară reautentificarea utilizatorului dacă noua resursă sau aplicaţie necesită un nivel mai ridicat de autentificare.
- Suport pentru autentificare globală (SSO) - Mecanismul Reverse Proxy trebuie să ofere mecanisme pentru autentificare globală. Trebuie să ofere posibilitatea de efectuare a mai multor operaţii de autorizare pentru resurse sau aplicaţii diferite fără să fie necesară

reautentificarea utilizatorului dacă noua resursă sau aplicaţie necesită un nivel mai ridicat de autentificare.

- Accelerarea Criptării/Decriptării SSL - Mecanismul Reverse Proxy trebuie să suporte mecanisme de criptare/decriptare hardware pentru a îmbunătăţi performanţa SSL
- Accelerarea Criptării/Decriptării SSL - Mecanismul Reverse Proxy trebuie să suporte mecanisme de criptare/decriptare hardware pentru a îmbunătăţi performanţa SSL.
- Suport pentru Split SSL Certificate - Mecanismul Reverse Proxy trebuie să ofere serverului suport pentru certificate SSL pentru sisteme client externe.
- Asigurare suport pentru următoarele mecanisme de criptare, fără a se limita la:
    - 128-bit RC2,
    - 128-bit RC4,
    - 256-bit AES,
    - 56-bit DES,
    - 168-bit triple DES

4.2.3.2.2 Scalabilitate

Din punct de vedere al scalabilităţii, Mecanismul Reverse Proxy trebuie să fie scalabil pentru a suporta zeci de mii de sesiuni simultane.

4.2.3.2.3 Securitate

- Legătură prin proxy - Toate conexiunile prin reţea către resurse şi aplicaţii din zona DMZ sau interne trebuie să fie iniţiate de la serverul reverse proxy. Adresele de reţea sau “namespace-urile” externe ale clienţilor nu vor fi permise în DMZ sau în serverele interne de web sau de aplicaţii. Serverul reverse proxy trebuie, în caz de eroare, să intre într-un mod de siguranţă sau de blocare a accesului, nu într-un mod “pass-thru.”
- Metode de autentificare - Serverul reverse proxy trebuie să suporte următoarele metode de autentificare:
    - Nume de utilizator/parolă,
    - Certificate Client x.509,
    - Autentificare RSA SecureID,
    - Autentificare NTLM,
    - LDAP.
- Suport pentru autentificare cu doi actori de autentificare - Serverul reverse proxy trebuie să suporte autentificare cu doi factori prin RSA SecureID hardware tokens şi combinarea a două metode de autentificare cu factor singular precum certificatele X.509 şi nume de utilizator/parolă.
- Impunerea criptării - Soluţia trebuie să permită definirea politicilor de securitate pentru a defini la orice nivel cerinţa criptării sesiunii.
- Politici si Restricţionări - Soluţia trebuie să includă politici de securitate configurabile care să permită impunerea de restricţii de acces in funcţie de interval de timp, adresa IP sau clase de adrese pentru a limita accesul la resurse. Soluţia trebuie să includă politici care să permită accesul utilizatorilor doar la acele resurse protejate pe care au dreptul sa le acceseze, în funcţie de rolul lor în organizaţie.
- Integrare LDAP si Server de aplicaţii - Soluţia trebuie să conţină un server de directoare LDAP pentru administrarea utilizatorilor şi să se integreze nativ cu serverul de aplicaţii.
- Administrare centralizată - Soluţia trebuie să ofere administrare centralizata bazata pe tehnologie web pentru administrarea utilizatorilor, grupurilor, rolurilor, permisiunilor, politicilor, domeniilor, resurselor protejate etc.
- Delegarea administrării - Soluţia trebuie să ofere un model administrativ flexibil care să permită mai multe niveluri de administrare precum şi delegarea administrării.

4.2.3.2.4 Disponibilitate

- Integrare cu mecanisme de balansare a sarcinii - Serverul Reverse Proxy trebuie să coexiste şi să opereze în spatele oricărei soluţii de balansare a încărcării pentru a echilibra traficul şi a oferi disponibilitate ridicată a sistemului.
- Suport pentru centre de date multiple - Serverul Reverse Proxy trebuie să suporte capabilitatea de a migra suportul pentru aplicaţie către alte servere proxy dintr-un centru de date alternativ sau dintr-un alt punct de conectivitate în eventualitatea unei probleme majore sau al unui eveniment de întreţinere.

4.2.3.2.5 Caracteristici pentru Monitorizare/Raportare

- Evenimente/Alarme - Soluţia trebuie să se integreze cu sistemul de monitorizare şi corelare de evenimente pentru a afişa evenimente şi alerte personalului administrativ.
- Auditare şi Raportare - Soluţia trebuie să includă mecanisme de auditare pentru toate evenimentele de autentificare, autorizare şi administrare, precum şi avertizări legate de componentele soluţiei, incluzând cel puţin:
  - Logări reuşite,
  - Logări nereuşite,
  - Conturile blocate,
  - Mesaje de acces neautorizat,
  - Toate încercările de acces,
  - Erorile de autorizare,
  - Utilizatorii anonimi,
  - Identificarea creării, modificării sau ştergerii,
  - Crearea, modificarea şi ştergerea politicii,
  - Evenimente suspicioase,
  - Urmărirea utilizatorilor anonimi.
- Înregistrările de audit vor fi scrise în format XML în fişiere ASCII neformatate.
- Istoricul schimbării/ reconfigurării - Soluţia trebuie să păstreze istoricul modificărilor configuraţiei pentru administrarea configurării şi pentru scopuri de investigare a eventualelor evenimente de securitate.
- Administrarea logurilor - Soluţia trebuie să suporte arhivarea logurilor de evenimente/alerte precum şi funcţionalităţi de export a acestora. Logurile trebuie reţinute pe termen lung şi informaţia din loguri trebuie să fie exportabilă în formate pentru post-procesare şi analiză.

Se vor include licenţe pentru soluţia/soluţiile de administrare a utilizatorilor şi control al accesului, dimensionate de către Ofertant conform nevoilor identificate în analiza cerinţelor documentaţiei de atribuire şi corelate cu modul de licenţiere al producătorului/producătorilor propus/propuşi, care să ofere suport pentru minim 140 utilizatori.

4.3 Infrastructură de susţinere a Activităţii Administrative IT

Infrastructura de susţinere a activităţii administrative IT trebuie să asigure departamentului IT din cadrul ANFP toate instrumentele necesare implementării acestui proiect şi în acelaşi timp să rezolve problemele semnalate din urma sesiunilor de audit de securitate (incluzând şi sesiunile tip ”pentest”).
Pentru a răspunde necesităţilor ANFP, infrastructura de susţinere a activităţi de administrare trebuie să ofere următoarele capabilităţi prin intermediul unor soluţii/componente COTS dedicate:

- Managementul activelor,

- Monitorizarea interacţiunii utilizatorilor cu aplicaţii specifice,
- Backup centralizat,
- Soluţie de backup şi restaurare granulară a serviciului director,
- Soluţie suport pentru audit de securitate,
- Help Desk.

Cerinţele detaliate pentru soluţiile componentele de mai sus se regăsesc în subcapitolele de mai jos.

4.3.1 Management activ IT

Activele instituţiei sunt incluse în fluxuri tehnologice complexe, ceea ce determină unificarea modalităţilor de operare şi gestionare a acestora. Soluţia propusă pentru managementul activelor vine in ajutorul procesului decizional din cadrul instituţiei prin combinarea managementului activelor IT cu procesele departamentale.

4.3.1.1 Caracteristici generale de management

Soluţia pentru managementul activelor IT trebuie să dispună de următoarele caracteristici:

4.3.1.1.1 Managementul activelor IT

Să include toate mecanismele de control necesare ţinerii evidenţei activelor IT pe întregul ciclu de viaţă:

- Urmărirea detaliilor privind activele IT (ex. imprimante) – inclusiv utilizarea, munca şi costurile asociate – de-a lungul timpului pentru a maximiza productivitatea şi a prelungi viaţa activelor.
- Certificarea locaţiilor şi a activelor – pentru a crea centre de cost atât la nivel de locaţie cat şi la nivel atomic, legat de active.
- Monitorizarea stării activelor şi a locaţiilor – pentru o abordare proactivă mai curând decât reactivă care să reducă indisponibilitatea activelor.

4.3.1.1.2 Managementul muncii

Să ofere suport pentru gestionarea muncii de mentenanţă planificată sau neplanificată, de la cererea iniţială şi generarea ordinului de lucru şi până la închiderea ordinului de lucru şi înregistrarea consumurilor reale. Personalul care planifică munca va putea să coreleze sarcinile cu resursele umane disponibile, să estimeze costurile şi bugetele necesare, să stabilească prioritățile şi să iniţieze activităţi de mentenanţă. Se vor furniza:

- Instrumente de urmărire în detaliu a resurselor, materialelor şi a echipamentelor utilizate pentru a reduce costurile cu munca şi cu materialele;
- Interfaţă grafică pentru distribuţia sarcinilor, planificarea resurselor, responsabilizarea personalului calificat pentru efectuarea sarcinilor;
- Funcţionalitatea de mentenanţă preventivă permite planificarea muncii de mentenanţă regulată precum şi preplanificarea resurselor necesare efectuării sarcinilor prevăzute.

4.3.1.1.3 Managementul serviciilor

Suport inclus pentru facilitarea cererilor de servicii pentru utilizatorii sistemului precum şi gestionarea acestora, care va permite:

- Oferte interne de servicii care sunt critice şi care susţin afacerea;
- Stabilirea de niveluri de servicii specifice fiecărei organizaţii în parte;
- Monitorizarea continuă a nivelelor de servicii;
- Proceduri de escaladare care să permită managementul optim al resurselor.

4.3.1.1.4 Managementul contractelor

Îmbunătăţirea controlului asupra contractelor cu furnizorii cu ajutorul acestui sistem integrat este dată de capacitatea de a administra contracte complexe de furnizare, leasing, închiriere, garanţie sau de muncă. Este permisă şi definirea de noi contracte tip, specifice fiecărui client în parte. Se vor furniza:

- Corelări cu nivelele de servicii aşteptate şi specificate de contracte, pentru a discrimina furnizorii neserioşi sau a căror calitate de furnizare este inconstantă sau slabă;
- O bibliotecă de termeni şi condiţii care va permite crearea de politici organizaţionale coerente;
- Notificări şi alerte automate care să permită realizarea condiţiilor contractuale, evitarea penalităţilor şi realizarea completă a contractelor.

4.3.1.1.5 Managementul materiilor prime şi al consumabilelor

- Soluţia trebuie să răspundă principalelor întrebări: “Ce”, “unde”, “când”, “cât în cantitate şi în valoare” – în relaţie cu materialele folosite de activele IT. Mişcările şi schimbările trebuiesc urmărite pentru a permite raportarea în timp real.
- Se vor urmări toate tranzacţiile din inventar.
- Soluţia trebuie să permită optimizarea şi planificarea inventarului pentru a satisface nevoile de mentenanţă şi cele privind cererea de materiale, disponibile acolo unde este nevoie de ele.

4.3.1.1.6 Managementul achiziţiilor

Suport inclus pentru toate fazele de achiziţie, inclusiv achiziţie directă şi reîmprospătarea inventarului. Cerere de oferte, cereri interne, furnizori, achiziţii, contracte – toate acestea sunt disponibile chiar şi prin integrarea cu alte sisteme ERP incluzând fără a se limita la tehnologii SAP, Oracle sau echivalent.

- Instrumente pentru managementul furnizorilor şi de analiză de performanţă a relaţiei cu aceştia;
- Instrumente de automatizare a monitorizării stocurilor şi a generării de comenzi care să permită comandarea din timp şi în cantităţile necesare a materialelor şi/sau a serviciilor necesare;
- Indicatori de performanţă specifici activităţilor de achiziţii.

4.3.1.2 Caracteristici de securitate

- Soluţia trebuie să includă de un mecanism de auditare astfel încât orice operaţiune efectuata în sistem să poată fi urmărită.
- Soluţia trebuie să fie accesibila prin interfaţa web securizata;
- Soluţia trebuie să includă instrumente de control acces/declarare a drepturilor la nivel de utilizator şi grupuri de utilizatori acordate în concordanta cu atribuţiile şi responsabilităţile fiecăruia.

4.3.1.3 Alte caracteristici

- Să fie o soluţie conformă standardul ITIL sau echivalent.
- Soluţia trebuie să includă instrumente de control acces/declarare a drepturilor la nivel de utilizator şi grupuri de utilizatori acordate în concordanta cu atribuţiile şi responsabilităţile fiecăruia.
- Definirea şi validarea unui flux de lucru unitar conform specificaţiilor ITIL dar şi conform proceselor organizaţiei pentru managementul mijloacelor fixe
- Administrarea fluxurilor de lucru în interfaţa grafică web în mod „drag-and-drop” cât şi în mod text prin constructor de expresii. Modulul grafic trebuie să pună la dispoziţia administratorului hărţile fluxurilor de lucru.

- Administrarea structurii soluţiei şi a bazei de date în interfaţa grafică web (application / database designer)
- Soluţia trebuie să permită definirea de şabloane ale activităţilor tipice de management al incidentelor, problemelor, ordinelor de lucru
- Soluţia trebuie să permită crearea unei scheme de utilizatori bazate pe grupuri şi roluri
- Soluţia trebuie să ofere posibilitatea de alocării responsabilităţilor în rezolvarea ordinelor de lucru în funcţie de organigrama instituţiei
- Soluţia trebuie să ofere posibilitatea de planificare şi urmărire a activităţilor necesare în vederea rezolvării sarcinilor de lucru
- Soluţia trebuie să ofere posibilitatea de planificare şi urmărire a activităţii de achiziţionare a activelor IT (mijloace fixe şi obiectelor de inventar)
- Soluţia trebuie să ofere posibilitatea de planificare şi urmărire a contractelor furnizor pentru achiziţii active (mijloace fixe)
- Soluţia trebuie să ofere posibilitatea de planificare şi urmărire a activităţilor de mentenanţă preventivă asupra activelor IT (mijloacelor fixe şi obiectelor de inventar)
- Soluţia trebuie sa ofere posibilitatea de a defini legături de precedenţă între comenzi de lucru şi task-uri. Soluţia trebuie sa iniţializeze în mod automat reţeaua de înregistrări rezultate, în care acestora li se aplică o acţiune „de la sfârşit la început", automatizând astfel fluxul schimbărilor de stare dintre înregistrări. De exemplu, dacă secvenţa de control a fluxului este activată la nivelul "plan de lucru" atunci toate sarcinile generate în momentul aplicării "planului de lucru" unei comenzi de lucru vor verifica dacă sarcina anterioară a fost finalizată. Dacă sarcina anterioară a fost încheiată, atunci statutul se modifică automat în „În curs de desfăşurare". Trebuie sa fie posibil ca nu orice sarcină succesivă să-şi schimbe statutul în „În curs de desfăşurare", până când sarcina imediat precedentă nu a fost finalizată. În momentul în care toate sarcinile sunt finalizate, starea comenzii de lucru poate fi schimbată în mod automat ca fiind „Finalizată".
- Soluţia va oferi posibilitatea de a îngloba "planurile de lucru" într-o relaţie ierarhică. Utilizatorii vor avea posibilitatea de a crea un "plan de lucru" care să facă referire la alt "plan de lucru". Acestea vor fi înglobate şi vor genera o ierarhie a comenzilor de lucru atunci când sunt aplicate unei comenzi de lucru (nu doar sarcinilor). Planurile de lucru sa poată fi înglobate la oricâte nivele este necesar.
- Modulul de "planuri de lucru" trebuie sa includă funcţia de adăugarea unui câmp "plan de lucru şablon" (template). Acesta va avea un domeniu asociat, prevăzut cu trei opţiuni:
  - Întreţinere,
  - Activitate,
  - Proces.

  Funcţionalitatea acestui câmp este să permită gruparea logică a planurilor de lucru, astfel încât interfaţa cu utilizatorul să poată fi modificată condiţionat.
- Soluţia trebuie sa ofere capabilitatea de a gestiona articole şi inventar pe baza unui set robust de reguli de stare şi capabilităţi. Utilizatorii trebuie sa poată urmări şi gestiona ciclul de viaţă al articolelor, de la creare până la ieşirea din uz, la fiecare dintre zonele funcţionale ale articolelor („Articol", „organizaţie", şi „inventar"). Înregistrările articolelor trebuie sa poată urma fluxul de lucru pentru a implementa un proces de afaceri sau un scenariu personalizat. De asemenea, trebuie sa suporte funcţii complete de stare pentru „unelte de lucru" şi „servicii".
- Soluţia trebuie sa ofere facilitatea de îngloba un flux de lucru înglobat de modificare a stării a fost adăugat aplicaţiilor Work Order. Pot fi definite relaţii de precedenţă între comenzi de lucru, activităţi şi sarcini. Controlul fluxului de lucru poate fi apoi setat în mod opţional într-una din aplicaţiile asociate planului de lucru sau comenzilor de lucru, pentru a guverna regulile de schimbare a stării dintr-o ierarhie şi/sau reţea de înregistrări. Înregistrările din fluxul de control sunt setate ca fiind în curs de desfăşurare

atunci când activităţile precedente lor sunt încheiate, îmbunătăţind graficul de lucru al responsabililor task-urilor alese, în scop de atenţionare, de exemplu. Înregistrările finalizate de pe o ramură a ierarhiei antrenează finalizarea până la părintele ramurii, mutând activitatea către următoarea fază eligibilă a proiectului. Înregistrările care au task-uri precedente nefinalizate nu pot fi configurate manual ca fiind în curs de desfăşurare, prevenind astfel începerea neprevăzută a sarcinilor care nu sunt finalizate.

- Soluţia trebuie să ofere posibilitatea de urmărire a timpilor de răspuns şi de rezolvare a problemelor si activităţilor (sarcinilor de lucru) prin grafice sau alerte (indici de performanţă - KPIs & SLAs)
- Soluţia trebuie să ofere posibilitatea de urmărire a fluxului de lucru de rezolvare a incidentelor cu stocarea structurată a informaţiilor referitoare la acţiunile desfăşurate
- Soluţia trebuie să ofere posibilitatea tratării diferite a incidentelor în funcţie de categoria la care se referă şi de impactul acestora asupra funcţionării organizaţiei
- Soluţia trebuie să ofere posibilitatea menţinerii şi regăsirii informaţiilor despre modul de rezolvare a diverselor tipuri de probleme
- Stocarea informaţiilor necesare în vederea realizării rapoartelor, analizelor şi previziunilor privitoare la ratele de defectare, tipurile de defecte, etc. referitoare la echipamentele care intră în componenţa sistemului de proces sau la componente ale acestor echipamente
- Soluţia trebuie să ofere integrarea nativă cu modulul pentru monitorizarea SLA-urilor în vederea asigurării unui nivel minim garantat al funcţionării sistemelor, echipamentelor şi aplicaţiilor asociate conducerii operative.
- Soluţia trebuie să ofere posibilitatea exportării, din orice meniu, de rapoarte în format Excel, fără instrumente specializate de raportare, printr-un singur click.
- Soluţia trebuie să permită şi să înregistreze nemodificabil toate operaţiunile care s-au executat pe un caz pe toata durata de viaţă a acestuia;
- Soluţia trebuie să dispună de mecanisme predefinite pentru implementarea funcţionalităţilor de Incident Management şi Problem Management.
- Soluţia trebuie să permită organizarea unei baze de date de informaţii (knowledge database), care să poată fi consultata în mod facil, diferenţiat pe profile de utilizator;
- Soluţia trebuie să înregistreze informaţiile intr-o baza de date relaţională.
- Soluţia trebuie să fie scalabilă atât din punct de vedere al numărului de utilizatori, cât şi din punct de vedere al volumului de date.
- Soluţia trebuie să fie uşor de exploatat astfel încât să fie minimizata posibilitatea de apariţie a erorilor umane şi să nu necesite o îndemânare speciala din partea utilizatorilor finali. Astfel:
  - Interfeţele grafice ale diferitelor componente trebuie să folosească acelaşi standard referitor la ferestre şi moduri de lucru, să fie unitare în structura, navigare şi funcţionalitate;
  - Trebuie să asigure o interfaţă prietenoasă utilizatorului, prezentându-i-se în orice moment instrucţiuni referitoare la activităţile pe care trebuie să le desfăşoare, posibilitatea de acceptare sau nu, facilităţi de navigare confortabilă utilizând mijloace naturale de căutare (meniuri bara, pop-up pull-down) şi să permită navigarea în toate modulele la care utilizatorul are acces fără deconectarea şi reconectarea utilizatorului;
  - Trebuie să permită autentificarea utilizatorilor o singura data, iar apoi să permită navigarea în toate modulele pentru care utilizatorul respectiv are atribuite drepturi de acces;
- Soluţia trebuie să dispună de un instrument de raportare specializat cu posibilitatea de generarea de rapoarte interactive
- Soluţia trebuie să permită ataşarea oricărui activ introdus de documente electronice (de diverse formate)

- Soluţia trebuie să poată trimite (inclusiv prin e-mail) mesaje de informare/avertizare către utilizatorilor;
- Soluţia trebuie să fie integrată cu soluţia de monitorizare de reţea şi SLA-uri astfel încât alarmele generate de acestea să deschidă automat incidente în soluţia de help-desk
- Soluţia trebuie să permită configurarea unor fluxuri de operaţiuni pentru rezolvarea cererilor de lucru în funcţie de tipologia acestora.
- Soluţia trebuie să permită utilizatorilor să consulte prin interfaţa web cererile de lucru de utilizatori din acelaşi grup şi stadiul rezolvării acestora, în acest fel existând posibilitatea reducerii redundanţei cererilor introduse;
- Soluţia trebuie să poată fi configurată, astfel încât să escaladeze automat cazurile în funcţie de prioritatea lor sau în situaţia în care acestea nu respecta condiţiile de calitate (timpul maxim admisibil pentru rezolvare);
- Soluţia trebuie să permită monitorizarea timpilor de rezolvare prin definirea de SLA-uri
- Baza de cunoştinţe a soluţiei trebuie să dispună de facilităţi de căutare după cele mai frecvente întrebări.
- Baza de cunoştinţe să permită supervizarea soluţiilor cazurilor dintr-o anumita categorie înainte ca acestea să fie disponibile pentru a fi transmise la client.
- Baza de cunoştinţe să permită definirea de drepturi diferite de acces la documentele publicate în funcţie de grupul de utilizatori.
- Soluţia trebuie să ofere posibilitatea extinderii şi management al configuraţiilor (Change and Configuration Management) pe aceeaşi platforma şi bază de date relaţională, fără configurare, doar prin activare. Prin urmare, soluţia trebuie să folosească un model de date şi o bază de date comună cu soluţia pentru managementul activelor (asset management) şi cea pentru managementul configuraţiilor (CCMDB). De altfel soluţia trebuie să ruleze fluxuri de lucru comune şi unitare în toate modulele menţionate.

Se vor include licenţe pentru soluţia de management a activelor IT, dimensionată de către Ofertant conform nevoilor identificate în analiza cerinţelor documentaţiei de atribuire şi corelată cu modul de licenţiere al producătorului propus, care să ofere suport pentru minim 8 utilizatori (implicaţi în managementului activelor IT) concurenţi.

4.3.2 Monitorizare a performanţelor aplicaţiilor

Soluţia/component de monitorizare a performanţelor aplicaţiilor trebuie să dispună de următoarele caracteristici:

4.3.2.1 Caracteristici generale

- Monitorizarea performanţei aplicaţiei (interacţiunii utilizatorilor cu aplicaţiile specifice) trebuie realizata prin captura traficului TCP prin metode pasive de tip network sniffing si total neintrusive.
- Soluţia pentru monitorizarea interacţiunii utilizatorilor cu aplicaţii specifice trebuie sa pună la dispoziţie metode de stocare a acestor informaţii capturate, iar managementul acestora trebuie sa fie automat.
- Soluţia trebuie sa fie capabila sa captureze si sa retina sesiunile HTTP/HTTPs si sa pună la dispoziţie un mecanism de playback prin care sa se poată derula sesiunile capturate.
- Soluţia trebuie sa fie accesibila într-o consolă web, fără instalare de plugin-uri si sa fie suportata minim de Internet Explorer, Mozila, Google Chrome, Opera si Safari.
- Sa permită crearea de panouri custom cu acces bazat pe roluri.
- Sa permită autentificarea integrata cu sisteme LDAP, dar cel puţin Active Directory, cu posibilitatea mapării utilizatorilor si a grupurilor din LDAP pe utilizatori si roluri din sistemul de monitorizare.
- Sa dispună de un mecanism de alertare bazat pe reguli.

- Sa dispună pentru fiecare tehnologie monitorizata de un set de reguli standard care sa poată fi customizate. De asemenea sa permită crearea de reguli noi.
- Sa dispună de un mecanism avansat de notificare si de acţiuni la apariţia unei alerte. Sa poată face alertare pe mail către recipienti aleşi in mod dinamic in funcţie de sistemele afectate, de serviciile de business din care fac parte respectivele sisteme, de perioada din zi (de exemplu alarmele care vin noapte sa fie trimise către persoana care este de serviciu).
- Sa permită executarea de scripturi automate la apariţia alarmelor (de exemplu sa poată elimina automat un proces care consuma 99% CPU si nu are ownerul “oracle”, sau “root”).
- Sa permită trimiterea unui trap SNMP la apariţia alarmelor.

4.3.2.2 Caracteristici funcţionale detaliate

- Înregistrarea cererilor end-to-end si a timpilor de reţea — Înregistrarea tuturor cererilor si răspunsurilor in aplicaţiile Web. Informaţia trebuie culeasa înaintea serverelor Web prin mecanisme de captura de trafic fără instalarea de pachete in serverele Web.
- Sa poată captura tranzacţii reale, sau sa reproducă tranzacţii simulate — Sa poată genera tranzacţii simulate pentru testarea performantei si disponibilităţii aplicaţiilor
- Sa poată analiza sesiuni individuale de activitate ale utilizatorilor pentru măsurarea performantei aplicaţiilor web - Sa captureze si sa stocheze sesiuni de lucru utilizator reale; sa reproducă sesiunea capturata din perspectiva utilizatorului final
- Sa poată monitoriza si alerta când anumite pagini sunt apelate si sa poată reproduce sesiunile derulate pe paginile monitorizate
- Sa dispună de capacitatea de a căuta sesiuni efectuate după cuvinte cheie din acestea
- Calcularea de timpi de răspuns ai sistemului (SLA) uri pe baza performantei — Formarea unor referinţe cu privire la timpii de acces si alertarea utilizatorilor când aceste valori sunt depăşite
- Maturatori detaliate geografic — Monitorizarea timpilor de răspuns defalcat pe locaţii geografice, sau alte grupări logice.
- Performanta serverelor Web si de aplicaţie — Monitorizarea serverelor Web şi de aplicaţie pentru metrici referitoare la configuraţia acestora: CPU, număr de servicii, număr de accese.
- Inspectare şi analiza de conţinut — Vizualizarea informaţiei exacte afişate în browser-ul utilizatorului final.
- Posibilitatea de a tria tranzacţiile — Captura si căutare în datele reale ale utilizatorilor pentru a putea vedea ce anume au făcut utilizatorii şi ce a răspuns sistemul. Posibilitatea de inspectare detaliata a detaliilor tehnice ale modului de interacţiune intre utilizator si aplicaţie.
- Replay de sesiune si tranzacţie — Posibilitatea de a reproduce exact activitatea unei sesiuni, sau a unei tranzacţii individuale. Posibilitatea de a găsi sesiunile si tranzacţiile pe baza filtrării după cuvinte cheie. Mecanismul de reply trebuie sa parcurgă pas cu pas paginile vizitate de utilizatori. La fiecare pagina trebuie sa se vadă modul in care utilizatorul a interacţionat: ce câmpuri a completat, ce opţiune a ales, ce link, sau buton a apăsat pentru a merge la pasul următor
- Reproducerea problemelor pentru Help-Desk — Posibilitatea de a asambla cu un singur click si de a trimite către help-desk detaliile unei sesiuni care a dat eroare
- Activitatea utilizatorilor trebuie capturată fără impact asupra serverelor – Metoda preferată de captura a sesiunilor utilizatorilor este network sniffing. Doar in acest mod se poate asigura impact zero asupra serverelor web.
- Soluţia trebuie sa permită filtrarea hit-urilor si gruparea acestora in funcţie de multiple criterii. De exemplu sa se poată grupa hit-uri după:

- DNS Time,
- Load Time,
- Page Completion Time,
- Processing Time,
- Redirect Time,
- Request Time,
- Response Time,
- TCP Time,
- Unload Time,
- Network Delay (ms),
- Page Back End Time (ms),
- Page Client Time (ms),
- Page End to End Time (ms),
- Hit Back End Time (ms),
- Hit Client Time (ms),
- Hit End to End Time (ms).

- Soluţia trebuie sa permită definirea de metrici suplimentare. De exemplu soluţia trebuie sa poată afişa numărul de accesuri pentru un hit, sau un grup de hit-uri.
- Soluţia trebuie sa permită definirea de situaţii de avertizare sau de eroare altele decât erorile normale HTTP. De exemplu, in pagina de login, daca se introduc valori greşite, soluţia va returna o pagina in care scrie "eroare la autentificare" fără a se genera vreo eroare HTTP. Se doreşte ca o astfel de situaţie sa poată fi identificata si marcata ca eroare.
- Soluţia trebuie sa permită eliminarea hit-urilor care conţin date sensibile in sensul in care acestea nu pot fi disponibile in interfaţa de căutare sau de playback
- Soluţia trebuie sa permită măsurarea timpilor care nu se regăsesc în traficul HTTP/S. De exemplu aplicaţiile Web 2.0 sau AJAX, paginile care au conţinut extern (care nu este in traficul capturat care au conţinut dinamic). Acest lucru poate fi realizat prin intermediul unor scripturi introduse in paginile web care prezintă interes.

Soluţia trebuie sa permită măsurarea performanţei experienţei (reale a) utilizatorului final în utilizarea aplicaţiilor web-based, astfel încât sa se poată optimiza performanta, îmbunătăţi capacitatea şi diagnostica rapid problemele. Se doreşte depăşirea limitărilor soluţiilor de monitorizare care urmăresc doar scenarii predefinite sau ale aplicaţiilor desktop-based care urmăresc numai un anumit subset de utilizatori în scopul concentrării pe urmărirea activităţii tuturor utilizatorilor, in timp real, permanent.
Se doreşte eliminarea valorilor de monitorizare diferite pe care le obţin operatorii aplicaţiilor informatice din instituţie, pe de o parte, si administratorii IT, pe de alta parte, pentru a se obţine o imagine completă a experienţei utilizatorului final, o strategie de monitorizare solida, precum si abilitatea de a identifica cele mai frecvente tranzacţii care performează ineficient.
Soluţia va permite setarea de alerte pe baza tranzacţiilor reale, precum şi analiza impactului de reţea şi web asupra experienţei utilizatorului final. Din punct de vedere funcţional, soluţia trebuie să îndeplinească următoarele cerinţe pentru atingerea scopului menţionat:

- Implementare rapida – dorim sa evităm interferenţa pe care un analizator de trafic ar aduce-o în fluxurile de date ale aplicaţiilor; de aceea, soluţia trebuie sa permită instalarea analizatorului pe un port de monitorizare pasiva, în faţa serverelor web sau de aplicaţii, însă in spatele firewall-ului pentru a putea fi protejat corespunzător. Din aceasta perspectiva, sistemul ar putea sa "vadă" fiecare pachet înainte de a ajunge la server si imediat după ce a ieşit, fără a interfera cu traficul normal.

- Performanta ridicata şi impact redus – soluţia nu trebuie sa producă nici un fel de impact asupra infrastructurii de reţea sau a aplicaţiilor. Se doreşte evitarea instalării de agenţi software sau programe, marcarea conţinutului web sau generarea de trafic de reţea adiţional. Sistemul trebuie sa poată începe monitorizarea, înregistrarea si analiza traficului utilizator imediat după instalare si configurare, fără a necesita arhitecturi suplimentare
- Vizualizarea completa a infrastructurii web – sistemul trebuie sa fie capabil sa examineze lanţul livrării de servicii din perspective variate, inclusiv utilizator final, server web, locaţia utilizatorului, situl web, pagina web, o succesiune de mai mult pagini, sau nivele de aplicaţie
- Rapoarte şi grafice personalizabile – sistemul trebuie sa dispună de o interfaţa grafica uşor de personalizat, destinata sa evidenţieze cauza-rădăcina a problemei de performanţă pe care o experimentează un utilizator. De asemenea, trebuie sa fie capabil sa asigure accesul facil la un set cuprinzător de metrici de performanta pentru fiecare componenta a lanţului de service delivery. Definirea de rapoarte personalizate, suplimentare care sa asigure corelarea si analiza măsurătorilor pentru resurse specifice ale infrastructurii web, ori maparea lor pe funcţionalităţi specifice de business, reprezintă o capacitate funcţionala de mare importanta.
- Alerte în timp real – sistemul trebuie sa dispună de funcţionalităţi de alertare care sa permită administratorilor si deţinătorilor de aplicaţii sa impună SLA-uri. Alertele trebuie sa poată fi definite pentru servere, pagini, situri specifice, ori alte resurse monitorizate, inclusiv tranzacţii utilizator si erori de conţinut.
- Vizualizarea sitului web prin ochii utilizatorului final – dorim ca soluţia agreată să fie capabilă să reproducă sesiunea de lucru a utilizatorului final, exact aşa cum este afişată in browser-ul acestuia. Justificam această cerinţă prin prisma faptului ca data fiind multitudinea de browsere, configuraţii ale terminalelor utilizator si elemente afişabile in paginile web, exista foarte multe situaţii in care operatorii help desk raportează o problema de navigare, problema care nu este detectată de administratorii de aplicaţii si a cărei sursă nu poate fi identificată. Este esenţial sa putem reproduce sesiunea exacta a utilizatorului final, astfel încât sa putem identifica exact configuraţia utilizată si momentul in care s-a produs eroarea.
- Oferirea unei vizibilităţi reale echipei de administrare – Erorile de aplicaţie intr-un site web de producţie sunt dificil de urmărit, atât din perspectiva timpului cat si din cea a alocării de resurse. Avem nevoie sa putem avea vizibilitate asupra disponibilităţii reale a siturilor web, sa putem vedea ce s-a întâmplat cu adevărat si sa putem determina exact unde cade responsabilitatea si sa diagnosticam sursa problemei.
- Oferirea unei vizibilităţi totale asupra siturilor web – a monitoriza o singura dimensiune a disponibilităţii aplicaţiilor web si a neglija layer-ul de interacţiune zilnica intre utilizatorii finali si aplicaţii reprezintă o problema critica. Este necesară furnizarea de capacităţi de “instant replay” care sa permită vizualizarea comportamentului utilizatorilor finali, precum si răspunsul exact al aplicaţiilor

Soluţia trebuie să ajute managerii IT si de aplicaţie sa înţeleagă nivelele acceptate ale serviciilor livrate către utilizatorii finali, pentru a asigura continuitatea afacerii in condiţii optime.

- Monitorizare şi corelare intre nivelul business si componentele de infrastructura,
- Monitorizarea tranzacţiilor şi corelarea intre ce face utilizatorul final şi comenzile care ajung la baza de date,
- Modelarea dependinţelor între aplicaţii,
- Detectare rapidă a cauzei primare a unei probleme şi rezolvarea acesteia.
- Soluţia trebuie sa permită integrarea cu orice server de aplicaţii Java, incluzând fără a se limita la, următoarele:

- IBM Websphere,
- Oracle WebLogic,
- Oracle SUN One,
- Apache Tomcat,
- Jboss AS,
- Oracle IAS.
- Microsoft IIS

Soluţia trebuie să fie capabilă să descopere automat aplicaţiile publicate în serverele de aplicaţii.
Soluţia trebuie să fie capabilă să descompună fiecare apel individual pana la nivel de metoda Java sau .NET si sa măsoare timpii de execuţie pentru fiecare din acestea
Soluţia trebuie să fie capabila sa ofere informaţii detaliate despre containerele Java:

- Detalii despre memorie (Heap, sau non-Heap),
- Detalii despre procesele "Garbage Collector",
- Detalii despre thread-uri.

Soluţia trebuie să ofere consumurile pentru fiecare cerere individuala, descompuse pe tehnologii:

- HTTP,
- Servlet,
- JDBC.

Soluţia trebuie să ofere pentru fiecare cerere individuala frazele SQL către bazele de date, inclusiv cu vizualizarea valorii variabilelor bind utilizate.
Soluţia trebuie sa prezinte intr-o interfaţă unitara aplicaţiile Java si .NET. Soluţia trebuie sa poată afişa sistemele Java sau .NET grupate pe sisteme, servere, aplicaţii, request-uri sau metode
Soluţia trebuie sa poată examina clasele monitorizate pana la nivel de obiect. Acest lucru ne va ajuta sa identificam obiecte care sunt utilizate si referite pentru perioada mare de timp (acest lucru făcând ca "Garbage Collector" să nu le curate).
Soluţia trebuie sa permită afişarea spaţiului ocupat in memorie şi durata de expirare a obiectelor pentru a putea identifica obiectele care ocupa permanent memoria serverului.
Soluţia trebuie să ofere un instrument care adresează proactiv aplicaţiile Java şi .NET si problemele de performanta legate de acestea. Totodată va dispune de o interfaţă intuitiva (cu capabilităţi drag-and-drop) care ajuta la administrarea mediului Java.
Soluţia trebuie să poată urmări request-urile unui singur utilizator în mediul J2EE sau .NET, de la cerere, componentă, metodă si până la variabile bind SQL trimire către baza de date.
Soluţia trebuie să poată monitoriza memoria heap, obiectele alocate şi activitatea "Garbage Collector" grupate după tranzacţie si utilizator pentru a identifica problemele de memorie.
Soluţia trebuie sa permită monitorizarea, controlul şi diagnosticarea echipamentelor de reţea, a serverelor, a sistemelor de operare si a altor echipamente de infrastructura IT. Soluţia va trebui sa gestioneze infrastructura ca si suport pentru aplicaţiile critice, din fiecare perspectiva, inclusiv vizualizarea nivelelor de servicii ale business-ului.
Suportul de management al infrastructurii va include sisteme de operare, echipamente de reţea, servere virtuale si maşini virtuale prin:

- Descoperirea automata a mediului fizic,
- Asigurarea suportului pentru ajustări in timp real in vederea asigurării unei performante optima la nivel de procesor, I/O, memorie, swap, procese, utilizatori,
- Interogarea fişierelor de log, cu căutarea si alertarea la apariţia unor pattern-uri stabilite,
- Managementul infrastructurii virtualizate,
- Managementul descoperirii si configuraţiei pentru servere de aplicaţii, servere de baze de date, servere web si echipamente de reţea.

Soluţia trebuie să poată captura starea întregii reţele prin monitorizarea în timp real a parametrilor funcţionali, alertarea asupra problemelor, raportarea detaliata si sa ofere un real suport pentru personalul IT in vederea remedierii problemelor de latine de banda, conectivitate, performanta a reţelei şi aplicaţiilor.
Soluţia trebuie sa ofere următoarele funcţionalităţi:

- Alertare avansata – sa notifice via e-mail sau SMS când performanţa se degradează, permiţând remedierea problemelor înainte să impacteze asupra experienţei utilizatorului. Alertele trebuie sa poată fi configurabile, sa suporte condiţii multiple si sa se raporteze la un baseline de performanta particularizat de aplicaţie pentru mediul informatic pe care îl monitorizează. Sa identifice si sa elimine alertele fals – pozitive.
- Monitorizarea aplicaţiilor – sa furnizeze vizibilitate in adâncime a proceselor ce rulează si contoarelor de performanta pentru aplicaţiile critice, serviciile de reţea si aplicaţiile web.
- Remedierea automata – sa poată lua automat masuri de restaurare a serviciilor, inclusiv restartarea aplicaţiilor si serviciilor Windows, sau sa restarteze serverele.
- Monitorizare de cloud – sa poată gestiona si monitoriza atât infrastructura locala, cat si mediile de cloud computing de la distanta, in aceeaşi interfaţă.
- Suport cross-platform – sa furnizeze monitorizare neintrusiva si fără încărcare asupra platformelor Windows, Linux sau Mac. In cadrul monitorizării, sa poată comunica informaţiile centrului de control, iar apoi sa livreze serviciile cerute.
- Monitorizare in timp real – sa furnizeze monitorizare in timp real si colectare de date, inclusiv in timpul procesului de depanare. Sa monitorizeze in timp real indicatorii de performanţă de pe routere, hub-uri, switch-uri, servere si aplicaţii.
- Interfaţa de lucru integrata – sa ofere o interfaţă web compatibila cu browser-ele comune, in interiorul căreia sa fie disponibile toate informaţiile critice, supraîncărcările de reţea si alertele de performanţă. De asemenea, sa permită efectuarea de setări soluţiei de monitorizare.
- Monitorizare wireless – sa poată monitoriza reţelele wireless. Sa centralizeze managementul reţelelor wireless distribuite, prin aplicarea de configuraţii comune si afişarea centralizată a datelor.
- Deployment facil – sa permită autodescoperire de echipamente, recunoaştere de echipamente descoperite si sa aibă capacitatea de a configura automat setul potrivit de instrumente de monitorizare pentru fiecare categorie de echipamente descoperite.
- Management de log-uri – sa poată colecta, analiza, alerta, raporta si arhiva loguri de evenimente de pe gazdele Windows, syslog de pe platformele UNIX/Linux si echipamente de reţea, precum si loguri de aplicaţie de pe serverele IIS si MS SQL.
- Suport pentru echipamente mobile – sa existe posibilitatea de a livra rapoarte si date de monitorizare către echipamente mobile.
- "Dashboard" de monitorizare – sa furnizeze o interfaţă de vizualizare tip dashboard, care sa conţină un set cuprinzător de date sumarizate privind performanta reţelei si a echipamentelor. "Dashboard-ul" trebuie sa fie uşor de customizat pentru a răspunde cerinţelor organizaţiei.
- Monitorizarea fluxului de reţea – sa permită vizualizarea si analiza in timp real a traficului de reţea. Sa stocheze datele de flux in vederea raportării istorice si optimizării capacităţii de reţea.
- Unelte de diagnostic – sa includă sau sa furnizeze suport pentru un set cuprinzător si centralizat de unelte de diagnosticare: utilitare de ping, mappere de porturi, managere de configuraţii echipamente, generatoare de trafic.
- Suport de tip "remote office" – sa furnizeze conectivitate securizata cu site-uri remote.

- Rapoarte asupra datelor colectate – sa permită generarea de rapoarte pentru toate datele colectate. Rapoartele trebuie sa poată fi exportate in formatele uzuale, tipărite sau expediate prin e-mail. Rapoartele trebuie sa poată fi generate ad-hoc sau un baza unui calendar. Prin rapoartele built-in, sa facă posibila analiza tendinţelor si planificarea capacităţii peste timp, in vederea anticipării cerinţelor de viitor.
- Acces bazat pe roluri – sa permită configurarea de conturi utilizator mapate pe roluri administrative.
- Backup de configuraţii – sa dispună de capacitatea de a realiza backup de configuraţie pentru routere si switch-uri.
- Suport pentru tehnologiile standard – sa suporte analiza de trafic personalizata pentru tehnologiile standard de pe piaţa, incluzând CISCO NetFlow si Juniper J-Flow. Sa ofere suport pentru minim: WMI, NetFlow, sFlow, J-Flow, SNMP.
- Managementul personalizat al monitorizării – sa permită setarea de politici de monitorizare aplicabile pe categorii de echipamente.
- SNMP enablement – sa activeze si sa configureze in mod automat SNMP pe echipamente in vederea includerii rapide in procesul de monitorizare a unor range-uri mari de echipamente.
- Suport pentru mediile virtualizate – sa descopere automat host-urile de virtualizare ESX si maşinile virtuale găzduite de acestea, si sa furnizeze statistici cheie din interiorul acestora: starea curenta, utilizare CPU / memorie / disc, precum si traficul pe interfeţe.
- Network mapping – Sa permită crearea de harţi de reţea actualizate in timp real.

Soluţia trebuie să sigure managementul sistemelor de operare eterogene pentru a furniza o abordare consistenta asupra unor date agregate. De asemenea, trebuie sa asigure managementul maşinilor fizice sau virtuale fără deosebire, dar si sa poată furniza un suport consistent pentru relaţia dintre un host de virtualizare si maşinile virtuale găzduite de acesta, precum si pentru relaţia dintre mai multe host-uri de virtualizare corelate.
Soluţia trebuie sa furnizeze grafice in timp real asupra proceselor cheie de sistem de operare, metrici si detalii ale metricilor de sistem destinate identificării momentului de început al unei probleme si a ajuta la izolarea cauzei rădăcină:

- Un model unificat pentru sisteme de operare eterogene, inclusiv colecţii agregate precum utilizare I/O pe sisteme multiple sau utilizare CPU agregata.
- Capacităţi grafice de diagnostic – vor putea fi vizualizate grafic, in timp real, procesele de baza pentru sistemele de operare, metrici si informaţii derulante in metricii de sistem pentru a servi la identificarea momentului apariţiei unei probleme si a ajuta la izolarea cauzei de baza.
- Colectarea a numeroase metrici – inclusiv si esenţial pentru utilizarea CPU, utilizatori top de sistem, disponibilitatea si consumul de memorie, top utilizatori I/O si tendinţe de dinamica a capacităţii.
- Monitorizarea conţinutului fişierelor log – vizualizarea evenimentelor de eroare din fişierele log OS si ridicarea de alarme când conţinutul unui eveniment corespunde filtrelor configurate.
- Monitorizarea activităţii de disc – informaţii despre nivelul de utilizare, capacitate, severitate, despre discuri si sistemele de fişiere.
- Verificări de sănătate ale grupurilor de procese – sa poată monitoriza acţiuni iniţiate de alte activităţi pentru previzionarea eşecurilor.

Soluţia trebuie să asigure maximum de flexibilitate în managementul infrastructurii de virtualizare, permiţând tratarea maşinilor virtuale ca si când ar fi echipamente hardware / software fizice. Scopul este de a adresa cu maxim succes administrarea si balansarea încărcării pe cele patru resurse de baza: procesor, memorie, disc si reţea ale unităţilor gazda; de asemenea,

de a depăşi limitările uneltelor de management native. Acestea fac dificila determinarea cauzei - rădăcină a unei probleme, mai ales in contextul in care datele sunt afişate in tab-uri multiple si sunt gestionate de servere de management disparate.
Pornind de la ideea ca performanta unei maşini virtuale si componentele sale de aplicaţie pot varia foarte mult in funcţie de performanta mediului de virtualizare ca întreg, si ca aceste infrastructuri sunt la rândul lor parte a unui întreg, dorim sa avem o viziune holistica, end-to-end a întregului mediu informatic, care sa includă si parametrii specifici ai infrastructurilor de virtualizare:

- O mai buna înţelegere despre cum impactează mediul virtual, livrarea serviciilor la nivel de aplicaţie – obţinerea unei vizualizări "de 360 de grade" asupra tuturor aplicaţiilor de la end-user la baza de date, si de la SL la infrastructura
- Determinarea cauzei rădăcină a unui incident sau problema înainte ca utilizatorii sa fie afectaţi.
- Urmărirea in timp a maşinilor virtuale pentru a înţelege impactul potenţial al acestora asupra aplicaţiilor si business-ului in general.
- O mai buna gestiune a alarmelor de pe maşinile virtuale si serverele fizice pentru un răspuns IT prioritizat
- Identificarea resurselor stocate si partajate intre maşinile virtuale pentru a preveni supra-alocarea si rezervarea nejustificata de resurse.
- Acolo unde se face referire la metrici sau criterii, ne referim la "W3C Navigation Timing interface" (sau echivalent) . Solutia trebuie sa utilizeze metricele standard suportate de toate browser-ele care suporta standardul "World Wide Web Consortium".
- Pentru fiecare set de hit-uri Solutia trebuie sa poata configura pragurile de alertare in functie de care se va calcul SLA. Acest lucru este necesar pentru ca timpii de raspuns vor fi diferiti de la o aplicatie la alta, sau chiar in interiorul unei aplicatii de la o sectiune la alta.

4.3.2.3 Alte funcţionalităţi

- Sa reducă timpul si efortul necesar gestionarii infrastructurii de virtualizare prin automatizare incorporata, fluxuri de lucru destinate remedierii alertelor, si administrare bazata pe context.
- Sa permită înţelegerea modului cum infrastructura suporta aplicaţii cheie si servicii de business, inclusiv abilitatea de a asocia costuri utilizării infrastructurii
- Sa suporte platforme hypervizor eterogene, minim VMWare si Hyper-V pe care sa le gestioneze intr-o singura consola comuna; de asemenea, sa permită gestionarea din aceeaşi consola, de multiple servere Virtual Center sau echivalent.
- Sa asigure managementul performanţei, sa măsoare capacitatea si sa livreze statistici pentru infrastructurile fizice si virtuale.
- Sa ofere o vizualizare holistica, multinivel a mediului virtual.
- Sa ofere modele bazate pe scenarii si alerte predictive pentru optimizarea si managementul infrastructurii.
- Sa furnizeze o interfaţă GUI de gestionare a întregului mediu virtual, cu vizualizări rapide ale marilor consumatori pentru fiecare resursa si posibilităţi de investigare rapidă.
- Sa permită investigarea proceselor client.
- Sa permită urmărirea asset-urilor si configuraţilor.
- Sa aibă funcţionalităţi de modelare a încărcării datorate migrărilor; sa modeleze utilizarea metricilor principali relativ la capacitatea gazdei destinaţie.
- Sa asigure managementul utilizării resurselor.
- Sa dispună de dashboard-uri de urmărire a performantei, capacitaţii, modificărilor, tendinţelor de previzionare si evenimentelor de infrastructura.

- Sa asigure monitorizarea sistemelor de operare fizice.
- Sa se integreze cu Virtual Center sau echivalent pentru extinderea monitorizării native.
- Sa dispună de abilitatea de a grupa maşinile virtuale si componentele in servicii pentru alinierea cu managementul de SL, end-user, infrastructura, baze de date, aplicaţii si reţea.

Se vor include licenţe pentru soluţia (incluzând toate componentele acesteia) de monitorizare a performanţelor aplicaţiilor, dimensionate de către Ofertant conform nevoilor identificate în analiza cerinţelor documentaţiei de atribuire şi corelate cu modul de licenţiere al producătorului propus, care să ofere suport pentru cel puţin 16 nuclee.

Notă: 1 nucleu = 1 core-procesor x86_64

4.3.3 Salvare şi restaurare centralizata a datelor

Soluţia de salvare şi restaurare a datelor trebuie să asigure o protecţie eficientă a datelor împotriva erorilor şi a dezastrelor prin stocarea copiilor de salvare şi arhivare pe medii de stocare "offline". Trebuie să fie un produs scalabil, putând asigura protecţia a mii de calculatoare pe care pot rula diverse sisteme de operare, de la laptop-uri la mainframe-uri, conectate prin internet, reţele WAN, LAN sau SAN şi să ofere posibilitatea de administrare centralizată prin Web, tehnici de stocare şi mutare inteligentă date şi automatizare bazată pe politici, pentru a reduce costurile de administrare şi impactul asupra computerelor si reţelei. Soluţia trebuie să dispună de următoarele caracteristici:

4.3.3.1 Caracteristici generale

- Administrare centralizată – web based,
- Suport pentru o mare varietate de hardware,
- Scalabilitate,
- Mutare şi stocare de date inteligentă,
- Automatizare bazată pe politici a proceselor de backup, arhivare şi restaurare,
- Capabilităţi pentru recuperarea în caz de dezastru,
- Capabilităţi de restaurare tip "bare metal",
- Capabilităţi de restaurare rapidă prin intermediul tehnologiilor de tip "captură continuă a schimbărilor de date la nivel de bloc" cu impact minim asupra sistemului de operare.

4.3.3.2 Caracteristici detaliate

- Soluţia trebuie să asigure salvarea şi restaurarea datelor şi arhivarea şi extragerea acestora
- Soluţia trebuie să permită efectuarea backup-ului doar pentru fişierele care au suferit schimbări de la ultimul backup şi pentru fişierele nou create. Pentru sistemul de fişiere FAT/NTFS, soluţia trebuie să fie capabilă de a salva doar porţiunea modificată a unui fişier.
- Administrarea soluţiei de backup trebuie să se poată realiza prin intermediul unei interfeţe web pentru mai multe servere de backup, indiferent de platformele pe care rulează acestea.
- Clienţii de backup trebuie să fie accesibili prin intermediul unei interfeţe web, astfel încât administratorii să aibă la dispoziţie un mecanism facil de operare de la distanţă.
- Soluţia trebuie să dispună de un model de administrare flexibil şi să permită accesul mai multor utilizatori (administratori şi operatori), fiecare cu nivel de autorizare diferit.
- Soluţia de backup trebuie să asigure copii de siguranţă pentru mai multe versiuni ale aceluiaşi fişier, astfel încât să ofere posibilitatea restaurărilor selective.

- Soluţia trebuie să fie capabilă de a şterge copiile de siguranţă ale versiunilor expirate ale fişierelor (în conformitate cu politica de backup) astfel încât să se elibereze spaţiu pe mediile de stocare (benzi).
- In cazul în care în timpul procesului de backup/restore conexiunea dintre client şi server se întrerupe, soluţia trebuie să fie capabilă de a relua acest proces din momentul întreruperii şi nu de la început.
- Securitate: soluţia trebuie să fie capabilă de criptarea datelor schimbate între client şi server în timpul procesului de backup/restore.
- Soluţia trebuie să permită setarea perioadelor de păstrare a datelor salvate, în funcţie de timpul la care a fost realizat backup-ul.
- Soluţia trebuie să conţină mecanisme de tipul "Bare Machine Backup & Restore" pentru cel puţin următoarele sisteme de operare: Windows, UNIX si Linux.
- Soluţia trebuie să ofere mecanisme de salvare şi restaurare pentru NAS fillere folosind protocolul NDMP.
- Salvare via SAN (Storage Area Network): datorita faptului că orice transfer de date în LAN se realizează prin protocolul TCP/IP (care este un protocol de nivel ridicat şi foloseşte intensiv resursele computerelor) facilitatea de salvare via SAN va reduce în mod considerabil şi impactul asupra resurselor. Soluţia trebuie să permită serverelor şi clienţilor care se conectează la SAN să folosească această conexiune directă cu mediul de stocare, astfel încât procesele de salvare/restaurare şi arhivare/dezarhivare să se desfăşoare prin intermediul SAN în loc de LAN, sau direct pe benzi sau în storage pool-ul de discuri al serverului. Soluţia trebuie să asigure salvare/restaurare fără încărcare LAN şi accesul clienţilor la librăria de benzi conectată la SAN
- Salvare / restaurare online baze de date: soluţia trebuie să asigure salvarea online (fără oprirea serviciilor) a bazelor de date incluzând cel puţin următoarele Oracle Database şi Microsoft SQL Server.
- Soluţia trebuie să permită restaurarea instantanee a datelor din aplicaţii precum Microsoft Exchange (la nivel de mesaj sau intrare in calendar), Microsoft SQL Server, Oracle, SAP, IBM DB2.
- Migrarea datelor: soluţia trebuie să ofere mecanisme de migrare automată, bazată pe politici, a fişierelor de date neutilizate sau utilizate rar de pe disc ("online") pe benzi ("offline"). Acest mecanism trebuie să fie transparent pentru utilizatorul final: fişierele migrate trebuie să fie vizibile pe mediul online (ca şi când ele s-ar afla fizic in acel loc) deşi fizic ele se afla pe medii "offline" (benzi).
- Recuperare în caz de dezastru: soluţia trebuie să ofere mecanisme pentru a automatiza restaurarea datelor de pe medii offline (benzi) în caz de dezastru.
- Soluţia trebuie să fie compatibilă cu cel puţin următoarele platforme (sisteme de operare): Windows (cel puţin 2003, 2008, 2012), Linux (cel puţin RedHat RHEL si Suse SLES), Oracle Solaris şi IBM AIX.
- Soluţia trebuie să suporte o mare varietate de medii de stocare, independent de producător pentru toate platformele suportate.
- Soluţia va utiliza o bază de date de tip relaţional pentru stocarea metadatelor şi a informaţiilor despre obiectele supuse operaţiunilor de salvare-restaurare.
- Soluţia va oferi suport pentru medii virtuale de tip VMware, prin integrarea la nivel hypervisor, fără a necesita instalarea unui agent de backup în fiecare maşină virtuală.
- Soluţia va oferi facilitatea de backup non-disruptiv la nivel de hypervisor, fără a afecta maşinile virtuale.
- Soluţia va oferi facilitatea de restaurare pe mai multe nivele de granularitate:
  - La nivel de fişier,
  - La nivel de volum,

- La nivel de maşină virtuală.

- Soluţia va oferi suport pentru salvare-restaurare rapidă şi eficientă la nivel de bloc folosind API-urile VMware vStorage pentru Protecţia Datelor şi de urmărire blocurilor care se schimbă (backup-uri incrementale şi „content aware”).
- Soluţia va oferi suport pentru descoperirea şi backup-ul automat al maşinilor virtuale nou create.
- Soluţia va oferi capabilitatea de distribuire a sarcinilor de backup către mai multe maşini de tip server virtual de backup în paralel.
- Soluţia va oferi mecanisme de compresie şi deduplicare (”Data reduction”) pentru eficientizarea utilizării reţelei şi a spaţiului de stocare.
- Serverul soluţiei de salvare-restaurare va oferi posibilitatea de replicare automată, incrementală, către un sistem aflat la distanţă (sistem “ţintă”), în scopul implementării unei soluţii de tip Disaster Recovery (hot standby). Se vor replica doar fişierele şi directoarele care nu există pe sistemul “ţintă” şi se vor şterge cele care au fost eliminate de pe serverul sursă. Multiple servere sursă se vor putea replica către un singur server “ţintă”. Comunicarea dintre sistemele sursă şi ţintă se va face prin intermediul unui protocol care va utiliza lăţimea de bandă disponibilă un mod optim.
- Soluţia trebuie să ofere un modul propriu de monitorizare a soluţiei de backup in ansamblu (server de backup, clienţi, dispozitive SAN, etc); vor fi disponibile rapoarte out-of-the-box pentru cel puţin următoarele tipuri de informaţii (modulul propriu de monitorizare a soluţiei de backup in ansamblu va fi inclus în soluţia de backup fără costuri adiţionale de licenţiere):
  - Informaţii clienţi de backup:
    - Detalii activitate client,
    - Istoric activitate client,
    - Recurenta activităţilor de backup,
    - Fişiere cărora nu s-a putut face backup,
    - Situaţia curenta a planificărilor activităţilor de backup,
    - Sumarul storage,
    - Rapoarte de tip Top N.
  - Informaţii server backup:
    - Detalii ale bazei de date server,
    - Resurse utilizate de server,
    - Throughput server,
    - Utilizare benzi,
    - Utilizare volume bandă,
    - Analiză capacitate utilizată.
- Datele culese de modulul de monitorizare vor fi păstrate într-o bază de date de tip Data Warehouse în scopul construirii de rapoarte istorice complexe, pentru determinarea tendinţelor şi planificare de capacitate. Baza de date Data Warehouse aferentă modului de monitorizare platformă backup, va fi inclusă în soluţia de monitorizare fără costuri adiţionale de licenţiere.
- Soluţia trebuie să genereze rapoarte cu privire la operaţiunile de salvare / restaurare. Modulul de raportare al soluţiei de backup (şi inclusiv pentru modulul de monitorizare al soluţiei de backup în ansamblu) va pune la dispoziţia administratorilor o soluţie de tip BI (Business Intelligence), cu ajutorul căreia se vor putea modifica rapoartele oferite out-of-the-box, sau se vor putea contrui rapoarte noi, în funcţie de necesităţile interne. Soluţia va fi disponibilă prin intermediul unei interfeţe web, şi va fi inclusă in soluţie fără costuri de licenţiere adiţionale. Rapoartele generate vor putea fi prezentate cel puţin în formatele: PDF, MicrosoftExcel şi HTML.

- Soluţia de backup-restore, soluţia de monitorizare a platformei de backup cât şi modulul de raportare trebuie să provină de la acelaşi producător şi să se integreze nativ, fără a necesita efort suplimentar de integrare.

Se vor include licenţe pentru soluţia de salvare şi restaurare centralizată a datelor, dimensionate de către Ofertant conform nevoilor identificate în analiza cerinţelor documentaţiei de atribuire şi corelate cu modul de licenţiere al producătorului propus, care să acopere un volum total de date de 20 TB.

4.3.4 Salvare si restaurare centralizata a serviciului director

4.3.4.1 Caracteristici generale

Se doreşte implementarea unei soluţii cu ajutorul căreia sa se poată efectua salvarea, respectiv recuperarea de Active Directory atat la nivel de serviciu director, cat si la nivel de obiect in AD.
Această soluţie trebuie să dispună ce următoarele caracteristici:

- Să reducă timpul de recuperare – Soluţia trebuie sa garanteze recuperarea online a obiectelor; disponibilitatea serviciului director trebuie sa rămână nealterată in timp, fără sa necesite restartare de controllere de domeniu sau izolare pe parcursul restaurării
- Să crească siguranţa in funcţionarea Active Direcotry – Soluţia trebuie sa ofere un mod flexibil si complet de recuperare a obiectelor. Obiectele şterse trebuie sa poată fi recuperate in integralitatea lor, cu toate atributele (inclusiv cele particulare, custom), SID-ul original si apartenenta la grupuri. Atât procedura de backup, cat si procedura de recuperare trebuie sa ofere simplitate si rapiditate, sa dispună de un mediu grafic de lucru si de mecanisme wizard-based
- Să furnizeze scalabilitate si performanta – Întrucât organizaţia noastră doreşte sa implementeze scenarii de recuperare in caz de dezastru cu recuperare in condiţii de indisponibilitate a serverelor având rol de domain controller si recuperare de pe conexiuni de backup lente, backup-urile realizate trebuie sa fie de dimensiuni reduse si sa poată fi centralizate pe un storage central
- Să reducă încărcarea administrativă – Procedurile de backup si recuperare trebuie sa poată fi derulate in timp scurt si sa poată fi efectuate de personal tehnic de nivel mediu. Procedurile de backup vor fi programate a se derula automat la intervale prestabilite, iar restaurarea trebuie sa se poata efectua de pe oricare din backup-urile stocate, folosindu-se o singura consola administrativa. Administratorii trebuie sa dispună de mecanisme de comparare si test a backup-urilor stocate
- Sa furnizeze rapoarte inteligente de activitate.
- Sa ofere suport pentru backup-ul si recuperarea Active Directory, AD LDS si Group Policy – Soluţia trebuie sa poată fi adaptata uşor mediilor eterogene AD / AD LDS, sa adreseze medii director mixte sau native Windows Server, cel puţin versiunile 2008 / 2008 R2/ 2012.
- Sa ofere automatizarea completa – Procedurile de backup de pe toate controller-ele de domeniu trebuie sa fie complet automatizate. Soluţia trebuie sa furnizeze centralizare de date si istoric de operaţiuni.
- Sa ofere recuperare la orice nivel – Soluţia trebuie să poată recupera atât Active Directory în întregime, cât si unităţi organizaţionale, obiecte din unităţi organizaţionale sau atribute de obiect existent, din backup-uri stocate de pe orice controller de domeniu.
- Recuperarea trebuie să se facă online si granular – Condiţia esenţială este ca procedura de recuperare sa nu necesite restartarea maşinilor sau serviciilor director, ori izolarea acestora. Obiectele director nu trebuie recreate in timpul restaurării de atribute (posibilitatea restaurării de atribute trebuie sa existe ca atare, fără a se apela la artificii

tehnice de recreare a obiectelor din backup-uri anterioare). Se accepta necesitatea izolării in cazul extrem de improbabil al unui defect la nivelul întregii scheme.

- Redundanta – Soluţia trebuie să permită restaurarea de obiecte dintr-un backup realizat pe un server care nu mai este disponibil.
- Toate procedurile de backup si recuperare trebuie sa poată fi implementate intr-o singura consola de administrare – Consola trebuie sa existe separat de aplicaţia in sine, pentru a putea fi accesata local de fiecare membru al personalului administrativ. Consola va dispune de un mediu grafic, wizard-based, care sa permită realizarea tuturor operaţiunilor administrative.
- Instalare si implementare uşoară – Soluţia trebuie sa poată fi implementata in mediul de producţie rapid şi să poată aduce beneficii imediat după instalare.

4.3.4.2 Caracteristici funcţionale

Soluţia trebuie sa realizeze in particular back-up centralizat complet de system state de pe toate controller-ele de domeniu din infrastructura Active Directory, eliminând orice posibilitate de downtime prelungit cauzat de coruperea sau modificarea necorespunzătoare a datelor director, de configuraţie sau Group Policy. Totodată, sa furnizeze capacităţi de restaurare completă, remote, online si granulara a datelor director – de la întregul forest pana la nivel de atribut de obiect. De asemenea, sa automatizeze toţi paşii manuali necesari unei restaurări de forest in cazul excepţional al unei coruperi de schema sau de baza de date AD. Pentru a limita si mai mult posibilitatea de a avea un downtime prelungit in caz de defect al domain controller-elor, chiar in cazul unei defectări la nivel hardware sau la nivel de sistem de operare, soluţia trebuie sa poată crea clone virtuale centrale securizate ale controller-elor de domeniu, care sa poată fi aduse temporar in online, replicate automat si puse la dispoziţia infrastructurii pe perioada unei posibile depanări a serverelor AD afectate.

Specific, soluţia trebuie sa poată:

- Restaura rapid, de la distanta, orice obiect sau atribut AD, in integralitatea sa si suplimentar funcţionalităţilor native de restaurare din repository-ul Active Directory.
- Restaura online, granular, date Active Directory, AD LDS si Group Policy.
- Realiza back-up-uri diferenţiale AD pentru a minimiza impactul asupra spaţiului, suportului de lăţime de banda si maximiza frecventa arhivarii.
- Introduce in carantina controller-ele de domeniu corupte pentru a preveni replicarea lor intr-un mediu nou restaurat, ori pentru a putea aduce in online copii virtuale actualizate ale acestora; duplicarea serverelor de AD intr-un mediu virtualizat trebuie sa permită ca in caz de nefuncţionare a oricăruia dintre ele, sistemele duplicate vor putea prelua sarcinile maşinilor nefuncţionale.
- Pune la dispoziţia administratorilor wizard-uri de restaurare de la nivel de atribut pana la nivel de forest, eliminând necesitatea utilizării uneltelor native in linie de comanda.
- Automatiza toţi paşii manuali necesari in restaurarea întregului forest in caz de corupere a schemei sau modificare improprii a acesteia.
- Elimina timpii pierduţi din cauza coruperii sau modificării improprii a datelor director, de configuraţie si Group Policy.
- Oferi administratorilor posibilitatea alegerii celei mai potrivite strategii de restaurare in caz de nevoie, inclusiv prin capacităţi de testare periodica a acestor scenarii.
- Restaura toate controller-ele de domeniu din forest simultan, dintr-o singura locaţie centrala.
- Realiza rapoarte comparative detaliate asupra tuturor obiectelor care au fost sterse sau modificate.
- Sa se integreze cu uneltele administrative AD – AD Users and Computers, AD Sites and Services, AD Domain and Trusts.
- Sa dispună de capacităţi flexibile de scripting cu Windows PowerShell.

Este obligatoriu ca funcţionalităţile extinse de restaurare descrise mai sus să fie asigurate prin integrarea cu funcţionalităţile native Active Directory, precum si cu soluţia de protecţie a datelor agreata. Respectiv, soluţia va trebui sa se integreze cu funcţionalităţile de:

- Backup centralizat la nivel de date, server, sisteme de operare si baze de date.
- Restaurare a serverelor dintr-o singura operaţie, fără a necesita reinstalarea sistemului de operare, serviciilor director si datelor succesiv.

De asemenea, în alegerea soluţiei optime se vor avea în vedere următoarele:

- Întrucât resursele administrative pe linie IT din ANFP sunt limitate, soluţia va trebui să suplinească activ efortul uman de backup si restaurare in cazul apariţiei unui incident, astfel să poată înlocui prin wizard-uri complete utilitarele de depanare nativă in linie de comanda - ce poate reduce bagajul de cunoştinţe tehnice pe care un tehnician alocat trebuie sa le consulte si sa le asimileze in vederea remedierii unui incident
- Soluţia de protecţie a datelor va dispune de următoarele caracteristici la nivel de interfaţă grafică:
  - Asigura o unica interfaţă grafică centralizata pentru managementul datelor director ce trebuie restaurate, indiferent de complexitatea incidentului care trebuie adresat,
  - Asigura wizard-uri liniare pentru întreg procesul de restaurare si comparare a datelor director,
  - Asigura remedierea la distanta a incidentelor director, inclusiv prin restaurarea online de date,
  - Asigura remedierea la distanta a coruperilor majore ale bazei de date director, inclusiv prin repornirea in modul DSRM a serverelor afectate si readucerea apoi in online a serviciilor director, in caz de nevoie – totul din aceasta consola unica centrala.
- Una din abordările ANFP pentru protecţia serverelor este asigurarea proactivă în vederea prevenirii apariţiei unui incident, si apoi remedierea sa intr-un timp cat mai scurt. Întrucât Active Directory este un serviciu cheie in cadrul organizaţiei, este critic sa se asigure o strategie funcţională, adaptat permanent, de recuperare in caz de dezastru. Pentru aceasta, soluţia va asigura următoarele capabilităţi:
  - Va asigura un mediu de test complet funcţional care sa permită verificarea cu regularitate a strategiilor de restaurare in caz de dezastru, astfel încât sa existe certitudinea ca in cazul unui dezastru, restaurarea se va putea face in câteva ore in loc de zile sau săptămâni,
  - Va permite elaborarea pentru mai multor strategii (planuri) de restaurare, si verificarea acestora in cadrul modulului de testare,
  - Va indica punctual motivele pentru care o strategie de restaurare poate eşua, precum si sa permită modificarea rapida a strategiei pentru asigurarea unui proces de restaurare coerent,
  - Va oferi posibilitatea alegerii celei mai bune strategii de restaurare intr-o situaţie data.
- Soluţia trebuie sa ofere facilitatea de a centraliza, cataloga si compara backup-urile efectuate.
- Soluţia va permite recuperare rapida, local si la distanta, a oricărui obiect sau atribut AD, respectiv restaurarea granulara a datelor Active Directory, AD LDS sau Group Policy.
- Soluţia va permite recuperarea rapida, local si la distanta, a unui domain controller in întregime, a Active Directory in integralitatea sa, sau chiar a întregului forest.
- Soluţia va asigura un mediu complet de testare a scenariilor de recuperare AD in caz de dezastru.
- Soluţia va permite construirea unui mediu de backup virtualizat complet al Active Directory, care sa conţină clone virtuale ale tuturor controller-elor de domeniu si care sa

poată fi ridicate la nevoie in online pentru a suplini funcţiile unui controller de producţie indisponibil.

- Soluţia va conţine in mod obligatoriu wizard-uri pentru principalele operaţiuni administrative AD, respectiv:
  - Backup de Active Directory sau controllere de domeniu distincte,
  - Restaurare online de date din AD,
  - Restaurare online de date din AD LDS,
  - Restaurare de Group Policy,
  - Reparare de system state pe un controller de domeniu, inclusiv baza de date AD si SYSVOL,
  - Extragerea datelor dintr-un backup creat anterior pentru operaţiuni de analiza si raportare,
  - Clonarea unui controller de domeniu dintr-un backup intr-un mediu distinct non-producţie.
- Sistemul de comparare sa adreseze detaliat toate obiectele care au fost şterse sau modificate, permiţând recuperarea rapida a informaţiilor.
- Soluţia trebuie sa se integreze cu uneltele administrative AD Users and Computers, AD Sites and Services, AD Domains and Trusts.
- Soluţia trebuie sa poată fi integrata cu sistemul actual de backup si recuperare a infrastructurii, inclusiv prin restaurarea din backup-uri de sistem realizate cu soluţiile terţe in producţie sau prin funcţionalităţi native Windows.
- Soluţia trebuie sa poată fi integrata cu alte aplicaţii ce adresează AD, prin customizare cu Windows PowerShell.
- Sa existe o baza de cunoştinţe la nivel de suport rezultata din îmbunătăţiri ale platformei si din experienţa implementării in medii de producţie diverse.
- Sa permită centralizarea backup-urilor din întregul sistem geografic intr-o locaţie unica de stocare.
- Sa existe un set de rapoarte predefinite, exportabile, care sa permită monitorizarea activităţii produsului si operatorilor.
- Sistemul trebuie sa fie scalabil, sa permită distribuirea pe medii geografice eterogene si in acelaşi timp sa asigure o administrare unitara, centralizata.
- Sistemul va permite implementarea granulara.
- Configurarea produsului trebuie sa fie bazata pe wizard-uri.

4.3.4.3 Caracteristici de arhitectura

- Soluţia trebuie sa ofere un management scalabil al serviciului director, putând gestiona multiple controllere de domeniu din site-uri diferite.
- Soluţia trebuie sa permită integrarea cu mediul director: sa existe/ruleze pe un server Windows si sa folosească arhitectura Active Directory a ANFP.
- Soluţia trebuie sa permită crearea de activităţi programate.
- Soluţia trebuie sa ofere un mecanism de încredere pentru a garanta integritatea si securitatea datelor.
- Soluţia trebuie sa ofere un mecanism de protejare a datelor stocate.
- Soluţia trebuie sa ofere o consola grafica unitara, wizard-based pentru derularea tuturor activităţilor de backup si restaurare.
- Soluţia nu trebuie sa impacteze sistemele monitorizate sau conexiunile de reţea.

4.3.4.4 Caracteristici de uzabilitate si interfaţare cu administratorii si operatorii de aplicaţie

- Toate operaţiunile efectuate pentru administrarea sau operarea in aplicaţie vor fi efectuate dintr-o consola administrativa unica.

- Consola va procesa automat autentificarea in aplicaţie, in baza credenţialelor de utilizator autentificat Windows.
- Consola va asigura un mediu grafic, vizual de administrare si operare.
- Consola va permite efectuarea de operaţiuni in Active Directory pe baza apartenentei administratorilor la grupul de securitate Domain Admins ori in baza delegărilor de permisiuni efectuate de un administrator de domeniu.
- Toate funcţionalităţile de administrare si operare prevăzute in caietul de sarcini vor fi asigurate de operarea in consola de management, si vor fi afişate in mod grafic, distinct pe categorii de acţiuni; interfaţa trebuie sa fie una deosebit de intuitiva si cu un nivel mare de uzabilitate.
- Consola va afişa in mod vizibil principalele operaţiuni administrative ce fac obiectul caietului de sarcini. Aceste operaţiuni vor fi in totalitate wizard-based.

Se vor include licenţe pentru soluţia de salvare şi restaurare centralizată a serviciului director, dimensionate de către Ofertant conform nevoilor identificate în analiza cerinţelor documentaţiei de atribuire şi corelate cu modul de licenţiere al producătorului propus, care să ofere suport pentru minim 140 de utilizatori.

4.3.5 Soluţie suport pentru audit de securitate

Pentru asigurarea conformităţii depline cu regulile de securitate interne ANFP şi standardele în domeniu se doreşte implementarea unei soluţii de investigaţie care sa sprijine ANFP la creşterea nivelului de securitate şi evitarea pierderii/scurgerii de date cu caracter confidenţial. Soluţia va facilita colectarea şi stocarea securizata a fişierelor tip log, raportarea şi alertarea de conformitate precum şi investigarea asupra neconformităţilor de securitate în ANFP.
Împreuna cu soluţia de securitate si gestiune acces (prezentată în documentul de faţă în capitolul ”Administrarea utilizatorilor şi controlul accesului”), soluţia de audit va asigura un management unificat al securităţii organizaţiei. De aceea, este cerinţa fundamentala ca soluţia de audit sa acopere întregul istoric de operaţiuni de administrare utilizatori şi să ofere informaţii consolidate asupra securităţii şi conformităţii organizaţionale. Soluţia suport pentru auditul de securitate va trebui să dispună de următoarele caracteristici:

4.3.5.1 Caracteristici generale

- Sa existe o evaluare permanenta a securităţii si conformităţii produselor la nivel de furnizor, prin raportarea la următoarele categoriile de securitate specificate de NIST 800 53 / ISO 27002 sau echivalent:
    - Evaluarea completa de securitate,
    - Dezvoltarea de cod si modele arhitecturale care sa acopere operaţiunile de securitate comune,
    - Pregătirea si supervizarea dezvoltatorilor pentru conştientizarea permanenta a problemelor de securitate a codului,
    - Evaluarea permanentă a vulnerabilităţilor in componentele terţe utilizate de soluţia agreata; aceasta procedura presupune ca eventualele corecţii de securitate sa fie aplicate in timp util,
    - Semnarea software-ului in cod digital pentru a preveni intruziunea,
    - Evaluarea metodelor de criptare a datelor in fluxurile operaţionale.
- Îndeplinirea de către furnizor a standardelor de securitate si conformitate prevăzute ca obligatorii prin lege
- Furnizorul soluţiei sa aibă implementate acele controale de securitate si conformitate care sa asigure îndeplinirea cerinţelor ISO 27001 sau echivalent.
- Sa fie asigurate funcţionalităţile necesare pentru:
    - Implementarea şabloanelor de software si hardware autorizate a rula in mediul informatic,

- Mentenanţa, monitorizarea si analiza de loguri de audit în integralitatea lor,
- Controlul utilizării privilegiilor administrative,
- Monitorizarea si controlul conturilor inactive,
- Protejarea împotriva furtului de date,
- Reacţia la incidentele de securitate.

Auditul de securitate va asigura automatizarea colectării log-urilor din entităţile fizice şi virtuale, va include un modul de alertare operaţională in timp real şi va furniza o platforma de investigaţii care să asigure un nivel de securitate optim prin evaluarea proactivă a riscurilor, furnizarea de rapoarte istorice pe orice perioada de timp si menţinerea unui control activ, permanent
Pentru a adresa cerinţele de conformitate definite în cadrul organizaţiei, soluţia agreata trebuie să poată îndeplini trei sarcini esenţiale:

- Setarea unui standard de baza al conformităţii si securităţii organizaţionale,
- Urmărirea activităţii utilizator,
- Alertarea asupra potenţialelor atacuri cibernetice.

Soluţia trebuie sa constituie un real suport pentru organizaţie in vederea auditului sistemului informatic. Pe baza suportului de produs si a informaţiilor furnizate de acesta, responsabilii de securitate vor trebui sa poată:

- Colecta date din mediul auditat si seta un standard de baza,
- Efectua modificările necesare pentru a acoperi minimul de cerinţe de securitate, care ar putea include delegare granulara de drepturi si segregare de responsabilităţi,
- Urmări activitatea zilnica a utilizatorilor,
- Asigura stocarea pe termen lung a tuturor datelor colectate,
- Pregătirea procedurilor de remediere, in caz de alertare asupra unor posibile devieri de la standard.

Soluţia va îndeplini toate cerinţele funcţionale care sa asigure auditul complet de securitate si conformitate in cadrul organizaţiei, îndeplinind sarcinile operaţionale necesare cu un minim de efort din partea personalului dedicate, adică:

- Să furnizeze colectare securizata a log-urilor de evenimente. Securitatea trebuie aplicata la sursa, la destinaţie si la transport.
- Să păstreze online cat mai multe date posibil; sa asigure stocarea flexibila a pana la 5 ani de date. Log-urile de evenimente vor fi arhivate si comprimate. Mecanismul de compresie cel mai eficient pentru datele online va avea un avantaj major.
- Să furnizeze o consola de raportare inteligenta. Sa dispună de un set semnificativ de rapoarte preconfigurate, dar sa permită totodată crearea facila de rapoarte noi. Aceste rapoarte sa poată fi redistribuite si exportate in formatele standard (PDF, XLS, TXT, CSV).
- Să furnizeze un modul de alertare configurabil. Alertele vor fi predefinite sau definite in cadrul implementării, si vor trebui sa poată fi mapate pe diverse scenarii; de asemenea, sa poată fi definite alerte pe evenimente corelate.
- Să furnizeze suport pentru conformitate, să dispună de mecanisme de răspuns la regulamentele interne şi externe, prin monitorizarea accesului la sistemele critice si detectarea activităţii neobişnuite.
- Să furnizeze automatizare completă a proceselor de colectare si normalizare de evenimente.
- Să monitorizeze activitatea utilizatorilor; sa colecteze si sa coreleze utilizatori si administratori si sa alerteze automat atunci intervin activităţi anormale.

- Să asigure integritatea log-urilor. Sa poată utiliza zone tampon pe sursele monitorizate, unde evenimentele sa fie duplicate la generare, astfel încât sa se evite posibilitatea de intervenţie umana asupra surselor de log-uri.
- Să asigure redundanta funcţională.
- Să furnizeze un mecanism de criptare si comprimare a datelor stocate, pentru un timp de retenţie nedefinit. Sa garanteze ca o data stocate, log-urile nu mai pot fi alterate in nici un mod.
- Să furnizeze capacităţi de analiza a anomaliilor; sa simplifice tendinţele activităţii de sistem si sa detecteze incidentele de securitate.
- Să permită customizarea colectării si raportării, pe baza de wizard-uri de configurare.
- Să permită managementul centralizat al agenţilor (instalarea si dezinstalarea automata si manuala a agenţilor).

Soluţia va dispune de următoarele capacităţi:

- Va furniza mecanisme de configurare ”wizard-based” care sa asigure conformitatea cu specificaţiile de securitate
- Va furniza management de evenimente mapat pe multiple site-uri si echipamente.
- Va permite colectarea logurilor de retea, de securitate, ale infrastructurii de virtualizare si de performanta a infrastructurii IT&C de pe toate platformele, cu sau fără agenţi:
  - UNIX / Linux,
  - Windows Server,
  - Infrastructuri HyperV si VMWare,
  - Echipamente cu capacităţi syslog,
  - Baze de date Oracle si MS SQL,
  - Aplicaţii personalizate,
  - Loguri de evenimente diverse in format text.
- Va asigura necesarul de audit pentru infrastructurile al căror audit native este deficitar sau inexistent: Active Directory, servere de fişiere si storage-uri, baze de date SQL, sistemul de mesagerie electronica.
- Va furniza capacităţi de management unificat al securităţii:
  - Scanare de vulnerabilităţi,
  - Detective si prevenire a intruziunilor,
  - Colectare de fluxuri in timp real.
- Va permite crearea facila de template-uri pentru includerea in procesul de monitorizare si centralizare a log-urilor non-standard.
- Va furniza un mecanism de încredere care sa garanteze integritatea si securitatea log-urilor pe parcursul colectării si transportului.
- Va furniza un mecanism de protecţie a datelor stocate. Aceste log-uri nu trebuie sa poată fi alterate de nimeni.
- Va furniza normalizarea log-urilor provenite din surse diverse, aducându-le la un numitor comun fără pierdere de informaţii.
- Va furniza un mecanism propriu de failover pentru componentele critice.
- Va asigura un impact minim asupra sistemelor monitorizate, colectarea trebuie sa poată fi efectuata cu sau fără agenţi. Alertarea trebuie implementata pentru toate platformele, independent de natura lor. Monitorizarea in timp real si alertarea vor fi de asemenea furnizate pentru sistemele pe care nu se pot instala agenţi (servere critice UNIX/Linux, routere, alte echipamente de reţea cu capacităţi de management).
- Va dispune de console de management, MMC şi/sau web-based.
- Se va integra cu sistemul de Active Directory existent pentru a permite granularizarea de roluri bazat pe Active Directory.

- Va dispune de un mecanism de raportare istorica, investigaţională. Mecanismul trebuie sa asigure o încărcare minima pe serverele de baze de date.
- Va avea o arhitectura modulara; va permite distribuirea modulelor astfel încât sa poată răspunde unor scenarii variate de implementare si sa scaleze unor cerinţe variate. De asemenea, scalabilitatea va asigura ca implementarea iniţială poate fi extinsa facil, fără reconfigurarea platformei.

Soluţia va colecta fişiere log şi evenimente la nivel regional şi va putea consolida la nivel central toate aceste fişiere log. In acest mod se vor asigura redundanta sistemului de log management şi utilizarea optima a lăţimii de banda prin programarea consolidării si centralizării logurilor in intervale de activitate redusa.
Întrucât colectarea, normalizarea si corelarea datelor sunt critice pentru succesul unui audit performant şi eficient, se vor respecta următoarele cerinţe:

- Să se poată colecta cantităţi mari de date folosind o arhitectura scalabila.
- Evenimentele sa fie stocate intr-o structura alta decât baza de date, pentru a minimiza cerinţele de stocare si pentru a permite stocarea datelor pentru cel puţin 5 ani. Aceste log-uri trebuie sa poată fi accesate in orice moment si importate selectiv intr-o baza de date pentru necesităţi de raportare, analiza si investigaţii.
- Evenimentele sa poată fi importate din arhive intr-o baza de date dedicata, pentru necesităţi de raportare programata si analize investigaţionale; importul sa poată fi granularizat in funcţie de necesităţi, inclusiv prin mecanisme automate, pentru a minimiza volumul de date asupra cărora se vor genera rapoarte.
- Să fie posibil accesul rapid la evenimentele stocate, cu costuri minime de spaţiu si fără a implica echipamente nesigure si lente cum ar fi benzile de backup.
- Să fie posibila filtrarea, arhivarea si criptarea log-urilor la sursa, pentru a minimiza impactul asupra reţelei si asigura securitatea datelor
- Să se poată derula căutări in evenimentele arhivate si sa se poată raporta pe baza unor criterii date.
- Să existe posibilitatea de granularizare detaliata a colectării.

Auditul serverelor partajate trebuie sa permită granularizare în cel mai mic detaliu, prin:

- Auditarea de partiţii, foldere sau fişiere distincte.
- Crearea de profile distincte de opţiuni de audit pentru fiecare server sau cale NTFS auditată.
- Auditarea de acţiuni distincte pe fiecare cale: scriere, modificare, ştergere, separat pe foldere si fişiere din folder.
- Auditarea activităţilor numai pe anumite tipuri de fişiere (pe extensie fişier) si filtrare după nume.
- Auditarea activităţilor administrative: creare si ştergere de folder partajat, modificare de permisiuni.
- Auditarea si raportarea asupra tuturor modificărilor pe fiecare server in timp real.

4.3.5.2 Caracteristici de raportare

Urmărirea activităţii utilizatorilor este critica pentru următoarele arii:

- Managementul utilizatorilor şi grupurilor,
- Accesul asupra fişierelor şi storage-urilor,
- Activităţile de logon si logoff,
- Activităţile administrative derulate asupra bazelor de date şi aplicaţiilor, inclusiv detectarea şi prevenirea de intruziuni.

Soluţia va dispune de următoarele capabilităţi:

- Să filtreze evenimentele colectate pentru a prezenta spre raportare numai acele evenimente necesare in rapoartele produse,
- Să optimizeze storage-ul pentru analize de date,
- Să furnizeze rapoarte predefinite, specifice problemelor; acestea sa fie prezentate in sursa deschisa pentru a putea fi customizate de personalul intern,
- Să furnizeze rapoarte conforme specificului nostru, care sa poată fi dezvoltate intern cu un minim de efort prin modificarea rapoartelor predefinite sau programarea de noi rapoarte intr-o interfaţă prietenoasa,
- Să dispună de posibilitatea customizarii rapoartelor, bazata pe o tehnologie standard de industrie,
- Să distribuie rapoartele către destinaţiile necesare: export in formatele comune, prin salvare pe disc sau expediere e-mail,
- Să poată fi uşor de generat si distribuit, in baza unei programări si bazat pe conţinut.

Pentru relevanţa raportărilor, sistemul de corelare a evenimentelor si raportare trebuie:

- Să asigure agregarea si afişarea contului utilizator in toate rapoartele, inclusiv in rapoartele generate din evenimente in care acesta nu este conţinut (de exemplu, evenimente care conţin numai adresa IP a staţiei de lucru),
- Să coreleze evenimente din surse situate geografic diferit sau din fusuri orare diferite.

In vederea derulării de analize investigaţionale, este cerinţa obligatorie ca soluţia sa include/furnizeze (în distribuţia ofertată) un portal care sa unifice toate sursele de date (evenimente de platforma, modificări in serviciul director, modificări de politici globale etc.) in rapoarte consolidate care sa reflecte nivelul de securitate si conformitate intern.
Portalul trebuie sa ofere o vizualizare consolidata a stării de conformitate organizaţională, utilizând informaţii din mai multe seturi de date diferite pentru a produce rapoarte integrate, consolidate de conformitate si securitate
Soluţia va prezenta în portalul de analiza investigaţională toate rapoartele predefinite sortate după tehnologie.

4.3.5.3 Caracteristici de alertare

Remedierea posibilelor violări de securitate si devieri de la conformitate pot fi posibile numai cu suportul unui mecanism de alertare inteligent, predefinit si complet customizabil.
Soluţia trebuie sa dispună de un mecanism de alertare asupra evenimentelor sensibile de securitate, cu posibilitatea de a crea noi alerte in baza unor politici flexibile. Noi reguli de alertare vor putea fi definite in baza unor criterii singulare, corelate sau de excludere, inclusiv:

- Eveniment singular – când un singur eveniment indica situaţia care necesita remediere,
- Evenimente corelate – când trebuie detectata o situaţie specifica, definita in termeni de evenimente care survin in aproximativ acelaşi timp,
- Cumul de evenimente – când trebuie detectata o situaţie in care acţiuni similare se derulează intr-o succesiune rapida,
- Lipsa unui eveniment – când se aşteaptă evenimente specifice intr-un anumit interval de timp sau intr-o anumita situaţie data, dar acest sau aceste evenimente nu mai au loc,
- Lipsa unui eveniment corelat – când trebuie urmărite situaţii sau procese in care acţiunile subsecvente nu mai au loc,
- Reguli particularizate – când se doreşte detectarea unei situaţii care nu poate fi definita prin celelalte modele de reguli.

Soluţia trebuie sa permită monitorizarea in timp real a sistemelor UNIX/Linux si echipamentelor de reţea, fără a avea nevoie de agenţi distribuiţi; de asemenea, sa permită monitorizarea in timp real a sistemelor Windows.

Sistemul de monitorizare in timp real va dispune de funcţionalităţi de confirmare si notificare. Sistemul va avea capacitatea sa notifice imediat administratorii asupra activităţilor de frauda si sa genereze acţiuni automate (dezactivarea contului utilizator compromis, anularea modificărilor frauduloase de permisiuni etc.) si va conţine o lista predefinita de alerte pentru a facilita implementarea de politici de securitate:

- Modificarea unui cont computer,
- Crearea unui cont computer,
- Ştergerea unui cont computer,
- Autentificare utilizator reuşită,
- Autentificare utilizator eşuată (cont blocat),
- Crearea unui cont utilizator,
- Ştergerea unui cont utilizator,
- Deblocarea unui cont utilizator,
- Membru adăugat unui grup,
- Membru şters dintr-un grup,
- Crearea unui nou grup,
- Ştergerea unui grup,
- Modificarea politicii globale de audit,
- Modificarea politicii de domeniu,
- Oprirea auditului,
- Adăugarea de drepturi administrative pentru un utilizator sau un grup,
- Ştergerea drepturilor administrative pentru un utilizator sau grup,
- Adăugarea unui membru intr-un grup administrativ,
- Încercarea de a modifica parola unui cont administrativ,
- Autentificarea reuşită in afara programului de lucru,
- Evenimente multiple de acces interzis,
- Evenimente multiple de autentificare eşuată,
- Tentative multiple de a modifica o parola,
- Evenimente de autentificare reuşită după un număr de autentificări nereuşite,
- Ştergerea unui log de audit,
- Salvarea unui log de audit.

4.3.5.4 Capabilităţi de audit

Sistemul de audit trebuie să ofere cel puţin posibilitatea de a efectua următoarele tipuri de audit, prin intermediul a două module, astfel:

Audit dedicat pentru Windows Active Directory

Modulul trebuie sa poată fi utilizat ca si platforma separata, furnizând astfel funcţionalităţi operaţionale suplimentare:

- Un motor de colectare in timp real a evenimentelor intr-o baza de date operaţională,
- Unelte de management pentru baza de date de audit,
- Baza de date operaţională are ca scop tinerea in online a datelor pana la 6 luni, fără a avea un impact major asupra serverului de baze de date,
- interfaţa client separata, care sa fie utilizata de administratorii de securitate ,
- Interfaţa client va include toate uneltele necesare administrării produsului,
- Interfaţa client va include un set predefinit de rapoarte si filtre in scop investigaţional.

În plus,

- Modulul trebuie sa extindă capacităţile de audit nativ Active Directory, cu scopul de a urmări activitatea utilizatorilor si administratorilor in detaliu, respectiv cine, când, ce,

unde a produs o modificare, de pe ce staţie, valoarea originala si cea curenta a tuturor schimbărilor; de asemenea, produsul trebuie sa poată urmări modificările aplicate asupra GPO.

- Modulul trebuie sa furnizeze un set predefinit de alerte inteligente, in timp real, când obiecte critice sunt modificate sau când sunt detectate anumite modele de schimbări.
- Modulul trebuie sa ofere un mecanism de protecţie împotriva modificărilor obiectelor critice din AD, cum ar fi ştergerea accidentala de unităţi organizaţionale sau modificarea setărilor in politicile de domeniu.
- Modulul trebuie sa poată urmări schimbările in nested groups.
- Modulul nu trebuie sa se bazeze pe logurile de audit native, dificil de activat si gestionat, si cunoscute ca producând informaţii incomplete si criptice de audit .

Audit dedicat pentru servere de fisiere si alte echipamente de stocare de fisiere

Modulul trebuie sa poată fi utilizat ca si platforma separata, furnizând astfel funcţionalităţi operaţionale suplimentare:

- Un motor de colectare in timp real a evenimentelor intr-o baza de date operaţională,
- Unelte de management pentru baza de date de audit,
- Baza de date operaţională are ca scop tinerea in online a datelor pana la 6 luni, fără a avea un impact major asupra serverului de baze de date,
- O interfaţă client separata, care sa fie utilizata de administratorii de securitate,
- Interfaţa client va include toate uneltele necesare administrării produsului,
- Interfaţa client va include un set predefinit de rapoarte si filtre in scop investigaţional.

Modulul trebuie sa înlocuiască capacităţile de audit nativ tip Object Access pentru servere Windows, cu scopul de a urmări in detaliu activitatea utilizatorilor si administratorilor pe serverele de fişiere, respectiv operaţiuni de citire, scriere, modificare, ştergere de fişiere, configurarea de foldere partajate si modificarea permisiunilor pentru cele existente.
Nu va fi acceptata nici o soluţie care foloseşte auditul Object Access pe maşinile gestionate. Object Access Audit este implicit dezactivat pe toate serverele si staţiile de lucru ale organizaţiei, datorita încărcării suplimentare semnificative pe care o aduce si dificultăţii in urmărirea evenimentelor generate.
Modulul trebuie sa permită configurarea de restricţii de acces distinct de mecanismele de partajare, securitate si moştenire specifice NTFS. Aceste configurări trebuie sa suprascrie permisiunile native.

4.3.5.5 Caracteristici de management unificat al securităţii

Modulul de management unificat al securităţii trebuie sa poată fi utilizat ca si platforma separata, si sa includă toate funcţionalităţile unei soluţii de securitate complete/integrate:

- Raportare si logging investigaţional pentru conformitate,
- Evaluarea vulnerabilităţilor, detectarea si prevenirea intruziunilor pentru managementul securităţii,
- Analize operaţionale si de investigaţii avansate,
- Un dashboard de evaluare in timp real al securităţii.

Arhitectura modulului trebuie sa permită o distribuire rapida si sa includă out-of-the-box toate funcţionalităţile necesare evaluării permanente de securitate.
Astfel, principalele funcţionalităţi pe care trebuie sa le aibă sistemul de management unificat al securităţii ce se livrează in cadrul prezentului proiect sunt următoarele:

- Funcţionalităţi IDS, care sa asigure detecţia si analiza in timp real a pachetelor de date din Internet, Intranet si segmente DMZ si evaluarea riscurilor de securitate.

- Posibilitatea creării de reguli de securitate care sa poată fi aplicate pe echipamentele de securitate ale Achizitorului.
- Actualizarea permanenta automata si manuala a aplicaţiilor software si a bibliotecilor interne privind vulnerabilităţile existente si descrierea vulnerabilităţilor din mai multe surse specifice dedicate, online.
- Scanarea periodica a reţelelor de date si infrastructurii IT&C a Achizitorului pentru identificarea timpurie a potenţialelor riscuri de securitate pe baza actualizărilor permanente ale surselor de informaţii online privind ameninţările cibernetice.
- Agregarea de date din mai multe surse, cum ar fi: echipamente de reţea, echipamente de securitate, servere cu funcţiuni dedicate (baze de date, web, proxy etc), echipamente desktop, aplicaţii antivirus etc.
- Prelucrarea si corelarea datelor, identificarea de atribute comune, de legături intre pachete de date si incidente de securitate sau de sistem, pentru a crea informaţii cu sens privind starea securităţii infrastructurii IT&C a Achizitorului.
- Alertarea imediata si programata a personalului de specialitate al Achizitorului cu privire la incidente de securitate identificate.
- Prezentarea sintetica si structurata a informaţiei in interfeţe tip panou de control (dashboard).
- Prezentarea structurata a informaţiei privind incidentele de securitate identificate, alertele ridicate, acţiunile întreprinse si pachetele de date, in rapoarte detaliate specifice.
- Respectarea, prin procedurile utilizate si mijloacele de prezentare a informaţiei, de standarde si norme specifice domeniului securităţii informaţiei.
- Arhivarea locala sau remote si păstrarea datelor pe termen lung, asigurarea de facilităţi privind analiza istorica a datelor, semnarea datelor cu semnătura digitala.
- Funcţionarea pe infrastructura dedicata proprie si pe baza de agenţi / senzori / standarde de transmisie a datelor, care sa asigure o încărcare minima pe infrastructura IT&C a Achizitorului.

Sistemul de detecţie a intruziunilor trebuie sa suporte următoarele cerinţe:

- Sa aibă o arhitectura scalabila, bazata pe senzori sau echivalent
- Sa detecteze toate tipurile de atacuri si vulnerabilităţi cunoscute pe următoarele nivele
  - La nivel de reţea (IDS):
    - concomitent pe mai multe segmente de reţea (minim 4 segmente), viteza per segment - 1 GBps,
    - sa includă o baza de date de atacuri cunoscute actualizabile automat zilnic,
    - sa includă un modul de detecţie a anomaliilor de trafic de reţea.
  - La nivel de sistem de operare (HIDS)
    - Sa monitorizeze registrii,
    - Să detecteze rootkit-urile,
    - Alertare si răspuns in timp real,
    - Verificare integritate fişiere critice la nivel de sistem de operare,
    - Lista modificări la nivel de file system (pe path-uri critice), la nivel de module de kernel rezidente, la nivel de useri si grupuri,
    - Să monitorizeze registrii,
    - Să detecteze rootkit-urile,
    - Alertare si răspuns in timp real,
    - Verificare integritate fişiere critice la nivel de sistem de operare,
    - Lista modificări la nivel de file system (pe path-uri critice), la nivel de module de kernel rezidente, la nivel de useri si grupuri.

- La nivel de reţea Wireless (WIDS):
    - Să monitorizeze retele 802.11a, 802.11b, 802.11g,802.11n,
    - Să detecteze programe interceptare activă a comunicaţiilor,
    - Să detecteze Access Point-uri neautorizate pe toate canalele de comunicaţie disponibile monitorizându-le pe fiecare in parte pe mai multe tehnologii disponibile (WIFI, Bluetooth),
    - Să monitorizeze traficul wireless atât stateless, cât şi statefull.

Sistemul de management unificat al securităţii trebuie sa ne ofere posibilitatea de a detecta vulnerabilităţile software de pe echipamentele noastre. Pentru detecţia acestor vulnerabilităţi, soluţia trebuie sa ne ofere următoarele capabilităţi:

- Raportare de vulnerabilităţi către administratorii de securitate si managementul acestora (sistem de ticketing).
- Descrierea vulnerabilităţilor din mai multe surse .
- Sugestii de remediere a vulnerabilităţilor.
- Integrare cu OSVDB.
- Posibilitatea efectuării scanărilor de vulnerabilităţi din mai multe puncte concomitent (senzori sau echivalent) si centralizarea într-un singur raport a rezultatelor.
- Rapoarte de comparare între 2 stări ale sistemului la momente diferite.
- Posibilitatea de predefinire a scanărilor in momente si zile .
- Management pentru false-positive.
- Generare de incidente de securitate in urma descoperiri de vulnerabilităţi.
- Baza de date de ameninţări actualizabila automat.
- Baza de date de vulnerabilităţi actualizabile automat.
- Sistem de gestiune a permisiunilor de securitate asupra activităţilor de evaluare de vulnerabilităţi
- Sistem de gestiune a permisiunilor de vizualizare asupra rapoartelor generate .
- Baza de date de adrese de reţea cunoscute ca potenţiale surse de atacuri (inclusiv actualizări).

Stabilirea gradului de risc al organizaţiei prin agregarea mai multor indicatori de risc cu următoarele capabilităţi:

- Graduri de risc diferite in funcţie de tipul de eveniment, prioritate si de activul software sau hardware.
- Riscul global al organizaţiei reprezintă starea de risc la care este supus sistemul informatic. Acesta trebuie calculat in funcţie de următorii parametri: pierderea furnizării unui serviciu, scurgeri de date, vulnerabilitatea sistemelor si confidenţialitatea sistemelor găzduite.
- Fiecare activ de reţea trebuie sa poată avea afişat nivelul general de risc, nivelul de vulnerabilitate, nivelul de disponibilitate.
- Panouri de control al riscului, personalizabile in funcţie de rolul operatorului si informaţiile de risc pe care utilizatorul este autorizat sa le vadă.
- Hărţi de risc per activ software sau hardware si per segment de reţea, personalizabile.

Sistemul de management unificat al securităţii trebuie sa includă un puternic motor de corelare. Acest motor trebuie sa aibă următoarele caracteristici:

- Să includă in motorul de corelare toate informaţiile generate/colectate de către sistemul de management unificat al securităţii.
- Să poată efectua corelare logica pe sursa hibrida, arhitectura recursiva, arhitectura ierarhica si sa includă definiţii flexibile pentru directive de corelare, inclusiv posibilitatea

definirii unui arbore de condiţii de corelare. Sa includă un set de complet de directive de corelare grupate pe tipuri de atacuri, si posibilitatea de a crea directive de corelare noi pe baza de wizard.
- Să permită intercorelare, respectiv prioritizarea sau deprioritizarea evenimentelor pentru care se cunoaşte nivelul de vulnerabilitate din zonele de detecţie si evaluare a vulnerabilităţilor.
- Să permită corelare pe baza de inventar.

Sistemul trebuie sa poată verifica daca activul atacat foloseşte sistemul de operare, serviciul sau aplicaţia pentru care atacul este conceput pentru înlăturarea falselor-positive:
- Sistemul trebuie sa poată face actualizare online de directive de corelare de la producător, cel puţin pentru regulile de corelare certificate, politicile predefinite, politicile de conformitate cu standardele de securitate.
- Sistemul trebuie sa poată crea diverse politici de corelare care sa trateze diferit evenimentele:
  - Să calculeze riscul pentru eveniment,
  - Să coreleze evenimentul,
  - Să trimită spre corelare evenimentul către un alt server,
  - Să execute diverse acţiuni: trimitere e-mail, execuţie de comenzi, stocarea evenimentelor, ridicarea de incidente de securitate, generarea de alarme si generarea de tichete de securitate.
- Alarmele trebuiesc administrate si rezolvate intr-un mod centralizat cu permisiuni pentru utilizatorii sistemului.
- Managementul alarmelor trebuie sa fie intr-o interfaţă web.
- Sistemul trebuie sa poată genera alarme de securitate din toate componentele (IDS, detectare de vulnerabilităţi, loguri etc.).
- Sistemul trebuie sa permită un număr nelimitat de alarme.
- Sistemul trebuie sa ofere istoricul modificărilor de stare ale alarmelor: ce componenta a trimis alarma, când a fost trimisă, ce administrator a văzut alarma şi când aceasta a fost rezolvata.
- Sistemul trebuie să conţină o baza de date ce conţine soluţii uzuale pentru anumite tipuri de incidente (similare).
- Sistemul trebuie sa poată prelua din surse externe a rezolvărilor anumitor tipuri de incidente (update pe internet).
- Sistemul trebuie sa suporte îmbogăţirea bazei de date cu soluţii adaptate propriilor sisteme si/sau generate din activitatea propriilor sisteme.

Sistemul trebuie sa includă un sistem de raportare care sa permită rapoarte generate pe baza tuturor informaţiilor colectate şi generate de sistem şi care pot include atât informaţii în timp istoric cat şi în timp real. În mod implicit, sistemul trebuie să includă peste 100 rapoarte şi sub-rapoarte clasificate în mai multe categorii (disponibilitate, securitate, analiza vulnerabilităţii etc) şi să permită utilizatorilor crearea propriilor lor rapoarte, inclusiv numai acele sub-rapoarte, care sunt de interes în ceea ce priveşte profilul de utilizator monitorizat şi nevoile specifice.
În funcţie de profilul sau si în conformitate cu permisiunile pe care le are, fiecare utilizator trebuie să poată crea rapoarte numai pentru acele active pe care le poate monitoriza.
- Sistemul trebuie sa includă un set de rapoarte predefinite, clasificate în următoarele categorii:
- Securitatea bazelor de date,
- Rapoarte din componente,
- Alarme,

- Incidente,
- Vulnerabilităţi,
- Disponibilitate,
- Statistici reţea ,
- Informaţii referitoare la patrimoniu si inventar ,
- Sistem de administrare incidente de securitate (ticketing) ,
- Rapoarte specifice pe standarde de securitate (ISO 27001 si PCI-DSS),
- Rapoarte pregenerate pe diverse perspective,
  - Administrare de securitate (rapoarte de securitate destinate administratorilor),
  - Conducere (rapoarte de nivel de risc, anomalii majore, rapoarte statistice de evenimente),
  - Auditori de securitate,
  - Administrativa – Rapoarte de inventar, de situaţie a activelor.

Sistemul va permite personalizarea rapoartelor şi crearea de rapoarte noi pe baza de wizard
Panouri de control:

- Sistemul va asigura mijloacele de afişare sintetica de informaţii in interfeţe de tip panou de control (dashboard).
- Fiecare utilizator al sistemului trebuie sa aibă posibilitatea sa îşi configureze propriul panou din interfaţa, inclusiv grafice sau indicatori care prezintă interes, în conformitate cu nivelul tehnic al utilizatorului şi permisiunile utilizatorului din cadrul sistemului.
- Un sistem pe baza de plugin-uri disponibile trebuie sa permită utilizatorilor să importe şi să exporte diferite obiecte pentru dashboard-ul fiecărui utilizator. Obiectele incluse în dashboard trebuiesc configurate cu uşurinţă folosind un wizard care permite, printre altele, includerea următorului conţinut:
  - Grafice si metrici dintr-un singur SQL query,
  - Conţinut HTML ,
  - Feed Atom / RSS,
  - Tabele predefinite,
  - Metrici,
  - Reprezentări grafice tip ”tag cloud”.

Se vor include licenţe pentru soluţia suport pentru audit de securitate (incluzând toate componentele/modulele acesteia), dimensionate de către Ofertant conform nevoilor identificate în analiza cerinţelor documentaţiei de atribuire şi corelate cu modul de licenţiere al producătorului propus, care să ofere suport pentru cel puţin 30 de echipamente tip server, 400 de echipamente tip client (desktop/laptop), permiţând accesul (şi lucrul) a cel puţin 1 auditor de securitate.

4.3.6 Suport Utilizatori

Soluţia de tip help-desk oferita va realiza gestionarea tuturor cerinţelor de service si suport ale Instituţiei. Aceasta soluţie va asigura administrarea problemelor apărute in cadrul instituţiei, escaladarea si transferul acestora, managementul alertelor si va oferi opţiuni avansate de căutare si raportare. Soluţia va dispune de următoarele caracteristici:

4.3.6.1 Caracteristici Generale

- Soluţia propusă trebuie sa se bazeze pe un pachet de soluţii software care sa ofere funcţionalităţi şi procese specifice pentru managementul şi administrarea incidentelor/ticketelor şi a relaţiilor cu solicitanţii.
- Soluţia propusă trebuie să includă modul de Service/Product Catalog fără costuri suplimentare, ca parte a împachetării de tip COTS – Commercial of the Shelf.

- Soluţia propusă trebuie să se bazeze pe un pachet de aplicaţii software disponibile comercial (tip COTS).
- Soluţia trebuie sa conţină funcţionalităţi proprii de securitate si audit.
- Soluţia trebuie sa includă funcţionalităţi avansate de securitate care în funcţie de roluri si drepturi, utilizatori sa nu poată vedea/accesa/modifica anumite câmpuri.
- Soluţia trebuie să poată funcţiona pe oricare dintre platformele software următoare: Windows, UNIX şi distribuţii majore Linux.
- Soluţia trebuie să poată utiliza sisteme de gestiune a bazelor de date ca: SQL Server, Oracle,. Specificaţi informaţiile privind certificările şi condiţiile de rulare pentru toate aceste sisteme.
- Soluţia ca partea a pachetului COTS trebuie sa includă baza de date si serverul de aplicaţii, fără costuri adiţionale.
- Accesul la soluţia de Help Desk trebuie sa se realizeze în întregime prin intermediul unei interfeţe WEB, accesibilă printr-un browser consacrat. Nu se admit soluţii tip client-server.
- Soluţia trebuie să ofere funcţionalităţi de help-online şi ghidare prin ecranele aplicaţiei.
- Soluţia trebuie sa aibă ca funcţionalitate COTS partea de knowledge management prin care orice ticket poate fi transformat într-un articol în componenta de knowledge management în aşa fel încât toţi utilizatorii sa poată vizualiza.
- Soluţia propusă trebuie să suporte minim următoarele procese ITIL v3: Incedent, Problem, Configuration, Change intr-o baza de date cu model unitar şi o aplicaţie unificată.
- Soluţia trebuie să includă COTS modul CMDB care sa aibă acelaşi model de date, structura şi baza de date ca Soluţia Help Desk şi să nu necesite integrări suplimentare cu aplicaţia de Service Desk/Service/Product Catalog.
- Ghidurile online de navigare şi operare trebuie să fie configurabile şi să se asigure posibilitatea dezvoltării de ghiduri noi.
- Ghidurile online de navigare şi operare trebuie să fie interactive îndrumând utilizatorul pas cu pas în efectuarea unei operaţii prin conducerea lui prin ecranele aplicaţiei care trebuie completate/actualizate.
- Pentru simplificarea procesului de învăţare/operare, ghidurile online de navigare şi operare trebuie să poată afişa porţiuni din ecranele care urmează a fi completate.
- Ghidurile online de navigare şi operare trebuie să permită afişarea continuă pe ecran a paşilor efectuaţi şi a celor care urmează a fi efectuaţi.
- Ghidurile online de navigare şi operare trebuie să permită salvarea şi reluarea proceselor întrerupte din locul în care au fost întrerupte.
- Soluţia trebuie să suporte reguli de business flexibile care pot varia conform unor factori multipli.
- Soluţia va oferi suport complet pentru orchestrarea de procese (workflow).
- Soluţia propusa trebuie să permită integrarea folosind servicii şi adaptări in conformitate cu standardele deschise, cum ar fi:
  - SOAP,
  - WSDL,
  - WS,
  - UDDI,
  - XML.

4.3.6.2 Caracteristici specifice

- Soluţia trebuie sa fie accesibila prin interfaţa web securizata.
- Trebuie să dispună de mecanisme predefinite pentru implementarea funcţionalităţilor de:

- Incident management,
- Problem management,
- Change management.

- Să fie uşor de exploatat astfel încât să fie minimizată posibilitatea de apariţie a erorilor umane şi să nu necesite o îndemânare speciala din partea utilizatorilor finali, astfel:
  - Trebuie sa asigure o interfaţa prietenoasa utilizatorului, prezentându-i-se in orice moment instrucţiuni referitoare la activităţile pe care trebuie sa le desfăşoare, posibilitatea de acceptare sau nu, facilitaţi de navigare confortabila utilizând mijloace naturale de căutare (meniuri bara, pop-up pull-down) si sa permită navigarea in toate modulele la care utilizatorul are acces fără deconectarea si reconectarea utilizatorului;
  - Sa permită introducerea incidentelor/ticketelor de către utilizatori prin interfaţa web de către operatorul serviciului de asistenta;
  - Sa permită ataşarea la incidentul introdus a documentelor electronice (de diverse formate);
  - Sa permită configurarea unor fluxuri de operaţiuni pentru rezolvarea incidentelor/ticketelor in funcţie de tipologia acestora.
  - Sa poată fi configurata astfel încât sa escaladeze automat incidentele/ticketele in funcţie de prioritatea lor sau in situaţia in care acestea nu respecta condiţiile de calitate (timpul maxim admisibil pentru rezolvare);
  - Sa permită monitorizarea timpilor de rezolvare;
  - Analiştii sa poată salva soluţiile propuse intr-o baza de cunoştinţe cu arborescenta pe subiecte, puncte de interes etc;
  - Baza de cunoştinţe trebuie sa dispună de facilităţi de căutare după cele mai frecvente întrebări şi să dispună de facilităţi de căutare in documentele ataşate (de exemplu fişiere de tip .pdf);
  - Funcţionalitatea de baza de cunoştinţe trebuie sa fie certificata KCS.
  - Sa ofere metoda de căutare a informaţiei de tip „arbore de decizie" in baza de cunoştinţe;
  - Baza de cunoştinţe sa permită definirea de drepturi diferite de acces la documentele publicate în funcţie de grupul de utilizatori;
  - Soluţia trebuie sa ofere posibilitatea reţinerii/înregistrării cererilor primite pe o varietate de canale de comunicare. Tratarea înregistrării trebuie sa fie aceeaşi indiferent de canal.
  - Un solicitant trebuie sa poată avea multiple incidente/tickete deschise simultan.
  - Soluţia trebuie sa ofere suport complet integrat pentru toate canalele de contact, inclusiv telefonic, e-mail, portal web.
  - Soluţia trebuie sa ofere capabilităţi de a alocare a incidentelor/ticketelor bazata pe capabilităţile angajaţilor.
  - Soluţia trebuie sa permită înregistrarea şi regăsirea istoriei complete de comunicare (mesaje recepţionate şi emise) a solicitantului, de pe toate canalele de interacţiune şi zonele de cereri, informări si servicii.
  - Soluţia trebuie să includă un sistem complet de gestiune a comunicărilor email permiţând gestionarea eficientă a volumelor mari de e-mailuri către şi de la solicitanţi (inbound/outbound) Toate e-mailurile trebuie asociate in mod automat cu profilul solicitanţilor.
  - Pentru tratarea interacţiunilor pe e-mail, interfaţa trebuie sa permită agentului să răspundă direct la e-mail, sa facă forward sau sa creeze un e-mail nou. De asemenea, trebuie să permită accesul la istoricul interacţiunilor cu acelaşi solicitant, astfel încât agentul să poată vizualiza întreaga lista de comunicări schimbate pana la momentul respectiv.

- Soluţia trebuie să ofere capabilităţi de parsing pentru emailurie inbound pentru diverse câmpuri cum ar fi expeditorul, corpul e-mailului, atributele emailului, în scopul procesării acestora.
- Trebuie oferită posibilitatea utilizării de şabloane pentru răspunsurile la emailuri.
- Soluţia trebuie să ofere mecanismele necesare colaborării controlate si a schimbului de informaţii on-line cu solicitanţii.
- Soluţia trebuie sa permită ca model de licenţiere un număr nelimitat de utilizatori care pot ridica tichete fără sa fie nevoie de licenţe pentru acest tip de utilizatori. Licenţierea va ţine cont doar de numărul utilizatorilor implicaţi în rezolvarea ticketelor (utilizatori de suport).
- Soluţia trebuie sa includă un tool inclus COTS, care sa aibă funcţionalitate de migrare/deployment a tuturor datelor/ecranelor/câmpurilor/fluxurilor definite in soluţie pentru a face migrarea la o versiune superioara sau deployment-ul pe medii de test si de dezvoltare facil.
- Soluţia trebuie sa fie ”Pink Certified” pentru toate procesele ITIL implementate.
- Soluţia trebuie sa permită integrarea cu capabilitatea care asigura infrastructura de fluxuri şi opţiunea de stocare a documentelor în acest sistem.

Se vor include licenţe pentru soluţia de suport utilizatori (help-desk), dimensionată de către Ofertant conform nevoilor identificate în analiza cerinţelor documentaţiei de atribuire şi corelată cu modul de licenţiere al producătorului propus, care să ofere suport pentru minim 8 utilizatori de suport concurenţi.

4.4 Infrastructură software de bază

Pentru a rula componentele infrastructurii de susţinere a lucrului cu fluxuri informatice şi ale infrastructurii de suport a activităţii de administrare pe componentele server (de aplicaţii şi de baze de date) ale infrastructurii hardware se va include o infrastructura software de bază compusă din:

- Sistem de operare tip server;
- Sistem relational de gestiune a bazelor de date.

4.4.1 Sistem de operare tip server

Sistemul de operare tip server va dispune de următoarele caracteristici:

Serviciu ”Director”:

- Suport pentru integrare cu serviciu de director si suport pentru:
  - Optimizarea fluxului de lucru al administratorului pentru găsirea rapidă a obiectelor din director,
  - Asistenţă mai bună şi mai eficientă în găsirea obiectelor în directoare mari,
  - Impact redus asupra serviciilor director în reţea,
  - Suport pentru implementare serviciu de director in virtualizare,
  - Suport pentru clonarea serverelor cu rolul de serviciu de director
  - Abilitatea de face o căutare în jos la o unitate organizatorică (OU - Organization Unit) din cadrul directorului,
  - Capacitate mai flexibilă de interogare pentru găsirea obiectelor în director, bazată pe atributele acestora.
- Serviciul de director pentru administrarea identităţilor trebuie să reducă complexitatea administrării directoarelor disparate, să scadă complexitatea asigurării redundanţei şi să crească calitatea şi accesibilitatea prin federalizarea mediului de director.

- Să permită folosirea structurii de director, constând din servicii de director pentru administrarea identităţilor şi servicii de meta-director în scopul îmbunătăţirii administrării.
- Serviciul de director pentru administrarea identităţilor va trebui să suporte LDAP sau echivalent.
- Serviciile de director pentru administrarea identităţilor trebuie sa suporte RFC 1823, ADSI, şi JNDI API.
- Aplicaţiile privilegiate de director pentru administrarea identităţilor trebuie sa fie capabile să obţină rezultate multiple, particularizate ale directorului pentru administrarea identităţilor.
- Monitorizarea, operaţiunile şi restaurarea directorului pentru administrarea identităţilor să poată fi delegate.
- Serviciile de director pentru administrarea identităţilor să poată suporta replicarea conţinutului.
- Serviciul de director trebuie să prezinte posibilitatea de modificare a topologiei infrastructurii, configuraţiei şi procedurilor operaţionale printr-un proces de administrarea a schimbării, iar modificările să poată fi delegate.
- Structura de director să poată fi administrate direct de un utilizator sau de aplicaţie .
- Sa ofere posibilitatea modificării accesului serviciului de director şi a procedurilor de administrare.
- Serviciul de director de management al identităţilor trebuie să aibă un singur root.
- Spaţiul de nume al serviciului de director pentru administrarea identităţilor să poată fi partiţionat într-un mod care sa reflecte sau nu structura organizaţională a organizaţiei.
- Convenţia de nume a organizaţiei să identifice unic persoanele folosind un identificator numeric unic ca valoare pentru atributul Relative Distinguished Name.
- Serviciul de director să permită adăugarea sau modificarea definiţiilor claselor de obiecte şi a topologiei spaţiului de nume.
- Serviciul de director să permită definirea politicilor de securitate.
- Serviciul de director trebuie să ofere posibilitate de acces anonim, acces cu autentificare simplă şi mecanisme puternice de autentificare prin LDAP.
- Să ofere posibilităţi de audit al accesului la serviciul de director şi al modificărilor aduse serviciului de director.
- Serviciul de director sa ofere abilitatea de a stoca certificate şi CRL-uri.
- Să asigure integrare cu serviciul de DNS
- Oferă posibilitatea de a efectua legături multiple prin Lightweight Directory Access Protocol pe o conexiune, în scopul autentificării utilizatorilor.
- Adaugă posibilitatea de a dezactiva comprimarea traficului de replicare între controlerele de domeniu care se află în situri diferite.
- Acceptă modificarea numelui DNS şi/sau numelui NetBIOS pentru domeniile existente într-un forest.
- Suport pentru dezactivarea definiţiilor atributelor şi claselor din schema Serviciului Director, astfel încât atributele şi clasele să poată fi redefinite dacă s-au strecurat erori la definirea iniţială.
- Oferă posibilitatea ştergerii obiectelor întârziate din Serviciul Director.
- Să permită administratorului Eliminarea restricţiilor RDN - Relative Distinguished Name incompatibile cu standardul de director X.500.
- Se permite memorarea şi reproducerea zonelor DNS memorate în partiţia de aplicaţie a Serviciului Director.

Fundaţie solidă:

- Să permită mutarea elementelor interactive din faza configurării în faza ulterioară instalării, eliminând interacţiunea administratorului la instalarea sistemului de operare;
- Sa ofere o interfaţă unică pentru configurarea şi monitorizarea serverului, cu programe de tip expert pentru optimizarea sarcinilor comune de administrare a serverului.
- Să ofere un nou shell opţional cu linie de comandă şi limbaj de script, ajută administratorii să automatizeze sarcinile de rutină de administrare a sistemului pe mai multe servere.
- Să ofere instrumente de diagnosticare puternice, care vă oferă vizibilitate permanentă asupra mediului serverului, fizic şi virtual, pentru a identifica şi rezolva rapid problemele care apar.
- Să permită administrarea serverului şi replicare a datelor optimizate pentru control îmbunătăţit al serverelor de la locaţii de la distanţă
- Să permită instalări minimale, în care sunt instalate numai rolurile şi caracteristicile de care aveţi nevoie, minimizând nevoile de întreţinere şi reducând zonele de atac de pe server.
- Să ofere un mijloc simplificat şi sigur de implementare rapidă a sistemului de operare Windows cu ajutorul instalării în reţea.
- Să conţină Internet Protocol versiunea 6 (IPv6), iar nodurile de clustere de la locaţii dispersate geografic sa nu mai trebuie să se găsească într-o subreţea cu acelaşi IP sau să fie configurate cu reţele locale virtuale (VLAN) complicate.
- Să ofere Network Load Balancing (NLB) si pe IPv6 şi include suport pentru mai multe adrese IP dedicate, care permite găzduirea mai multor aplicaţii în acelaşi cluster NLB.

Virtualizare:

- Să permită virtualizarea rolurile de server sub formă de maşini virtuale (VM) separate care rulează pe aceeaşi maşină fizică, fără a fi necesara achiziţia de software de la terţi.
- Să ofere replicarea maşinilor virtuale către gazde situate in locaţii la distanta; capabilitatea de replicare sa poată fi oferita intre gazde care sunt membri ai unui cluster sau gazde independente.
- Să ofere replicare maşinilor virtuale si datelor de pe un echipament de stocare pe celalalt.
- Suport pentru arhitecturi de tip NUMA in interiorul maşinilor virtuale.
- Suport pentru minim 320 procesoare logice şi minim 4 TB memorie la nivelul gazdei.
- Suport pentru minim 64 procesoare virtuale si minim 1 TB memorie la nivelul maşinilor virtuale.
- Suport pentru clustere cu minim 64 de noduri si minim 8000 de maşini virtuale.
- Suport pentru disc virtual în maşină virtuala pana la 64 TB de informaţie.
- Suport pentru minim 1024 de maşini virtuale pe o gazda.
- Să se poată implementa mai multe sisteme de operare – Windows, Linux şi altele – în paralel pe un singur server.
- Să ofere clustering-ul gazdelor sau al maşinilor virtuale care rulează pe gazde WSv şi backup-ul maşinilor virtuale în timp ce acestea rulează.
- Să permită programelor accesate de la distanţă să fie deschise cu un singur clic şi să fie utilizate ca şi cum ar rula pe calculatorul utilizatorului final.

Web:

- Să conţină un design modular şi opţiuni de instalare ce permit numai instalarea caracteristicilor strict necesare, reducând zonele de atac şi simplificând administrarea actualizărilor.
- Să permită copiere setărilor site-urilor Web pe mai multe servere Web, fără a fi necesară configurare suplimentară.

- Să ofere administrarea delegată a aplicaţiilor şi a site-urilor pentru control personalizat asupra diferitelor componente ale serverului Web.
- Să conţină administrarea integrităţii serverului Web, alături de instrumentele complexe de diagnosticare şi depanare ce permit vizibilitatea şi urmărirea cererilor care rulează pe serverul Web.
- Izolare îmbunătăţită a pachetelor de aplicaţii menţine site-urile şi aplicaţiile izolate, crescând securitatea şi stabilitatea.
- Suport CGI mai rapid pentru rularea aplicaţiilor PHP, a script-urilor Perl şi a aplicaţiilor Ruby.
- Integrarea strânsă cu funcţiile ASP.NET şi o locaţie de stocare a configuraţiei pentru toate setările configuraţiei platformei Web
- Să ofere suport pentru protocol HTML 5 si WebSocket
- Să ofere un depozit central pentru stocarea certificatelor digitale folosite pentru protecţia site-urilor web.
- Să ofere administrare la distanta pentru mai multe servere web dintr-o singura consola
- Să ofere posibilitatea de a găzdui servicii web in regim partajat de tip „multi-tenant" pentru mai multe site-uri web in regim de izolare
- Să ofere posibilitatea de a măsura consumul de resurse al serverelor web partajate
- Să ofere posibilitatea de a limita consumul de resurse de procesor, memorie sau lăţime de banda consumate de serverul web
- Să ofere suport pentru arhitecturi de tip NUMA cu suport pana la 128 CPU core.
- Să ofere un model de extensibilitate flexibil permite personalizarea, cum ar fi adăugarea de module noi utilizând cod nativ sau administrat.

Securitate:

- Să ofere un mecanism ce asigura că reţeaua şi sistemele nu sunt compromise de calculatoare virusate, izolând şi/sau depanând calculatoarele care nu se conformează politicilor de securitate pe care le-aţi stabilit.
- Să ofere un mecanism de protecţie împotriva aplicaţiilor periculoase.
- Să ofere flexibilitate criptografică crescută, suportând algoritmi de criptare standard şi definiţi de utilizator, permiţând crearea, stocarea şi preluarea mai facilă a cheilor criptografice.
- Să permită o metodă mai sigură pentru autentificarea locală a utilizatorilor de la sucursale şi birouri de la distanţă, cu ajutorul unei replici read-only a bazei de date AD principale.
- Să permită stabilirea mai simplă de relaţii acreditate între parteneri cu directoare de identităţi şi de acces diferite care rulează în reţele diferite, permiţând conectarea unică (SSO) în reţele.
- Să conţină un modul pentru monitorizarea stării autorităţilor de certificare (CA).
- Să conţină un serviciu pentru prevenirea scurgerilor de informaţii confidenţiale din interiorul organizaţiei către exterior prin intermediul fişierelor.
- Să ofere protecţie îmbunătăţită împotriva furtului de date şi a expunerii hardware-ului serverului dacă este pierdut sau furat, oferind ştergere mai sigură a datelor când renunţaţi la servere.
- Să ofere sistem de clasificare a informaţiilor pentru informaţii partajate cu configurarea automata a politicilor de acces prin politici de grup aplicate prin intermediul serviciu.

Alte capabilităţi:

- Suport pentru minim 320 procesoare logice.
- Suport pentru minim 4 TB memorie.

- Suport pentru minim 2048 de procesoare virtuale.
- Suport pentru clustere cu minim 64 de noduri.
- Suport pentru redundanta la nivelul plăcii de reţea cu pana la 32 de placi de reţea în regim de „teaming”.

Se vor include licenţe pentru sistemul de operare tip server, dimensionate de către Ofertant conform nevoilor identificate în analiza cerinţelor documentaţiei de atribuire şi corelate cu modul de licenţiere al producătorului propus, care să ofere suport pentru rularea a cel puţin 8 instanţe virtualizate pe fiecare din serverele de aplicaţii şi a cel puţin 2 instanţe virtualizate pe fiecare din serverele de baze de date incluse în infrastructura hardware (ofertată).

4.4.2 Sistem relaţional de baze de date

Sistemul relaţional de baze de date va dispune de următoarele caracteristici:

- Sistemul relaţional de baze de date trebuie sa ofere un suport implicit scalabil, disponibil si sigur pentru baze de date relaţionale, incluzând instrumente integrate de raportare si analiza, business intelligence, consolidare / integrare de date, si Data Mining.
- Sistemul trebuie sa includă in mod nativ o platforma care să permită procesarea complexa a evenimentelor, consistenta a datelor in medii heterogene, facilităţi avansate pentru dezvoltare si servicii proprii de Business Intelligence (self-service BI).
- Disponibilitate ridicata şi mentenanţă :
  - Posibilitatea efectuării backup-ului in multiple fişiere simultan pentru a putea efectua operaţia pe discuri diferite in paralel,
  - Posibilitatea efectuării backup-ului direct intr-o soluţie de cloud public, respectând normele de securitate.
- Raportare consolidata şi managementul depozitelor de date:
  - Depozit de date relaţional si instrumente OLAP: sistemul sa ofere in mod nativ soluţii OLAP si data warehouse;
  - ETL (Extract, transformation, load): funcţionalităţi native de extragere a datelor din diferite surse de date (SQL Server, Oracle, Excel, Web services), realizarea de filtrări, agregări si diferite alte transformări asupra datelor şi în final stocarea datelor în data warehouse.
  - Baze de date multidimensionale native: stocarea datelor intr-un cub cu mai multe dimensiuni, in vederea interogării mai uşoare a datelor si construirii rapoartelor relevante.
  - Posibilităţi de raportare din surse de date cum ar fi: liste SQL Server, Oracle, SQL Server Analysis Services, SAP NetWeaver BI, Hyperion, Sharepoint List, Teradata, SQL Azure si SQL Server Parallel Data Warehouse , XML
  - Posibilităţi de raportare cu moduri multiple de vizualizări: hărţi, sparklines si indicatori.
    - Hărţi: Posibilitatea de creare de rapoarte folosind Map Wizard care permite vizualizarea datelor sub forma unui model geografic care poate prelua datele dintr-o galerie de hărţi pe baza de interogări SQL sau dintr-un fişier stocat in sisteme tip ESRI. Elementele dintr-o harta pot fi poligoane (pentru reprezentare de arii), linii (pentru reprezentarea de rute si drumuri) si puncte (reprezentând locaţii diverse). Se pot adăuga date adiţionale de afişare sau atenţionări interactive folosind hărţi online.
    - Sparklines: Posibilitate de creare rapoarte folosind tabele si matrici pentru a afişa date agregate.
    - Indicatori: Posibilitatea de vizualizarea a datelor intr-un mod rapid folosind metode grafice (icoane).

- Raportare “ad hoc”: utilizatorii sa poată edita propriile rapoarte pe baza unui model (template), fără să deţină cunoştinţe de baze de date sau despre structura acestora. Serviciile de raportare sa fie incluse în produs, fără add-on-uri suplimentare.
- Interogare si analiza ad-hoc si self-service a datelor: facilităţi de interogare a datelor disparate in momentul solicitării rapoartelor.
- Extragerea si editarea dinamica a rapoartelor utilizând instrumente familiare de tip Office (i.e. Microsoft Excel) si interfeţe noi intuitive si productive care includ hărţi, sparklines si indicatori.
- Să permită exportarea rapoartelor in Excel, fisiere CSV, o alta baza de date, fişiere XML,
- Să permită exportul in documente tip PDF, TIFF.
- Să permită exportul datelor intr-un feed de date folosind serviciul Atom.

- Gestionare facila a obiectelor bazelor de date:
  - Instrumente de dezvoltare a obiectelor din baza de date: soluţia trebuie sa ofere unelte de dezvoltare pentru modulele ETL (Extract, Transform, Load), pentru design-ul bazelor de date atât relaţionale cat si multidimensionale, pentru design-ul rapoartelor.
  - Unelte pentru administrarea bazelor de date si a proceselor uzuale care se executa asupra bazelor de date precum si al rapoartelor.
  - Posibilitatea de definire si gestionare a obiectelor bazei de date (tabele, indecsi, proceduri stocate, triggere) direct din instrumentele folosite de dezvoltatori pentru scrierea aplicaţiilor.
  - Loc central care oferă posibilitatea administrării entităţilor de date şi ierarhiilor din multiple baze de date cu posibilitatea versionării.

- Performante ridicate ale sistemului de baze de date:
  - Auditarea operaţiilor: auditarea trebuie să includă informaţii despre momentul în care au fost citite datele, în plus faţă de orice modificare a datelor. Produsul trebuie să ofere caracteristici precum configurarea îmbunătăţită şi managementul auditurilor în server. Produsul să definească specificaţiile de audit în fiecare bază de date, astfel încât configuraţia auditului să poată fi adaptată pentru diversele bazele de date.
  - Colectarea datelor de performanţă: facilităţi de optimizare şi depanare a performanţei server-ului de baze de date, pentru a furniza administratorilor o perspectivă interactivă cu privire la performanţă.
  - Sistem de monitorizare extins al evenimentelor: sistem general de tratare a evenimentelor la nivel de server prin captarea, filtrarea şi reglarea evenimentelor generate de procesele de server. Evenimentele trebuie sa poată fi captate si exportate in diferite formate de ieşire, inclusiv Event Tracing for Windows (ETW), pentru corelarea cu aplicaţiile sistemului de operare şi ale bazelor de date, permiţând astfel o monitorizare completă a sistemului.
  - Comprimarea backup-urilor pana la 60%: menţinerea online a backup-urilor pe disc este o operaţie scumpă şi laborioasă, astfel încât este necesara implementarea unei soluţii de comprimare rapida a backup-urilor bazelor de date.
  - Asigurarea continuităţii activităţii organizaţiei: duplicarea datelor prin tehnologii de tip data mirorring.
  - Livrarea automata a log-urilor bazei de date către Data Recovery Center.

- Implementarea structurilor de date complexe:
  - Posibilitatea nativa de modelare a structurilor de date de tip arbore: metode încorporate pentru crearea şi operarea pe noduri ierarhice.

- Posibilitatea stocării datelor binare mari, precum documente şi imagini, ca parte integranta a bazei de date, păstrând în acelaşi timp consecvenţa tranzacţională.
- Căutare complexa la nivel de text, folosind indecsi specializaţi; efectuarea rapidă a căutărilor în acest tip de date.
- Managementul performant al coloanelor cu valori rare: modalităţi eficiente pentru administrarea spatiilor necompletate dintr-o bază de date relaţională, astfel încât valorile de tip NULL să nu consume spaţiu fizic.
- Posibilitatea creării de tabele cu mai mult de 1.024 de coloane.
- Suport pentru definirea datelor de tip spaţial pentru consumul, extinderea şi utilizarea informaţiilor în aplicaţii activate din punct de vedere spaţial. Datele de tip spaţial trebuie sa corespunda standardelor din domeniu, precum Open Geospatial Consortium (OGC).

- Utilizarea unei platforme avansate pentru dezvoltarea de aplicaţii complexe de procesare a evenimentelor (CEP):
  - Posibilitatea de dezvoltarea de aplicaţii bazate pe evenimente folosind platforma de procesare a evenimentelor pentru a se permite interogări continue si latenta de milisecunde.
- Posibilitatea de dezvoltare de aplicaţii care să crească valoarea de business prin scăderea costului de extragere, analiza şi corelare a datelor permiţând monitorizarea si managementul datelor în timp real.
  - Costuri totale de deţinere. Sistemul trebuie sa ofere mecanisme pentru reducerea costului total de deţinere (TCO), si prin implementarea administrării bazate pe politici pentru:
    - Definirea si managementul politicilor de configurare a sistemului,
    - Monitorizarea şi prevenirea modificărilor asupra sistemului prin crearea de politici împotriva configurării,
    - Detectarea problemelor de conformitate cu politicile direct din interfaţa de administrare a server-ului,
    - Posibilităţi de virtualizare pentru a creste ROI (Return On Investment) prin consolidare si virtualizare.

Se vor include licenţe pentru sistemul relaţional de baze de date, dimensionate de către Ofertant conform nevoilor identificate în analiza cerinţelor documentaţiei de atribuire şi corelate cu modul de licenţiere al producătorului propus, care să ofere suport pentru rularea a minim 3 instanţe, fiecare având cel puţin 4 nuclee.
Notă: 1 nucleu = 1 core-procesor x86_64.

4.5 Infrastructură Hardware

În subcapitolele următoare sunt detaliate cerinţele privind echipamentele din cadrul proiectului pentru a căror livrare se va aloca o perioadă de maxim 55 de zile de la data ordinului de începere a contractului.

4.5.1 Server de Aplicaţii

Se vor include 3 echipamente (în configuraţie identică) de tip Server de Aplicaţii care să îndeplinească cerinţele de mai jos:

Componentă	**Caracteristici**
Procesor	Procesor in arhitectura x86_64 cu frecevenţa minim 2.0 GHz, minim 8

	nuclee processor si minim 20MB memorie cache.
Procesoare instalate	Minim 2
Memorie RAM	• Minim 96 GB RAM instalata, de tip ECC DDR3, cu suport pentru ECC, ChipKill, Memory rank sparing, Memory Mirroring sau tehnologii echivalente; • Suport pentru minim 24 sloturi de memorie cu posibilitate de upgrade la cel puţin 768 GB.
Capacitate stocare pe HDD-uri	• Suport pentru minim 16 discuri interne SAS si minim 32 discuri interne de tip SSD; • Minim 3 x 300 GB / 10 krpm SAS instalate.
Unitate optica	Unitate interna de tip CD-RW/DVD-RW.
Controller RAID	• Controller RAID SAS 6 Gbps, suport pentru RAID 0, 1, 10, 5, 50; • Server-ul trebuie sa suporte controller cache cu memorie de minim 2GB (acest controller trebuie sa fie certificat de către producătorul server-ului şi trebuie sa apară pe site-ul acestuia sau in documentaţia tehnica a server-ului).
Interfata grafica	• Integrata pe placa de baza; • Minim 16 MB RAM (memorie dedicată).
Interfete de retea	• 4 x Gigabit Ethernet; • Suport pentru TOE (TCP Offload Engine), WoL, NIC Teaming cu capabilităţi de loadcing şi failover; • Suport pentru adăugarea a cel puţin doua porturi 10Gb Ethernet RJ-45 sau SFP+ fara ocuparea slot-urilor de expansiune PCI.
Interfete SAN	2 x port FC 8 Gbps cu cablu de minim 5m de fibra optica.
Sloturi PCI de expansiune	• Minim 6 carduri PCI-Express 3.0; • Opţional, serverul va putea fi echipat cu sloturi PCI-X.
Porturi	• 1 x port serial; • 2 x video; • 6 x USB; • 1 x RJ45 pentru management; • 2 x USB interne pentru hipervizor virtualizare si/sau unitate de banda interna.
Management	• Sistem incorporat de monitorizare pentru: discuri interne, ventilatoare, surse de alimentare cu energie electrica, temperatură; • Panou cu LED-uri de indicatoare de stare pentru diagnosticarea rapida a stării de funcţionare a componentelor critice si software pentru management; • Analize predictive de eroare pentru: discuri interne, memorii, procesoare, surse alimentare cu energie electrica, regulatoare de tensiune, ventilatoare, cu posibilitatea anunţării administratorului de sistem despre iminenta defectare a uneia dintre component; • Management de la distanta, redirectare interfaţa grafica, tastatura si mouse, posibilitate de pornire/oprire de la distanta, suport pentru remote media (virtual CD si floppy), suport pentru SSL, LDAP.

Format	• Format: "rack-mountable" in rack standard de 19"; • Maxim 2U; • Kit de montare in rack inclus.
Electroalimentare / răcire	• Ventilatoare: "hot swap" cu viteza de rotaţie variabila; • Surse de alimentare cu energie electrica: o redundante, o "hot swap", o minim 550W fiecare;
Sisteme de operare suportate	• Serverul trebuie sa compatibil cu cel puţin următoarele sisteme de operare: o Microsoft Windows Server 2008, o Microsoft Windows Server 2012, o Microsoft Windows Server 2012 R2, o Red Hat Enterprise Linux 5/6, o SUSE Linux Enterprise Server 10/11, o VMware v4.x/5.x.

4.5.2 Server de Baze de Date

Se vor include 2 echipamente (în configuraţie identică) de tip Server de Baze de Date care să îndeplinească cerinţele de mai jos:

Componentă	**Caracteristici**
Procesor	Procesor in arhitectura x86_64 cu frecvenţa minim 1.9 GHz, minim 10 nuclee procesor si minim 25MB memorie cache.
Procesoare instalate	Minim 2
Memorie RAM	• Minim 96 GB RAM instalata, de tip ECC DDR3, cu suport pentru ECC, ChipKill, Memory rank sparing, Memory Mirroring sau tehnologii echivalente; • Suport pentru minim 24 sloturi de memorie cu posibilitate de upgrade la cel puţin 768 GB.
Capacitate stocare pe HDD-uri	• Suport pentru minim 16 discuri interne SAS si minim 32 discuri interne de tip SSD; • Minim 3 x 300 GB / 10 krpm SAS instalate.
Unitate optica	Unitate interna de tip CD-RW/DVD-RW.
Controller RAID	• Controller RAID SAS 6 Gbps, suport pentru RAID 0, 1, 10, 5, 50; • Server-ul trebuie sa suporte controller cache cu memorie de minim 2GB (acest controller trebuie sa fie certificat de către producătorul server-ului si trebuie sa apară pe site-ul acestuia sau în documentaţia tehnica a server-ului).
Interfaţa grafica	• Integrata pe placa de baza; • Minim 16 MB RAM (memorie dedicată).
Interfeţe de reţea	• 4 x Gigabit Ethernet; • Suport pentru TOE (TCP Offload Engine), WoL, NIC Teaming cu capabilităţi de loadcing şi failover; • Suport pentru adăugarea a cel puţin doua porturi 10Gb Ethernet RJ-45 sau SFP+ fără ocuparea slot-urilor de expansiune PCI.
Interfeţe SAN	2 x port FC 8 Gbps cu cablu de minim 5m de fibra optica.

Sloturi PCI de expansiune	• Minim 6 carduri PCI-Express 3.0; • Opţional, serverul va putea fi echipat cu sloturi PCI-X.
Porturi	• 1 x port serial; • 2 x video; • 6 x USB; • 1 x RJ45 pentru management; • 2 x USB interne pentru hipervizor virtualizare si/sau unitate de banda interna.
Management	• Sistem incorporat de monitorizare pentru: discuri interne, ventilatoare, surse de alimentare cu energie electrica, temperatură; • Panou cu LED-uri de indicatoare de stare pentru diagnosticarea rapida a stării de funcţionare a componentelor critice si software pentru management; • Analize predictive de eroare pentru: discuri interne, memorii, procesoare, surse alimentare cu energie electrica, regulatoare de tensiune, ventilatoare, cu posibilitatea anunţării administratorului de sistem despre iminenta defectare a uneia dintre component; • Management de la distanta, redirectare interfaţa grafica, tastatura si mouse, posibilitate de pornire/oprire de la distanta, suport pentru remote media (virtual CD si floppy), suport pentru SSL, LDAP.
Format	• Format: "rack-mountable" in rack standard de 19"; • Maxim 2U; • Kit de montare in rack inclus.

Electroalimentare / răcire	• Ventilatoare: "hot swap" cu viteza de rotaţie variabila;
	• Surse de alimentare cu energie electrica:
	  ○ redundante,
	  ○ "hot swap",
	  ○ minim 550W fiecare.

Sisteme de operare suportate	• Serverul trebuie sa compatibil cu cel puţin următoarele sisteme de operare:
	  ○ Microsoft Windows Server 2008,
	  ○ Microsoft Windows Server 2012,
	  ○ Microsoft Windows Server 2012 R2,
	  ○ Red Hat Enterprise Linux 5/6,
	  ○ SUSE Linux Enterprise Server 10/11,
	  ○ VMware v4.x/5.x.

4.5.3 Server de Stocare Unificată

Se va include 1 echipament de tip Server de Stocare Unificată (SAN) care să îndeplinească cerinţele de mai jos:

Componentă	**Caracteristici**
Descriere generala	• Sistem de stocare centralizata • Minim 2 controllere redundante si hot-plug, cu failover automat
Protocoale de acces	• Minim FC, iSCSI, NFS, CIFS, HTTP • Sistemul se va livra cu toate protocoalele activate

	• Sistemul trebuie sa permită utilizarea simultana a tuturor protocoalelor de acces
Porturi de acces	• 8 porturi Ethernet 1Gbps, instalate, SFP-uri incluse • 4 porturi FC 8 GB instalate • 2 porturi pentru seriale pentru consola de acces • 2 porturi pentru LAN Management
Memorie cache instalată	12 GB
Capacitate de stocare instalata	Minim 24 discuri SAS fiecare cu capacitatea de minim 600 GB (minim 10k RPM).
Carcasă	Sistemul în configuraţia ofertată trebuie să se încadreze în maxim 2U spaţiu rack.
Protecţia datelor pe disc	• Sistemul trebuie să permită implementarea de matrici RAID si a discurilor de tip hot-spare. • Sistemul trebuie sa asigure conectarea către fiecare unitate HDD prin intermediul a doua cai de acces redundante cu fail over automat.
Redundanta sistemului si suportul pentru operaţiuni de întreţinere fără întreruperea serviciilor	• Sistemul trebuie sa includă controllere redundante cu failover automat, alimentarea cu energie trebuie sa fie redundanta – minim 2 surse de alimentare. • Sistemul trebuie sa includă controllere, surse de alimentare si discuri in tehnologie HotSwap – extragerea, completarea sau înlocuirea lor sa poată fi realizata on line. • Adăugarea unităţilor de expansiune trebuie sa poată fi realizata online fără întreruperea conexiunilor cu unităţile de expansiune deja instalate.
Conectivitate (hosts)	Numărul minim de host-uri suportate trebuie sa fie de cel puţin 256
Sisteme de operare (host) suportate si certificate	• Sistemele de operarea minim certificate trebuie sa fie: Microsoft Windows 2008, VMware ESX, RedHat Linux, Suse Linux, IBM AIX, HP-UX, SUN Solaris, Mac OS. • Sistemul de stocare trebuie sa fie livrat împreună cu driverele de multipath şi load balancing incluse in configuraţia propusă.
Sertare de expansiune	Sertarele de expansiune trebuie să suporte cel puţin următoarele tipuri de discuri: SSD, SAS, SATA si discuri cu autocriptare.
Scalabilitate	• Numărul de discuri suportate la nivelul sistemului de stocare , minim 144. • Sistemul trebuie să suporte mecanisme de tip cluster de stocare, funcţionarea in mod concurent si consolidarea capacităţii de procesare si stocare împreună cu alte echipamente din aceeaşi gama. Sistemul trebuie sa suporte minim 4 noduri cluster.
Funcţionalităţi software la nivel de controller	• Sistemul trebuie să permită realizarea copiilor locale instantanee – tip Snapshot. • Sistemul trebuie sa permită restaurarea instantanee a copiilor tip Snapshot. • Sistemul trebuie suporte realizarea copiilor locale integrale tip Clona. • Sistemul trebuie sa suporte realizarea de clone locale virtuale ale seturilor de date. • Sistemul trebuie sa suporte realizarea copiilor la distanta a

	seturilor de date, in maniera sincrona si asincrona, atât prin protocol SAN cat si protocol NAS . • Sistemul trebuie sa suporte backup si restaurare disk-to-disk pe un echipament secundar din aceeaşi gama. • Sistemul trebuie sa suporte definirea de volume tip WORM.
Funcţionalităţi software de eficientizare a spaţiului	• Echipamentul trebuie sa permită utilizarea mecanismelor de tip Thin Provisioning sau echivalent: mecanismul trebuie sa permită alocarea către servere a unor capacităţi mai mari decât cele instalate fizic in interiorul sistemului de stocare. • Echipamentul trebuie să permită deduplicarea datelor stocate atât la nivel de bloc cat si la nivel de fişier, în mod transparent pentru serverele host. • Echipamentul trebuie sa suporte compresia datelor stocate, în mod transparent pentru serverele host.
Optimizarea performantei	Echipamentul trebuie să dispună de un mecanism de prioritizare a accesului aplicaţiilor la volumele de date, cu cel puţin 5 nivele de prioritate implementate.
Integrarea serviciilor de copiere pentru back-up la nivel de aplicaţii	• Echipamentul trebuie sa ofere suport la nivel de controler pentru funcţionalităţi de backup si restaurare prin care sa asigure protecţia datelor in maniera consistenta cel puţin pentru: MS Windows , Linux , Exchange, SQL Server, SharePoint, Oracle, SAP, VMware si Hyper-V. • Operatiunea de backup trebuie sa se realizeze fără oprirea serviciilor la nivel de aplicaţie.

4.5.4 Echipament Cabinet

4.5.4.1 Cabinet tip A

Se va include 1 echipament Cabinet tip A care să îndeplinească cerinţele de mai jos:

Componentă	**Caracteristici**
Descriere generala	Rack standard 19” si accesorii dimensionate corespunzător pentru găzduirea si alimentarea tuturor echipamentelor (tip server) din sediului central al ANFP.
Rack	• Rack standard 19” de dimensiune 42U. • Rack-ul va fi livrat împreună cu toate componentele care asigura montarea respectiv electroalimentarea redundanta (PDUs) a echipamentelor ofertate.
Consola si Switch KVM	• Modul de tip KVM inclus, „rack-mounted”, include: o monitor TFT (Rezoluţie minima 1280 x 1024 at 75 Hz), de min. 17”; o tastatură USB cu dispozitiv integrat de tip „touch-pad” sau similar. • Switch-ul KVM va asigura conectarea a minim 8 servere (vor fi incluse toate cablurile si componentele necesare acestei conectări). • KVM-ul trebuie sa suporte conectare remote pentru operaţiunile de administrare.

4.5.4.2 Cabinet tip B

Se va include 1 echipament Cabinet tip B care să îndeplinească cerinţele de mai jos:

- Înălţime: Cadru rack 19" / 24 U ;
- Dimensiuni: 600 x 1000 mm ;
- Conectivitate: se vor include 2 unităţi tip PDU (Power Distribution Unit), fiecare cu minim 4 socket-uri C13.
- Altele:
  - Se va include un Switch KVM cu minim 8 porturi cu suport pentru conectare remote pentru operaţiuni de administrare;
  - Monitor de minim 17 inch cu rezoluţie minima 1280 x 1024.
  - Se va include kit-ul pentru montare in rack.

4.5.5 Echipament UPS

4.5.5.1 Echipament UPS tip A

Se va include 1 echipament UPS tip A care să îndeplinească cerinţele de mai jos:

Componentă	**Caracteristici**
UPS	• Unitate discreta independenta de tip on-line dubla conversie, monofazata (1/1) de minim 11KVA. • Unitatea UPS trebuie sa ofere un timp de funcţionare in regim de avarie de minim 5 minute la o încărcare de 100% si minim 14 minute la o încărcare de 50%. • Unitatea UPS trebuie sa permită extinderea timpului de funcţionare in regim de avarie prin cel puţin un modul discret de baterii, integrabil in structura fără necesitatea opririi alimentarii echipamentelor deservite. • Componentele interne ale unităţilor UPS, inclusiv bateriile, vor fi de tip hot-swap permiţând astfel deservirea (inclusiv înlocuirea acestora) fără oprirea sarcinii. • Unitatea UPS va include modul de management pentru monitorizare la distanta, inclusiv software de management si indicatori frontali pentru suprasarcina si nivel încărcare module de baterii. • Eficienta: minim 96%. • Conectori: minim 8 x IEC 320 C19. • Porturi: minim USB şi RS-232.

4.5.5.2 Echipament UPS tip B

Se va include 1 echipament UPS tip B care să îndeplinească cerinţele de mai jos:

- Putere:
  - cel puţin 3300VA;
  - cel puţin 3000W.
- Tip: Rackmount cu posibilitate de conversie in Tower (kit-ul de conversie inclus).
- Spaţiu ocupat in rack: Maxim 2.
- Topologie: On-line dubla conversie.
- Conectori ieşire: Cel puţin 6 x IEC C13 si 2 x IEC C1.

- Porturi: Minim USB si serial.
- Autonomie:
  - cel puţin 4minute la încărcare maxima;
  - cel puţin 12minute la încărcare 50%.
- Timp de reîncărcare: cel mult 3 ore pentru încărcare la 80% din baterie.
- Zgomot: Cel mult 45db in modul de operare normal.

4.5.6 Switch FC

Se vor include 2 echipamente (în configuraţie identică) de tip Switch FC care să îndeplinească cerinţele de mai jos:

Componentă	**Caracteristici**
Arhitectura sistem	• Suport pentru funcţionalitatea de baza pentru reţele de date (SAN). • Scalabil şi resilient.
Porturi FC	• Minim 12 porturi FC "non-blocking" activate, cu posibilitatea de scalare pana la dublul numărului de porturi activate ofertate. • Porturile trebuie sa fie de tip 16 Gbps cu facilitatea de auto-descoperire si operare la 2, 4, 8 si 16 Gbps.
"Transceivers"	Un numar de "transceivers" SFP+ 8 Gbps "shortwave" (SW) egal cu numărul de porturi activate ofertate.
Cabluri	(Pentru fiecare switch) se va include un număr minim de cabluri de fibra optica "multi-mode" de minim 5m, egal cu numărul de porturi activate ofertate precum si cablurile de alimentare cu energie electrica.
Management	Software de management si monitorizare (de tip sistem de operare) care sa asigure minim următoarele funcţionalităţi: • Interfaţa grafica (GUI) de administrare, configurare si mentenanţa pentru switch-uri si SAN; • Zonare care sa asigure segmentarea "fabric"-ului SAN in mai multe SAN-ui private virtuale, cu restricţii de comunicare intre echipamente si politici aplicabile la nivel de zona; • "Full fabric" pentru conectarea intre switch-uri; • Suport pentru protocoalele / standardele: SNMP, SSH, HTTP, SMI-S. • Port de management de tip RJ45 Ethernet.
Alte funcţionalităţi	Se va include licenta de tip "extended fabric".
Format	• Tip "rack-mounted" • Dimensiunea de maximum 1U • Se va include kit-ul de montare în rack.
Alimentare cu energie electrica	Minim 2 surse de alimentare cu energie electrica redundante si "hot-swap".

4.5.7 Switch Ethernet

Se vor include 2 echipamente (în configuraţie identică) de tip Switch Ethernet 24-port care să îndeplinească cerinţele de mai jos:

Componentă	**Caracteristici**

Carcasa	• Tip: Rack-mount; • Dimensiuni: 19 inch, 1U – înălţime maximă.
Interfeţe/Porturi	• 24 X 10/100/1000 Mbps RJ45; • Slot extensie pentru SFP sau SFP+; • Posibilitatea de mărire a densităţii porturilor fie prin stack-are fie prin inserare de module adiacente, cu throughput de cel puţin 480 GBPs intre elementele stivei sau pe backplane-ul modular; • Suport pentru cel puţin 2 uplinkuri de 10GE, fie integrat fie prin ataşarea unor module suplimentare.
Memorie	• DRAM: minimum 4 GB; • Flash: minimum 2 GB .
Performante	• Capacitate de switching: minim 88 Gbps; • Throughput pachete 64B: minim 65 Mpps; • Mărime tabela MAC: minim 32000 intrări; • Rute Ipv4: minim 24000 intrări; • Grupuri IPv4 IGMP: minim 255; • VLAN-uri configurabile: minim 255; • Jumbo frames - 9016 B.
Management	• Interfaţă tip Command-line; • Suport browser web; • Suport protocoale: SNMP, Telnet, SSH; • Software de management de reţea inclus.
Tehnologii, standarde şi protocoale suportate	• Echipamentele vor dispune de porturi dedicate interconectării mai multor switch –uri intr-o arhitectura redundantă, sub forma de unui singur switch, virtual, care sa aibă un singur management. Tehnologia de interconectare trebuie sa asigure: o Viteza de transfer de minim 80 Gbps intre switchuri; o Un număr de minim 9 switch-uri intr-un acelaşi cluster; o Comutarea datelor intre doua porturi de pe acelaşi switch sa se facă local, fără utilizarea magistralei de interconectare; o Posibilitatea agregării porturilor de pe switch-uri diferite prin protocol “LACP - Link Aggregation Control Protocol”, conform standardului IEEE802.3ad; o 802.3ae 10 Gigabit Ethernet; o 802.1Q VLAN Tagging; o 802.1p Class-of-Service (CoS) Tagging for Ethernet frames; o 802.1x Port-based network access control. • Sistemul de operare al echipamentului va oferi urmatoarele facilitati Ethernet switching: o sistem de detectare a link-urilor unidirecţionale; o protocol de propagare automata a VLAN-urilor; o posibilitatea blocării traficului per port (unicast, multicast si broadcast);

	○ PVRST+ (Per-VLAN Rapid Spanning Tree Plus) pentru interconectarea cu echipamentele existente din ANFP; ○ facilităţi de WLAN Controller, fie integrate, fie prin instalarea de module suplimentare ce pot oferi suport pentru minim 40 AP-uri si până la 2000 de clienţi wireless. • Sistemul de operare al echipamentului va oferi următoarele facilităţi de securitate: ○ Liste de control al accesului si de filtrare a traficului la nivel de port; ○ Mecanism de segregare a traficului din acelaşi VLAN, care sa restricţioneze comunicaţia dintre hosturi aparţinând aceleaşi reţele IP; ○ Controlul accesului în reţea bazat pe IEEE 802.1X; ○ Limitarea numărului de adrese MAC pe un port, prin mecanism "Port Security" sau echivalent; ○ Securizarea traficului DHCP prin mecanism "DHCP Snooping" sau echivalent; ○ Securizarea traficului ARP prin mecanism "Dynamic ARP Inspection" sau echivalent; ○ Prevenirea furtului sau a utilizării neautorizate de adrese IP prin mecanism "IP source guard" sau echivalent; ○ Prevenirea interceptărilor de trafic si a perturbaţiilor ce pot apărea intr-o reţea ce foloseşte Spanning Tree Protocol, prin mecanisme "Spanning Tree Root Guard" si "Bridge Protocol Data unit Guard" sau echivalent. • Sistemul de operare al echipamentului va oferi următoarele facilităţi de rutare IP: ○ Rutare statica IPv4 si IPv6; ○ Rutare dinamica bazata pe protocoalele RIPv2 si OSPFv3; ○ Posibilitatea balansării traficului spre o destinaţie prin cel puţin 8 intermediari diferiţi; ○ Host Standby Routing Protocol (HSRP) pentru interconectarea cu echipamentele existente ale ANFP. • Sistemul de operare al echipamentului va oferi următoarele facilităţi IP Multicast: ○ Rutare traffic multicast; ○ Source-Specific Multicast (SSM); ○ PIMv2; ○ Bidirectional PIM. • Sistemul de operare al echipamentului va oferi suport pentru QoS: clasificare, marcare, limitare si plasare a traficului in cozi cu servire planificata. Limitarea traficului se va putea face cu minimum 64 de politici per port.
Condiţii de operare	• Sistem de răcire cu aer din fata si laterale către in spate; • Alimentare redundanta (la 220V AC) si partajarea

	consumului intre membrii stivei sau prin inserarea unor surse suplimentare; • Temperatura de lucru: (cel puţin) -5°C la 45°C; • Umiditate relativa acceptata: (cel puţin) 5% - 95%, fără condensare.
Caracteristici electrice	• Sursa de alimentare cu suport pentru standardele româneşti: 220 VAC / 50 Hz; • Opţiune pentru sursa redundanta.
Accesorii incluse	• 1 cablu de alimentare energie electrică tip schuko conform standardelor româneşti; • 1 kit de instalare in rack de 19".
Caracteristici fizice maxime	• Maxim 4.5 x 44.5 x 46.0 cm; • Maxim 7,5 Kg. •

4.5.8 Echipament de Securitate

Se vor include 2 echipamente de securitate (în configuraţie identică) de tip Firewall/VPN care să îndeplinească cerinţele de mai jos:

Componentă	**Caracteristici**
Carcasa	• Tip: Rack-mount • Dimensiuni: 19 inch, 1U – înălţime maximă
Interfeţe/Porturi	• 6 X 10/100/1000 Mbps RJ45. • 1 X RJ45 management console • 2 X USB 2.0 • 1 slot pentru carduri de extensie
Memorie	• DRAM: minimum 4 GB • Flash: minimum 4 GB
Performante	• Firewall throughput: minim 1 Gbps • Număr de conexiuni firewall: minim 100.000 • Număr de conexiuni/sec firewall: minim 10.000 • VPN 3DES/AES throughput: minim 200 Mbps • IPS Throughput: minim 250 Mbps • Interfeţe virtuale (VLAN): minim 50 • Sesiuni IPsec VPN: minim 250 • Sesiuni Remote VPN: minim 250 • Sesiuni SSL VPN: minim 2
Management	• Interfaţă tip Command-line • Suport browser web • Suport protocoale: SNMP, Telnet, SSH
Condiţii de operare	• Temperatură: (cel puţin) 0 la 40ºC • Umiditate relativă: (cel puţin) 5% to 95%, fără condens

Caracteristici electrice	• Sursa de alimentare cu suport pentru standardele româneşti: 220 VAC / 50 Hz • Putere maximă consumată: maxim 56W la performante maxime
Caracteristici fizice maxime	• Maxim 4.5 x 44.5 x 46.0 cm; • Maxim 7,5 Kg.
Standarde minime de securitate, mediu, electromagnetice şi certificări de securitate	• EN 60950 IEC 60950 Sau echivalente • EN55022 Class A, EN61000-3-2, EN61000-3-3 Sau echivalente • • FIPS 140-2 Level 2, Common Criteria EAL4 US DoD Application-Level Firewall for Medium-Robustness Environments Sau echivalente
Update-uri software	• Minim 3 ani
Accesorii incluse	• 1 cablu consolă • 1 cablu de alimentare energie electrică tip schuko conform standardelor româneşti • 1 kit de instalare in rack de 19"

4.5.9 Scaner A3

Se va include 1 echipament tip Scaner A3 care să îndeplinească cerinţele de mai jos:

Componentă	**Caracteristici**
Tip scaner	Scaner plat
Formate hârtie suportate	A3, A4, A5, A6, B4, B5, B6, Letter, Legal, Executive
Rezoluţie scaner	600 DPI x 600 DPI (orizontal x vertical)
Profunzime de culoare	• Intrare minim 48 bits color / 16 bits monocrom • Ieşire minim 24 bits color / 8 bits monocrom
Senzor cu ultrasunete	Da
Afişaj LCD	Panou interfaţă de reţea
Viteză de scanare la rezoluţie de 200/300 dpi (măsurată pentru dimensiune A4)	• Monocrom 40 Pagini/min • Color 40 Pagini/min • Monocrom 80 imagini/min • Color 80 imagini/min
Alimentare automată cu documente	200 Pagini
Fiabilitate ciclu de lucru zilnic	Minim 5000 pagini
Duplex scan	Da, standard automat
Caracteristici	• ignoră paginile goale, • prelucrare avansată imagini, • setări prestabilite, • divizare automată a intervalului, • corectare automată a poziţiei înclinate a hârtiei, • recunoaştere automată multi-document,

	• detectare automată culori şi alb-negru, • ieşire pe ecran dublă (numai Windows), • rotire automată a imaginii, • îmbunătăţire text, • netezire muchii, • mascare neclarităţi, • documente împărţite pe orizontală şi pe verticală, • corecţie cotor, • creare automată de foldere, • recunoaştere coduri de bare, • acceptă OCR A şi B pe zone, • separare lucrări manuală/automata
Formate ieşire	• scanare către JPEG, • scanare către TIFF, • scanare către multi TIFF, • scanare către PSF, • scanare către pdf / batch, • scanare către PDF căutabil, • scanare către PDF sigur, • scanare în PDF/A
Caracteristici comprimare fişier	• comprimare hardware JPEG, • comprimare TIFF (JPEG(7), CITT G4, LZW), comprimare PDF
Funcţii avansate	• scanare către email, scanare către FTP, • scanare către Microsoft SharePoint, • scanare către imprimare, • scanare către folder Web, • scanare către folder de reţea
Conectivitate	Interfaţă Ethernet (100 Base-TX/10 Base-T)
Setări Ethernet	10BASE-T / 100BASE-TX / 1000BASE-T / Duplex integral / Semiduplex
Tip panou	LCD cu 5 rânduri cu funcţii de scanare prin buton de comandă
Suport pentru protocoale	• TCP/IP, • DHCP, • DNS, • SNMP, • SLP, • HTTP
Suport pentru IPv6	Da
Funcţii de scanare prin buton de comandă	Da (cu soluţii Document Capture Pro sau echivalent)
Blocare panou prin parolă	Da (cu soluţii Document Capture Pro sau echivalent)
Tensiune de alimentare	100 V - 240 V
Driver	• TWAIN, • WIA, • ISIS

Consum de energie	Cel mult: • 85 Waţi funcţionare normală, • 20Waţi (economic) • 4,5 Waţi (în standby)
Nivel de zgomot în timpul funcţionării	Cel mult 68 dB (A)
Accesorii livrate cu echipamentul	• cablu alimentare, • instrucţiuni de utilizare, • software

4.5.10 Scaner A4

Se vor include 4 echipamente (în configuraţie identică) de tip Scaner A4 care să îndeplinească cerinţele de mai jos:

Componentă	**Caracteristici**
Tip scaner	Scaner plat
Formate hârtie	A4, A5, A6, B5, Letter, Legal, Executive
Rezoluţie scaner	1.200 DPI x 1.200 DPI (orizontal x vertical)
Profunzime de culoare	• Intrare 48 Bits Color / 16 Bits Monocrom, • Ieşire 24 Bits Color / 8 Bits Monocrom
Senzor cu ultrasunete	Da
Afişaj LCD	Panou interfaţă de reţea
Viteză de scanare la rezoluţie de 200/300 dpi (măsurată pentru dimensiune A4)	• Monocrom 40 Pagini/min • Color 40 Pagini/min • Monocrom 80 imagine/min • Color 80 imagine/min
Fiabilitate ciclu de lucru zilnic	Minim 4000 pagini
Alimentare automată cu documente	Minim 100 pagini
Duplex Scan	Da
Caracteristici	• ignoră paginile goale, • setări prestabilite, • divizare automată a intervalului, • corectare automată a poziţiei înclinate a hârtiei, • detectare automată culori şi alb-negru, • ieşire pe ecran dublă (numai windows), • rotire automată a imaginii, • îmbunătăţire text, • netezire muchii, • funcţiune cropping îmbunătăţită pentru ajustarea mărimii, • mascare neclarităţi
Formate ieşire	• scanare către JPEG, • scanare către TIFF, • scanare către multi TIFF, • scanare către PSF, • scanare către pdf / batch, • scanare către pdf căutabil, • scanare către PDF sigur, • scanare în PDF/A
Caracteristici comprimare fişier	• comprimare hardware JPEG,

	• comprimare TIFF (JPEG(7), CITT G4, LZW), • comprimare PDF
Advanced document integration	• Scanare către email, • scanare către FTP, • scanare către Microsoft SharePoint, • scanare către imprimare, • scanare către folder web, • scanare către folder de rețea
Conexiuni	Interfaţă Ethernet (100 Base-TX/10 Base-T)
Panou pentru interfață de rețea	Integrat
Setări Ethernet	10BASE-T / 100BASE-TX / 1000BASE-T / Duplex integral / Semiduplex
Tip panou	LCD cu 5 rânduri cu funcţii de scanare prin buton de comandă
Suport pentru protocoale	• TCP/IP, • DHCP, • DNS, • SNMP, • SLP, • HTTP
Suport pentru IPv6	Da
Funcţii de scanare prin buton de comandă	Da (cu soluţii Document Capture Pro sau echivalent)
Blocare panou prin parolă	Da (cu soluţii Document Capture Pro sau echivalent)
Driver	• TWAIN, • WIA, • ISIS
Consum de energie	Cel mult: • 50 Waţi (funcţionare normală), • 18 Waţi (economic) • 5 Waţi (în standby)
Accesorii livrate cu echipamentul	• cablu alimentare, • software • cablu USB • instrucţiuni de utilizare

4.5.11 Laptop pentru Administrare

Se vor include 3 echipamente (în configuraţie identică) de tip Laptop (pentru administrare) care să îndeplinească cerințele de mai jos:

Componentă	**Caracteristici**
Procesor	Minim Intel Core i5 3340M 2.7GHz vPRO sau echivalent
Memorie RAM	• Suport pentru SO-DIMM DDR3L minim 8 GB • Minim 4 GB instalată
Display	• Tip: TFT, XGA • Diagonală: maxim 10,1” • Vizibilitate: vizibil în lumina soarelui • Mod de lucru: Tablet PC cu Touchscreen

	• Touchscreen: de tip Dual, rezistiv 5 degete şi digitizer • Protecţie ecran: dotat cu folie de protecţie a ecranului (înlocuibilă)
Video	Minim Intel HD Graphics 4000 sau echivalent
Luminozitate ecran	• Minim 500cd/m2 maxim 6500 cd/m2 (în raport cu lumina exterioară) • Senzor de lumină ambientală
Porturi / Sloturi de expansiune	• 1 x USB 2.0 • 1 x USB 3.0 • 1 x 10/100/1000 RJ45 • 1 x RJ11 • 1 x Port replicator 100 pin • 1 x PCMCIA • 1 x Express Card • 1 x Firewire IEEE1394a • 1 x COM RS232 (compatibil 16550a) • 1 x VGA • 2 x Conector antena externa • 1 x Card Reader SD/SDHC/SDXC
Conectivitate wireless	• 802.11a/b/g/n wireless LAN • BlueTooth V4.0 + EDR, class 1 • Modem 3G+/HSPA+ 21Mbps (integrat)
HDD amovibil	• Minim 500 GB • Cu protecţie la şocuri şi căderi de la minim 175cm înălţime, cu încălzire şi uşor accesibil
Carcasă	• Rezistent la şocuri şi vibraţii • Cu protecţie la porturile I/O împotriva prafului şi a ploii.
Tastatură	Waterproof
Acumulator	• Amovibil, • Li-Ion, • Minim 10h autonomie
• Temperatura de operare	Cel puţin de la -28 la +60 grade Celsius
• Securitate	• Chip integrat TPM TCG v1.2, sau echivalent • Port Kensington lock
• Sistem de operare	Microsoft Windows 8 Professional cu posibilitate de downgrade la Microsoft Windows 7 Professional (sau echivalent)
• Software	Microsoft Office 2013 Professional sau echivalent
• Garanţie	minim3 ani

4.5.12 Echipament tip Thin Client

Se vor include 3 echipamente (în configuraţie identică) de tip Thin Client (pentru administrare) care să îndeplinească cerinţele de mai jos:

Componentă	**Caracteristici**
Procesor	• Minim 2 nuclee de procesare • Minim 1.5 GHz frecvenţă

Cabilităţi video	Minim 1920 x 1200 pixel
Porturi	Cel puţin: • Audio in: 1 • Audio out: 1 • Microfon: 1 • USB: 4 • DVI: 2 • Tastatura/Mouse: 2 x PS2 • Ethernet (RJ-45): 1 x 10/100/1000
Platformă de virtualizare	Suport pentru distribuţii linux open-source de tip ”openThinClient” sau echivalent.

Garanţia echipamentelor furnizate va fi de cel puţin 3 ani.

4.6 Alte cerinţe tehnice

4.6.1 Cerinţe generale

Aşa cum s-a precizat in capitolul 1 – „Informaţii generale”, Sistemul e-ANFP va ajuta la îmbunătăţirea calităţii şi eficienţei serviciilor furnizate de către ANFP în vederea modernizării capacităţii administrative a instituţiilor publice din România. Totodată Sistemul e-ANFP va include infrastructura hardware cât şi infrastructura software de suport constituită din sistem de operare tip server (cu suport pentru virtualizare) şi sistem relaţional de baze de date, sisteme pentru care pachetele de licenţiere vor asigura complet accesul concurenţial al funcţionarilor publici şi personal contractual din cadrul ANFP Sediul Central.
Pe baza informaţiilor prezentate în capitolul 2.1 – ”Obiective” şi în capitolul 2.3 – ”Obiectul achiziţiei” din cadrul prezentului document, se evidenţiază următoarele cerinţe generale minime menite a fi îndeplinite de către Sistemul e-ANFP:

- Sa fie un sistem web-based, care respecta arhitectura 3-tier, astfel:
  - să includă un server de gestiune a bazelor de date relaţionale;
  - să includă un server de aplicaţii;
  - să fie accesibil utilizatorilor prin intermediul unui browser web (ex. : Microsoft Internet Explorer, Mozilla Firefox, etc.);
- Componentele software ale sistemului sa fie instalate intr-un mediu virtualizat;
- Să ofere suport multi-utilizator in mod concurenţial;
- Să ruleze în cadrul unei reţele LAN şi să poată fi accesat via WAN/web;
- Să implementeze modelul bazei de date centralizate, găzduita de serverele pentru gestiunea bazelor de date relaţionale;
- Să ofere mecanisme şi facilităţi avansate de :
  - Managementul şi arhivarea documentelor electronice;
  - Suport pentru lucrul în regim de flux;
  - Captură a documentelor;
  - Management a activelor IT;
  - Monitorizare a performantei aplicaţiilor;
  - Salvare/restaurare în mod centralizat a datelor/informaţiilor;
  - Salvare/restaurare a serviciului director;
  - Audit de securitate;
  - Suport utilizatori;
  - Administrare utilizatori (şi profile de utilizatori);

- Control granular al accesului;
- Criptare a datelor/informaţiilor;
- Interconectare a aplicaţiilor;
- Asigurare a înaltei disponibilităţi (a Sistemului);
- Scalabilitate (a Sistemului).

- Să includă o infrastructura hardware de suport compusă din:
  - Servere de aplicaţii, baze de date şi stocare unificată;
  - Echipamente de conectivitate şi securitate (în reţea);
  - Echipamente de scanare;
  - Echipamente (tip client) de lucru pentru personalul administrativ IT.
- Să implementeze o interfaţa utilizator centralizata si ergonomica, customizata nevoilor utilizatorilor din ANFP;

Nota: Cerinţele de mai sus vor fi rafinate şi definitivate de către Ofertantul câştigător in timpul fazei de analiza din cadrul implementării proiectului

4.6.2 Cerinţe de arhitectură

Sistemul Informatic Managerial e-ANFP va respecta cerinţele detaliate în cadrul capitolului 3 – ”Arhitectură Sistem Informatic” din prezentul document, cu menţiunea că, pentru implementarea acestei arhitecturi, se vor lua în consideraţie componentele software de bază - respectiv sistem de operare tip server şi sistem relaţional de baze de date – prezentate în cadrul capitolului 4.4 – ”Infrastructură software de bază” (din prezentul document). Oferta va include arhitectura detaliată a Sistemului propus, care va evidenţia (cel puţin) distribuţia maşinilor virtuale per server, numărul de procesoare virtuale şi memoria alocată fiecărei maşini virtuale, componentele software instalate pe fiecare maşină virtuală, tipul distribuţiei componentelor software (Standard / Professional / Enterprise /etc.) precum şi versiunea acestora, repere de interconectare şi de integrare între componente (acolo unde e cazul).

4.6.3 Cerinţe de integrare/interfaţare

Din punct de vedere a integrării/interfaţării Sistemului Informatic Managerial e-ANFP cu alte sisteme (sau aplicaţii informatice) aflate în uz la Achizitor se vor lua în considerare următoarele considerente:

- În cadrul capitolelor de arhitectură funcţională a Sistemului, respectiv 3.1.1 – ”Lucrul cu Fluxuri Informatice” şi 3.1.2 – ”Susţinerea Activităţii Administrative IT” din prezentul document, sunt specificate toate componentele/sistemele informatice utilizate în prezent de către ANFP şi care fac subiectul comunicării (respectiv interfaţării) cu componentele Sistemului Informatic Managerial e-ANFP;
- Specificaţiile tehnice (detaliate) privind interfaţarea Sistemului Informatic Managerial e-ANFP se vor definitive în perioada de analiză din cadrul implementării proiectului (respectiv a Sistemului Informatic Managerial e-ANFP).

4.6.4 Cerinţe de disponibilitate şi scalabilitate

Din punct de vedere al disponibilităţii şi scalabilitatii, Sistemului Informatic Managerial e-ANFP trebuie sa respecte următoarele cerinţe :

- Sa ofere suport pentru înalta disponibilitate, atât din punct de vedere hardware cat si software, astfel :
  - Infrastructura hardware să includă:
    - (minim) 3 servere de aplicaţii (în configuraţii identice) ;
    - (minim) 2 servere de baze de date (în configuraţii identice) ;
  - Serverul pentru stocare unificată să includă (minim) 2 noduri fizice identice (”controller”-e);

- Următoarele echipamentele să fie în număr de (minim) 2 (în configuraţii identice):
    - switch FC,
    - switch Ethernet,
    - de securitate.
  - Memoria folosită în serverele (fizice) de aplicaţii şi baze de date să ofere suport pentru ECC, ”memory mirror” sau tehnologii echivalente;
  - Sursele de alimentare ale serverelor (fizice) să ofere suport pentru redundanţă;
  - Ventilatoarele serverelor (fizice) să ofere suport pentru redundanţă;
  - Serverele să ofere suport pentru utilizarea matricilor RAID.
- Sa ofere suport pentru scalarea sa, atât din punct de vedere hardware cat si software, astfel :
  - Să permită adăugarea de noi servere (fizice) de:
    - aplicaţii,
    - baze de date,
    - stocare unificată.
  - Să permită adăugarea de memorie (suplimentară) serverelor (fizice);
  - Serverele (fizice) sa ofere suport pentru adăugarea ulterioara de hard-disk-uri.

4.6.5 Cerinţe de virtualizare

Sistemul va oferi suport pentru virtualizare astfel pentru :

- Separarea nivelului logic al aplicaţiilor (componente Sistemului Informatic Managerial e-ANFP) de infrastructura hardware (de suport a rulării Sistemului).
- A avea posibilitatea creării de instanţe virtuale multiple la nivel de aplicaţii;
- Alocării dinamice a resurselor fizice către instanţele virtuale care au cea mai mare nevoie de procesare;
- Eliminării eventualelor conflicte la nivel de procesor, memorie sau sistem de operare ce ar putea apărea rulând mai multe aplicaţii in cadrul aceleiaşi instanţe (non-virtuale) de aplicaţie.

Se va evidenţia în cadrul Ofertei corelarea acestor cerinţe cu arhitectura propusă pentru Sistemului Informatic Managerial e-ANFP.

4.6.6 Cerinţe de securitate

Sistemului Informatic Managerial e-ANFP trebuie să îndeplinească următoarele cerinţe (generale) de securitate:

- Să ofere mecanisme şi facilităţi avansate de securitate, pentru:
  - gestiunea bazelor de date;
  - controlul şi monitorizarea accesului la resursele informatice;
  - gestiunea drepturilor şi rolurilor pentru utilizatori;
  - colectarea şi agregarea informaţiilor aferente evenimentelor de securitate;
  - rafinarea rolurilor de administrare in cadrul componentelor sistemului.
- Să ofere suport pentru:
  - Autentificare si autorizare unica;
  - Durata sesiunii active (in urma autentificării) sa fie configurabila dar sa existe si posibilitatea de autorizare pe toata durata sesiunii;
  - Asigurarea accesului (personalului administrativ IT) pe baza de parola si utilizator in baza unui protocol SSL.
- Fiecare componenta a Sistemului Informatic Managerial e-ANFP (server, switch, etc.) ce este interconectata cu o alta resursa in baza protocolului TCP-IP va fi protejata, după caz,

de firewall software (iptables, firewall antivirus, etc.) sau de liste de acces configurate local pe acesta (in cazul echipamentelor hardware sau tip appliance).

- Intercomunicaţia intre resursele Sistemului Informatic Managerial e-ANFP va fi limitata doar pe porturile necesare bunei funcţionări a acestuia.
- Toate serviciile ce nu sunt necesare bunei funcţionări a Sistemului Informatic Managerial e-ANFP vor fi oprite implicit şi vor fi configurate să nu pornească în cazului unui reboot.

4.6.7. Condiţii generale

Ofertantul trebuie să descrie în detaliu metodologia după care va derula activităţile de dezvoltare/configurare şi testare internă şi vor demonstra integrarea acestor proceduri cu procedurile de analiză şi proiectare.

Ofertantul trebuie să prezinte detaliat livrabilele care vor rezulta în urma prestării serviciilor corespunzătoare etapelor de dezvoltare/configurare şi testare internă.

5. Instruirea în cadrul contractului

Oferta trebuie sa cuprindă sesiuni de instruire pentru personalul ANFP, utilizatori finali şi personal administrativ IT, conform cerinţelor detaliate mai jos şi în subcapitolele următoare.

Ofertanţii vor propune în cadrul ofertelor un plan (calendar) de sesiuni de instruire, cu menţiunea că aceste sesiuni se vor încadra în ultimele 4 luni din calendarul implementării proiectului.

Sesiunile de instruire se vor efectua după modelul ”în clasă”. O grupă de cursanţi poate avea maxim 12 membri.

Pe lângă transferul de cunoştinţe de specialitate către utilizatorii şi administratorii Sistemului, sesiunile de instruire a utilizatorilor de la Sediul central al ANFP vor include obligatoriu următoarele două module:

- Modul de dezvoltare durabilă, în care se va urmări atât conştientizarea importanţei acestui concept, cât şi instruirea în domeniul problemelor de mediu
- Modul dedicat temei de egalitate de şanse, în care se va urmări conştientizarea importanţei şi promovarea conceptului de egalitate de şanse.

Serviciile de instruire, model ”în clasă”, vor fi susţinute in Limba Română de către instructori specializaţi ai Ofertantului şi vor avea loc intr-o locaţie pusă la dispoziţie de către ANFP.

Ofertantul câştigător va livra materialele necesare instruirii atât în format electronic, cât şi în format tipărit, cu respectarea prevederilor de identitate vizuala aferente proiectelor finanţate prin Programul Operaţional Dezvoltarea Capacităţii Administrative, în sensul că suportul de curs, materialele de birotica folosite la instruire, slide-urile, precum si diplomele participanţilor la instruire vor trebui să conţină aceste elemente de vizibilitate.

În cadrul sesiunilor de instruire Furnizorul va asigura nu mai târziu de luna a 9 a contractului instruirea personalului ANFP conform prevederilor legale cu privire la:

1. calificări/atestări care să certifice cunoaşterea standardelor ISO/IEC 27001 sau a standardelor echivalente şi a versiunilor ulterioare ale acestora;
2. certificări/atestări în domeniul administrării bazelor de date şi a sistemelor de operare;
3. calificări/atestări în domeniul arhivistic.

Cursurile anterior menţionate pot fi cuprinse şi în cadrul cursurilor identificate mai jos sau pot fi organizate sesiuni distincte dedicate acestora.

5.1 Utilizatori de la Sediul Central

Sesiunile dedicate utilizatorilor finali ai ANFP de la Sediul Central vor ţine cont de următoarele considerente:

Nr.	Denumire curs	Număr de utilizatori instruiţi (per curs)	Număr minim de zile (per curs)	Tip	Observaţii
1	Servicii de digitizare şi arhivare (general)	6	2	Nivel: Mediu Mod: În clasă	Aspecte tehnico-funcţionale privind digitizarea şi arhivarea electronica.
2	Servicii de arhivare (aprofundat)	2	3	Nivel: Avansat Mod: În clasă	Instruire aferentă arhivarii electronice (în sensul Legii nr. 135/2007 (r1), privind arhivarea documentelor in forma electronica şi a Ordinului nr. 493/2009 privind normele tehnice şi metodologice pentru aplicarea Legii nr. 135/2007).
3	Utilizare Sistem Informatic Managerial e-ANFP (general)	48	2	Nivel: Mediu Mod: În clasă	Aspecte tehnico-funcţionale privind utilizarea Sistemului Informatic Integrat e-ANFP, care vor include: • Lucrul cu fluxuri de documente şi captură.
3	Utilizare Sistem Informatic Managerial e-ANFP (aprofundat)	8	5	Nivel: Avansat Mod: În clasă	Aspecte tehnico-funcţionale privind utilizarea Sistemului Informatic Integrat e-ANFP, care vor include: • Lucrul cu fluxuri de documente şi captură; • Lucrul cu fluxuri de integrare şi procese de lucru.

5.2 Utilizatori din teritoriu

Pentru utilizatorii din teritoriu se va crea şi publica (prin intermediul platformei de e-Learning utilizată în prezent de Achizitor) un curs (digital) ce va conţine aspect tehnico-funcţionale de utilizare a semnăturii electronice calificate elaborat pe baza manualul de utilizare a semnăturii electronice şi se va adresa unui profil de utilizator de nivel mediu.

Notă: detalii tehnice privind platforma de e-Learning utilizată în prezent de ANFP vor fi puse la dispoziţia Ofertantului câştigător în perioada de analiză din cadrul implementării proiectului Sistem Integrat Managerial e-ANFP.

5.3. Personal IT

Sesiunile dedicate personalului IT din ANFP (Sediul Central) vor ţine cont de următoarele considerente:

Nr	Denumire	Număr de	Număr	Tip	Observaţii

.	curs	utilizatori instruiţi (per curs)	minim de zile (per curs)		
1	Amenajare cameră servere	2	1	Nivel: Avansat Mod: În clasă	Aspecte tehnico-funcţionale privind utilizarea şi mentenanţa (tuturor) echipamentelor dedicate amenajării camerei serverelor (incluse în proiect).
2	Administrare echipamente şi produse software	4	12	Nivel: Avansat Mod: În clasă	Aspecte tehnico-funcţionale privind administrarea (tuturor) echipamentelor şi produselor software (incluse în proiect), alocându-se astfel: • Server (de aplicaţii şi de baze de date), server de stocare unificată, switch (FC, Ethernet): minim 1 zi; • Echipament de securitate, echipament tip Thin Client: minim 1 zi; • Infrastructură de susţinere a lucrului cu Fluxuri informatice (toate componentele ofertate): minim 5 zile; • Infrastructură de susţinere a Activităţii Administrative IT (toate componentele ofertate): minim 5 zile.
3	Audit de securitate	2	În funcţie de Producător	Nivel: Avansat Mod: În clasă sau clasă virtuală	Instruire EC-Council - ”Certified Security Analyst Course” sau MILE2 - ”Information Systems Security officer” sau echivalent, care va conţine următoarele module: • Managementul securităţii, al riscului şi al incidentelor • Controlul accesului (identificare, autentificare) • Modele de securitate şi criteriu de evaluare • Securitate operaţională • Criptografie (simetrică, hashing, asimetrică,

					PKI) • Securitatea reţelei (protocoale, echipamente, conectică), VPN • Telefonie • Wireless • Securitate fizica • Repere de arhitectură • Tipuri de atacuri • Repere de securitate software (inclusive malware) • Repere de securitate a bazelor de date • Continuitatea business-ului • Recuperarea în caz de dezastru • Repere legislative şi etice Instruirea se va susţine de instructori certificaţi (de către Producătorul cursului) pentru instruire pe cursul propus. Programa cursului va fi programa oficială a Producătorului cursului. Numărul minim de zile va fi cel recomandat de către Producătorul cursului. Validitatea sesiunii propuse în cadrul ofertei va putea fi ulterior verificată de către ANFP la Producătorul (oficial) al cursului.

6. Managementul Contractului, Organizare şi Metodologie

6.1 Cerinţe privind derularea contractului

6.1.1 Management de contract

Activitatea de management de proiect în cadrul proiectului ”*e-ANFP - Întărirea capacităţii instituţionale a ANFP în vederea asigurării unui management performant al funcţiei publice şi funcţionarilor publici la nivelul administraţiei publice centrale şi al serviciilor publice din subordinea/coordonarea autorităţilor publice centrale şi locale prin implementarea de instrumente inovatoare”*, cod SMIS 36675, este asigurată de către echipa de proiect a ANFP.

Ofertantul trebuie să prezinte în cadrul propunerii tehnice descrierea detaliată a metodologiei proprii de management de proiect pe care o va utiliza în cadrul contractului.

Ofertantul trebuie să prezinte în cadrul propunerii tehnice planul (calendarul) de derulare pentru prestarea serviciilor pe toată durata contractului. Planul trebuie să conţină toate activităţile pe care le va desfăşură precum şi etapele/subetapele determinante de realizare a activităţilor, dependenţele dintre activităţi, jaloanele de proiect (milestones), rezultatele activităţilor şi alocarea resurselor în vederea prestării serviciilor ofertate astfel încât să fie atinse obiectivele contractului. Ofertantul trebuie să propună planul de derulare a activităţilor cât mai detaliat posibil şi să răspundă cerinţelor de etapizare şi înscriere în termenele de realizare ale contractului. În perioada ulterioară semnării contractului, planul poate fi modificat doar cu aprobarea Achizitorului.
Implementarea Sistemului Informatic Managerial e-ANFP trebuie să acopere cel puţin următoarele activităţi:

- Analiza;
- Proiectare;
- Dezvoltare/configurare inclusiv testare internă;
- Implementare (deployment) în mediul de producţie;
- Testare şi teste de acceptanţă;
- Intrarea în execuţie.

Planul care va fi prezentat împreună cu oferta trebuie să fie dezvoltat folosind tipurile de activităţi menţionate mai sus împreună cu alte activităţi considerate a fi necesare.
Ofertantul trebuie să prezinte în cadrul propunerii tehnice modalitatea în care se va realiza raportarea progresului pentru activităţile din cadrul contractului, care se va realiza lunar. Se va detalia modul de raportare în ceea ce priveşte intervalele de raportare, formularele folosite, conţinutul informaţional al raportării precum şi circuitul de aprobare al raportărilor de progres lunare.
Ofertantul va prezenta în cadrul propunerii tehnice modul în care se va gestiona rezolvarea problemelor care pot să apară pe parcursul contractului. Se va descrie procesul de management al problemelor şi formularele care vor fi utilizate pentru managementul problemelor, escaladarea şi rezolvarea acestora.
Ofertantul trebuie să prezinte în cadrul proiectului modalitatea (metodologia) prin care se va realiza comunicarea între participanţii la contract.
Ofertantul va prezenta în cadrul propunerii tehnice planul de acceptanţă care va fi utilizat în cadrul proiectului pentru recepţiile/acceptanţele parţiale şi recepţia/acceptanţa finală. Se va prezenta planul împărţit pe etape precum şi formularele aferente recepţiilor/acceptanţelor parţiale şi recepţiei/acceptanţei finale.
Ofertantul va prezenta în cadrul propunerii tehnice şi modalitatea de tratare a schimbărilor în cadrul contractului. Se va prezenta procedura de management al schimbărilor precum şi formularele care vor fi utilizate în cadrul acestui proces pe durata contractului.
Ţinând cont de complexitatea şi durata contractului, Ofertantul trebuie să ia în considerare necesitatea prestării unui număr corespunzător de zile-om pentru activităţile contractului prin alocarea experţilor necesari. În vederea atingerii obiectivelor contractului, prestatorul poate suplimenta numărul de resurse alocat activităţilor pe perioada derulării contractului, fără a afecta bugetul alocat.

6.1.1.1 Raţionament

Oferta prezentată trebuie sa includă:

- Viziunea proprie asupra realizării contractului, din care sa reiasă modul in care a înţeles contextul şi scopul acestuia.
- Identificarea aspectelor esenţiale legate de îndeplinirea obiectivelor contractului şi a rezultatelor aşteptate şi o scurtă descriere a acestora. Se vor prezenta şi detalia minim 5

aspecte considerate esenţiale de către ofertant pentru atingerea obiectivelor contractului de audit.

- Identificarea şi descrierea riscurilor care afectează execuţia contractului de audit şi prezentarea unei soluţii viabile de răspuns la risc. Ofertanţii vor prezenta un registru conţinând cele mai importante 5 riscuri ale contractului. Pentru fiecare risc, se va face o prezentare completă a cauzei, riscului şi efectului, precum şi o analiză a probabilităţii şi impactului. De asemenea, se vor prezenta recomandările/acţiunile planificate de evitare sau reducere.

6.1.1.2 Strategia abordării

Ofertantul va prezenta pe larg (în cadrul ofertei prezentate) organizarea pe care şi-o propune pentru a-şi desfăşura activitatea în cadrul proiectului, conform cu metodologia propusă.

În subcapitolele următoare sunt detaliate cerinţele privind activităţile din cadrul implementării Sistemului e-ANFP.

6.1.2 Analiza

Va presupune analiza tehnică a soluţiei informatice pe baza specificaţiilor rezultate în urma fazei de analiză precum si proiectarea şi programarea soluţiei integrate.
Rolul principal al fazei de analiză este de a înţelege corect obiectivele proiectului înainte de proiectarea şi implementarea unui sistem care să le îndeplinească.
În vederea implementării sistemului, Prestatorul va trebui să execute activităţi de analiză care să asigure premizele unei implementări eficiente.
Achizitorul va acorda tot sprijinul necesar pentru înţelegerea cât mai bună şi completă a contextului în care va fi implementat sistemul.
Ofertantul trebuie să descrie în detaliu metodologia după care va derula activităţile de analiză.
Ofertantul trebuie să descrie instrumentele pe care le vor utiliza astfel încât să poată asigura:

- Colectarea şi evidenţa cerinţelor;
- Trasabilitatea cerinţelor pornind de la obiectivele proiectului până la specificaţiile tehnice pentru demonstrarea acoperirii integrale a tematicii proiectului;
- Modelarea proceselor şi activităţilor în conformitate cu standarde de modelare şi reprezentare recunoscute (UML sau echivalent).

Ofertantul trebuie să prezinte detaliat livrabilele care vor rezulta în urma prestării serviciilor corespunzătoare etapei de analiză. Descrierea trebuie să conţină cel puţin următoarele informaţii:

- Formularul/formularele care vor fi utilizate pentru fiecare livrabil;
- Descrierea conţinutului fiecărui livrabil;
- Modul în care va fi interpretat conţinutul livrabilelor.

Analiza se va efectua după caz la sediul Achizitorului sau la Prestator şi va avea ca finalitate un pachet de specificaţii funcţionale agreat de comun acord. Serviciile de analiză vor acoperi cel puţin următoarele aspecte:

- Analiza contextului existent;
- Înţelegerea structurii organizatorice a Achizitorului;
- Analiza situaţiei din momentul de faţă din cadrul instituţiei Achizitorului prin şedinţe de analiză, chestionare etc. Se vor identifica procesele operaţionale (la nivelul organizaţiei) care vor fi impactate prin implementarea soluţiei proiectului;
- Identificarea nevoilor şi neajunsurilor pe care instituţia doreşte să le rezolve prin realizarea acestui proiect. Prin aceasta se va avea în vedere înţelegerea în detaliu a obiectivelor generale şi specifice ale proiectului;

- Definirea cerinţelor informaţionale pentru noul sistem. Se va contura astfel, imaginea viitorului sistem informaţional prin stabilirea proceselor operaţionale care să precizeze parcipanţii, momentul intervenţiei acestora, locaţia sau contextul, modalitatea de intervenţie şi informaţia procesată. Pentru prezentarea proceselor operaţionale se vor utiliza instrumente de modelare a proceselor şi activităţilor în conformitate cu standarde de modelare şi reprezentare recunoscute (UML sau echivalent);
- Stabilirea actorilor care vor interacţiona în viitorul sistem.

Se vor evidenţia activităţile care urmează a fi automatizate dacă este cazul, astfel încât să se identifice clar funcţiile viitorului sistem informatic şi modul în care acesta va ajuta la îndeplinirea obiectivelor proiectului;
La realizarea imaginii viitorului sistem, se vor avea în vedere sistemele informatice existente, care vor conlucra la îndeplinirea obiectivelor proiectului, indiferent dacă acestea sunt interne sau externe organizaţiei Achizitorului. Se vor avea în vedere volumul şi frecvenţa interacţiunilor de integrare între sisteme.

6.1.2.1 Etape generale

Rolul principal al fazei de analiză şi elaborare a specificaţiilor este de a înţelege corect obiectivele proiectului înainte de proiectarea şi implementarea unui sistem care să le îndeplinească.
Datele de intrare sunt:

- Contractul, pentru termene şi condiţii;
- Propunerea tehnică, pentru aria de acoperire a proiectului;
- Cerinţele clientului colectate şi evaluate în timpul aceste faze.

Procesul constă din următoarele faze :

- Alegerea metodei de colectare a cerinţelor;
- Aplicarea metodei alese de colectare a cerinţelor;
- Evaluarea şi clarificarea cerinţelor;
- Elaborarea specificaţiilor corespunzătoare cerinţelor;
- Analizarea specificaţiilor corespunzătoare cerinţelor împreună cu Achizitorul;
- Aprobarea specificaţiilor corespunzătoare cerinţelor.

6.1.2.2 Etape specifice

În faza de analiza se va ţine cont de cel puţin următoarele etape specifice:

6.1.2.2.1 Stabilirea modelului de securitate

Se vor trata următoarele aspecte:

- Tipuri de utilizatori;
- Roluri;
- Grupuri (respectiv maparea peste organigrama existentă);
- Excepţii;
- Drepturi.

6.1.2.3 Analiza proceselor

6.1.2.3.1 Identificarea proceselor de lucru ce urmează a fi implementate

Se va întocmi o listă cu procesele ce urmează a fi automatizate (şi implementate).

6.1.2.3.2 Identificare scenariilor de utilizare

”Use case diagram” este un tip de diagramă din care reiese modul de utilizare a sistemului informatic - modul în care utilizatorii interacţionează cu acesta (în corespondenţă directă cu task-urile acestor utilizatori). Utilizarea use case diagram este utilă pentru a crea o imagine generală asupra sistemului.

6.1.2.3.3 Identificarea actorilor

Se vor identifica actorii pentru toate fluxurile din pasul anterior. Se vor identifica şi consemna rolurile generale gen: şef departament, director direcţie, utilizator aparţinând unui departament/direcţie, etc.
Pentru specificarea actorilor umani este de preferat să se folosească alias-uri în locul numelor de utilizatori/grupuri. Acest mod de abordare oferă o serie de avantaje printre care: dinamicitatea fluxurilor de lucru, elimina nevoia de a modifica fluxurile în cazul schimbărilor de persoane.

6.1.2.3.4 Identificarea paşilor

Se vor trata următoarele aspecte:

- Paşii manuali;
- Paşii automaţi;
- Deciziile;
- Notificările;
- Ramurile executate în paralel (punctele de split);
- Punctele de reconectare (join);
- Condiţiile de încetare a unui flux;
- Condiţiile de repornire a unui flux (manual/automat).

6.1.3 Proiectare

Rolul principal al fazei de proiectare este de a descrie la un nivel suficient de detaliat sistemul care urmează a fi implementat. În vederea implementării sistemului, Prestatorul va trebui să execute activităţi de proiectare care să asigure premizele unei implementări eficiente.
Proiectarea sistemului dorit, care va conţine detalierea la nivel tehnic a cerinţelor şi specificaţiilor rezultate din activitatea de analiză pentru toate nivelurile şi componentele sistemului care va fi realizat:

- Arhitectura de sistem - va prezenta cel puţin următoarele niveluri: hardware, comunicaţii, componente software instalate (sisteme de operare, produse COTS), arhitectura logică cuprinzând descrierea componentelor de sistem, a celor dezvoltate sau personalizate şi caracteristicile funcţionale şi non-funcţionale ale acestora;
- Scenarii (cazuri) de utilizare - din care să reiasă modul de utilizare a sistemului informatic din perspectiva utilizatorului final, modul în care utilizatorii interacţionează cu sistemul, în corespondenţă directă cu activităţile menţionate în cadrul proceselor operaţionale ale acestor utilizatori. Scenariile de utilizare trebuie să cuprindă şi interacţiunile cu sistemele externe, astfel încât să fie evidenţiat exact modul în care este fructificată o integrare la nivel de sistem informatic. De asemenea, scenariile de utilizare vor fi însoţite de o listă a actorilor sistemului şi maparea acestora cu actorii de business. Pentru prezentarea cazurilor de utilizare se vor folosi instrumente in conformitate cu standarde de modelare şi reprezentare recunoscute (UML sau echivalent);
- Modelul de securitate - la nivel logic (organizarea pe roluri, grupuri, drepturi, poziţia în structura organizatorică etc.) şi la nivel fizic (servere, comunicaţii, aplicaţii etc.);

- Integrările la nivel de componentă software - pentru fiecare interacţiune se va specifica sistemul sursă/destinaţie, modalitatea de implementare, canal de comunicare, setul şi structura de date transferate, reguli specifice de validare etc);
- Rapoarte ce vor fi realizate în cadrul sistemului - vor fi descrise rapoartele, care sunt informaţiile conţinute, care sunt criteriile de filtrare dacă este cazul şi tipul de livrare al acestora (timp real, la cererea utilizatorului sau automatizate la un anumit moment de timp programat apriori).

Proiectarea sistemului trebuie să ofere o soluţie optimă, urmărindu-se uşurinţa şi eficienţa realizării şi implementării soluţiei, în cadrul restricţiilor de ordin tehnic, organizatoric sau financiar. În procesul de proiectare, implicarea Achizitorului este esenţială în confirmarea cerinţelor informaţionale şi a priorităţilor din organizaţie, realizându-se în acest mod înţelegerea şi pregătirea pentru acceptanţa noului sistem. De aceea, este esenţial ca Prestatorul să comunice frecvent cu echipa Achizitorului pe tot parcursul derulării proiectului.
Documentul/documentele de specificaţii, rezultate în urma activităţilor de analiză şi proiectare, vor descrie soluţia în detaliu, vor conţine informaţii privind toate funcţionalităţile necesare şi vor sta la baza stabilirii şi realizării testelor de acceptanţă.
În urma activităţilor de analiză şi proiectare, pentru a se obţine un sistem final operaţional se vor desfăşura activităţi de dezvoltare, configurare, testare şi implementare (deployment).

6.1.4 Dezvoltare, configurare şi testare internă
Ofertantul trebuie să descrie în detaliu metodologia după care va derula activităţile de dezvoltare/configurare şi testare internă şi vor demonstra integrarea acestor proceduri cu procedurile de analiză şi proiectare. Ofertantul trebuie să prezinte instrumentele folosite în desfăşurarea activităţilor de dezvoltare, configurare şi testare internă. Ofertantul trebuie să prezinte detaliat livrabilele care vor rezulta în urma prestării serviciilor corespunzătoare etapelor de dezvoltare/configurare şi testare internă.

6.1.5 Implementare (deployment) în mediul de Producţie
Se va face implementarea aplicaţiei la sediul Achizitorului. Această activitate va presupune instalarea sistemului software pe infrastructura aferentă şi configurarea sistemului software în conformitate cu specificaţiile prevăzute în documentele de analiză acceptate. Ofertantul trebuie să descrie în detaliu metodologia după care va derula activităţile de implementare (deployment) în mediul de Producţie al Achizitorului. Ofertantul trebuie să prezinte împreună cu oferta procedurile de implementare din cadrul propriei organizaţii şi vor demonstra integrarea acestor proceduri cu procedurile referitoare la dezvoltare/configurare şi testare internă.
Ofertantul trebuie să prezinte detaliat livrabilele care vor rezulta în urma prestării serviciilor corespunzătoare etapei de implementare. Descrierea trebuie să conţină cel puţin următoarele informaţii:
- Formularul/formularele care vor fi utilizate pentru fiecare livrabil;
- Descrierea conţinutului fiecărui livrabil;
- Modul în care va fi interpretat conţinutul livrabilelor.

6.1.6 Testarea şi testele de acceptanţă
Activitatea de Testare (şi teste de acceptanţă) va presupune verificarea soluţiei informatice dezvoltate, conform scenariilor de testare agreate în etapa de analiză.
Ofertantul trebuie să descrie modalitatea în care va realiza testarea sistemului şi testele de acceptanţă specifice. Ofertantul trebuie să prezinte metodologia de testare după care se vor realiza activităţile de testare în timpul desfăşurării proiectului. Ofertantul trebuie să prezinte instrumentele de testare folosite.

Achizitorul (cu asistenţa Prestatorului) va rula toate scenariile pentru testele de acceptanţă ale întregului sistem sau componentă livrată. Testele de acceptanţă se vor derula în conformitate cu Planul de Teste realizat de Prestator şi agreat de Achizitor, plan ce va fi în concordanţă cu întregul ciclu de realizare al proiectului: etape de testare distribuite pe iteraţii, seturi de funcţionalităţi sau alte tipuri de teste.
Planul de testare pentru acceptanţă va cuprinde toate testele necesare pentru a demonstra acoperirea în întregime a cerinţelor din prezentul caiet de sarcini. Astfel, se va avea în vedere faptul că sistemul funcţionează corect din punct de vedere al respectării cerinţelor, consistenţei datelor, al constrângerilor de timp, al validărilor de date şi al gestiunii erorilor, inclusiv pentru funcţionalităţile existente care au fost extinse sau modificate. Criteriul de succes - sistemul trece toate testele definite în planul de testare agreat împreună cu Achizitorul.
0 primă variantă a planului de testare va fi prezentată odată cu oferta. Planul detaliat de testare, însoţit de scenariile de testare, va fi realizat de către Prestator şi aprobat de Achizitor înainte de fiecare etapă de testare agreată prin planul de proiect.

6.1.7 Intrarea în producţie
Ofertantul trebuie să prezinte planul care va fi utilizat la trecerea în producţie a sistemului. Planul prezentat trebuie să ţină cont de legăturile logice între subsisteme astfel încât să se asigure o trecere în producţie coerentă şi cu impact minim asupra activităţilor zilnice a angajaţilor Achizitorului.

6.1.5 Echipa de proiect

Pentru efectuarea şi ducerea la bun sfârşit a serviciilor incluse în scopul proiectului (a se vedea capitolul 2.3.1 – ”Servicii” din prezentul document), echipa de proiect propusă de Ofertant va include următoarele profile de experţi:

- Manager proiect;
- Expert componentă managementul documentelor;
- Expert analist de business;
- Expert infrastructură;
- Expert dezvoltator software;
- Expert securitatea informaţiei;
- Expert arhitect de sistem;
- Expert soluţii management de documente;
- Expert soluţii de infrastructură hardware şi software;
- Expert implementare si administrare soluţii de management al performantelor aplicaţiilor;
- Expert implementare si administrare soluţii de securitate a informaţiei si management de incidente;
- Expert audit si securitate;
- Expert arhivist.

În continuare sunt detaliate principalele activităţi vizate a fi îndeplinite de experţi în cadrul proiectului, per profil de expert.

Manager proiect

- Gestionează echipa de experţi şi este responsabil de derularea contractului;
- Alcătuirea calendarului de activităţi corelat cu contractul de prestări servicii şi anexele acestuia, disponibilitatea personalului Achizitor şi resursele disponibile din partea Prestatorului;

- Impunerea, monitorizarea calendarului de activităţi către grupul gestionat;
- Propunerea, acolo unde este cazul, a modificărilor care se impun cu privire la calendarul de activităţi, (re)alocarea resurselor sau modificarea termenelor;
- Menţinerea relaţiei cu toate părţile angrenate în lucrul la proiect precum şi cu echipa de management a proiectului;
- Responsabil cu raportarea privind derularea contractului.

Expert componentă managementul documentelor

Responsabilităţile Expertului component managementul documentelor includ următoarele activităţi specifice:

- Proiectarea (atât la nivel de arhitectură de ansamblu cât şi la nivel de modul constituent) a componentei de management a documentelor;
- Efectuarea configurărilor/dezvoltărilor în cadrul componentei de management documente;
- Efectuarea testărilor la nivel de componentă de management a documentelor şi participarea în cadrul sesiunilor de testare integrată a Sistemului Informatic Managerial e-ANFP;
- Documentarea configurărilor/dezvoltărilor efectuate;
- Participarea (dacă e cazul) la instruirea utilizatorilor/administratorilor şi/sau întocmirea manualelor/documentaţiilor de utilizare a componentei de management a documentelor;
- Definirea/crearea rapoartelor asociate componentei de management a documentelor;
- Participarea la implementarea inter-conectării componentei de management a documentelor cu alte sisteme/componente informatice (ex. structura de Director tip Microsoft Active Directory utilizată de ANFP).

Se impune cel puţin un expert componentă management documente, ajutat dacă va fi cazul de resurse nenominalizate în proiect, deoarece numărul tipurilor de documente de lucru şi numărul fluxurilor asociate sunt semnificative (mai mult de 150 fluxuri de lucru).

Expert analist de business

Responsabilităţile Expertului analist de business includ următoarele activităţi specifice:

- Analiza cerinţelor tehnico-funcţionale ale Achizitorului;
- Participare la modelarea datelor şi la design-ul funcţional şi al rapoartelor;
- Elaborarea fluxurilor de informaţie şi a specificaţiilor de interconectare;
- Suport în definirea ecranelor-utilizator;
- Documentarea activităţilor;
- Colaborarea cu echipele tehnice;
- Asistenţă (dacă e cazul) în sesiunile de testare integrată a Sistemului Informatic.

Se impune cel puţin un expert analist de business, ajutat dacă va fi cazul de resurse nenominalizate în proiect.

Expert infrastructură

Responsabilităţile Expertului infrastructură includ următoarele activităţi specifice:

- Punerea în funcţiune, instalarea şi configurarea echipamentelor (hardware) din cadrul proiectului incluzând servere, echipamente de reţelistică/securitate, etc. (restul de echipamente hardware);
- Documentarea activităţilor efectuate;
- Întocmirea documentaţiilor tehnice de administrare şi participarea, dacă e cazul, la sesiunile de instruire a personalului administrativ ANFP;

- Participarea la sesiunile de testare individuală a echipamentelor precum şi la sesiunile de testare unitară a Sistemului Informatic Managerial e-ANFP.

Se impune cel puţin un expert infrastructură, ajutat dacă va fi cazul de resurse nenominalizate în proiect.

Expert dezvoltator software

Responsabilităţile Expertului dezvoltator software includ următoarele activităţi specifice:

- Instalarea, configurarea diverselor componente (software) utilizate în cadrul proiectului;
- Testarea integrată şi participarea la testarea unitară a Sistemului Informatic Integrat e-ANFP;
- Documentarea pachetelor de lucru;
- Întocmirea documentaţiilor tehnice şi/sau manualelor de utilizare, şi, dacă e cazul, participarea la sesiunile de instruire a utilizatorilor ANFP;
- Colaborarea cu expertul analist de business;
- Întocmirea rapoartelor în cadrul componentelor (software) de lucru.

Se impune cel puţin doi experţi dezvoltatori software, ajutaţi dacă va fi cazul de resurse nenominalizate în proiect.

Expert securitatea informaţiei

Responsabilităţile Expertului de Securitate a informaţiei includ următoarele activităţi specifice:

- Definirea nivelelor de risc acceptabile per domeniu/zona funcţională a Sistemului Informatic Integrat e-ANFP;
- Implementarea celor mai avansate trend-uri în domeniul securităţii informatice în zonele de lucru în cadrul proiectului;
- Auditarea Sistemului Informatic Managerial e-ANFP d.p.d.v. securitate informatică;
- Întocmirea rapoartelor de securitate asociate;
- Colaborarea cu expertul analist de business;

Se impune cel puţin un expert securitatea informaţiei, ajutat dacă va fi cazul de resurse nenominalizate în proiect.

Expert arhitect de sistem

Responsabilităţile Expertului arhitect de sistem includ următoarele activităţi specifice:

- Responsabil cu arhitectura de nivel macro a Sistemului Informatic Managerial e-ANFP;
- Acordarea de suport la definirea modelelor de date, fluxurilor de informaţie, ecranelor utilizator, nevoilor de securitate, definirea rapoartelor;
- Colaborarea cu expertul analist de business;
- Implementarea celor mai avansate trend-uri în domeniul arhitecturii enterprise în zonele de lucru în cadrul proiectului;
- Documentarea activităţii efectuate;
- Acordarea de suport în testarea Sistemului Informatic Managerial e-ANFP;
- Acordarea de suport, dacă va fi cazul, în instruirea utilizatorilor şi/sau personalului administrativ ANFP.

Se impune cel puţin un expert arhitect de sistem, ajutat dacă va fi cazul de resurse nenominalizate în proiect.

Expert soluţii management documente

Responsabilităţile Expertului în soluţii de management al documentelor includ următoarele activităţi specifice:

- Suport în proiectarea la nivel macro a componentei de management a documentelor;
- Implementarea celor mai avansate trend-uri în domeniu în zona managementului de documente;
- Supervizare a configurării/dezvoltării/raportării în cadrul componentei de management a documentelor;
- Participarea, daca e cazul, la întocmirea documentaţiilor şi la sesiunile de instruire de nivel avansat pe componenta de management a documentelor;
- Documentarea pachetelor de lucru;
- Suport în scalarea (şi zonei de Change Management per componentă) Sistemului Informatic Managerial e-ANFP (dacă va fi cazul).

Se impune cel puţin un expert soluţii management documente, ajutat dacă va fi cazul de resurse nenominalizate în proiect.

Expert soluţii de infrastructură hardware şi software

Responsabilităţile Expertului în soluţii de infrastructură hardware şi software includ următoarele activităţi specifice:

- Supervizarea punerii în funcţiune, instalării şi configurării echipamentelor (hardware) din cadrul proiectului incluzând servere, echipamente de reţelistică/securitate, etc. (restul echipamentelor);
- Documentarea pachetelor de lucru per echipament;
- Întocmirea specificaţiilor de scalare (dacă va fi cazul);
- Responsabil pe zona de Change Management în cadrul infrastructurii Sistemului Informatic Managerial e-ANFP (dacă va fi cazul);
- Întocmirea documentaţiilor tehnice de administrare şi participarea, dacă e cazul, la sesiunile de instruire a personalului administrativ ANFP;
- Implementarea celor mai avansate trend-uri în domeniu în zona infrastructurilor hardware-software.

Se impune cel puţin un expert în soluţii de arhitectură hardware şi software, ajutat dacă va fi cazul de resurse nenominalizate în proiect.

Expert implementare soluţii de management al performantelor aplicaţiilor

Responsabilităţile Expertului în implementarea soluţiilor de management a performanţelor aplicaţiilor include următoarele activităţi specifice:

- Analiza detaliată dedicată zonei de management performanţe aplicaţii;
- Instalarea, configurarea şi dezvoltarea în cadrul componentelor de management a performanţelor;
- Testarea unitară a produselor de management a performanţelor aplicaţiilor şi participarea la sesiunile de testare unitară a Sistemului Informatic Integrat e-ANFP;
- Întocmirea documentaţiilor specifice şi acordarea de suport în instruirea personalului administrativ e-ANFP;
- Colaborarea cu experţii pe infrastructură din cadrul proiectului;
- Definirea şi impunerea nivelelor optime de lucru a Sistemului Informatic Integrat e-ANFP pentru atingerea celei mai înalte performanţe posibile.

Se impune cel puţin un expert implementare soluţii de management al performantelor aplicaţiilor, ajutat dacă va fi cazul de resurse nenominalizate în proiect.

Expert implementare soluţii de securitate a informaţiei si management de incidente

Responsabilităţile Expertului în implementarea soluţiilor de Securitate a informaţiei şi management de incidente includ următoarele activităţi specifice:

- Definirea specificaţiilor detaliate de securitate informatică şi în zona managementului de incidente;
- Definirea procedurilor de lucru în cadrul managementului incidentelor;
- Definirea şi implementarea SLA-ului pe zona management incidente;
- Definirea şi implementarea specificaţiilor de Securitate;
- Monitorizarea Sistemului Informatic Integrat e-ANFP dpdv securitate informatică şi management incidente;
- Aplicarea best practice-urilor din domeniu şi impunere celor mai avansat trend-uri în domeniul managementului de incidente;
- Întocmirea rapoartelor de securitate asociate zonei de management incidente;
- Colaborarea cu expertul analist de business;
- Suport în instruirea personalului administrativ ANFP.

Se impune cel puţin un expert implementare soluţii de securitate a informaţiei şi management de incidente, ajutat dacă va fi cazul de resurse nenominalizate în proiect.

Expert audit si securitate

Responsabilităţile Expertului pentru audit şi securitate includ următoarele activităţi specifice:

- Definirea specificaţiilor detaliate de securitate informatică în zona testelor de penetrare;
- Colaborarea cu ceilalţi experţi de securitate din cadrul proiectului;
- Auditul Sistemului Informatic Managerial e-ANFP d.p.d.v. vulnerabilităţi informatice;
- Impunerea celor mai avansate tendinţe din zona protecţiei cibernetice;
- Definirea modului de monitorizare preventivă a securităţii şi complianţei Sistemului Informatic Managerial e-ANFP cu standardele de securitate în domeniu;
- Documentarea pachetelor de lucru;
- Participarea la instruirea personalului administrativ ANFP.

Se impune cel puţin un expert audit şi securitate, ajutat dacă va fi cazul de resurse nenominalizate în proiect.

Expert arhivist

Responsabilităţile Expertului arhivist includ următoarele activităţi specifice:

- Digitizarea documentelor fizice (scanare/captură);
- Procesarea schemei de metadata a documentelor (constituirea indexului acestora);
- Alinierea cu standardele în domeniu şi cu legislaţia arhivelor electronice;
- Constituirea şi documentarea procedurilor şi a fluxului de lucru în digitizare şi arhivare electronica;
- Suport pentru încărcarea cu date (primare) a Sistemului Informatic Integrat e-ANFP;
- Constituirea documentaţiilor/manualelor de instruire şi participarea la sesiunile de instruire din cadrul proiectelor;
- Acordarea de consultanţă de specialitate personalului ANFP implicat în arhivarea documentelor (fizice şi/sau electronice).

Se impun cel puţin cinci experţi arhivişti, ajutaţi dacă va fi cazul de resurse nenominalizate în proiect.

■ Niciun expert propus nu trebuie să se afle în vreun conflict de interese cu responsabilităţile acordate lor şi/sau cu activităţile pe care le vor desfăşura în cadrul contractului. În plus, pe toată durata de implementare a contractului, Prestatorul va lua toate măsurile necesare pentru a preveni orice situaţie de natură să compromită realizarea cu imparţialitate şi obiectivitate a activităţilor desfăşurate pentru realizarea obiectivelor contractului.

Prestatorul, în desfăşurarea activităţii sale, este obligat să respecte legislaţia specifică privind protecţia muncii. Informaţii detaliate privind reglementările care sunt în vigoare la nivel naţional şi se referă la condiţiile de muncă şi protecţia muncii, securităţii şi sănătăţii în muncă, se pot obţine de la Inspecţia Muncii sau de pe site http://www.inspectmun.ro/Legislatie/legislatie.html . Propunerea tehnică va fi însoţită de **Formularul nr. 24 -** Declaraţie prin care ofertantul să confirme că la elaborarea ofertei, a ţinut cont de obligaţiile referitoare la condiţiile de muncă şi protecţia muncii, care sunt la nivel naţional, precum şi că le va respecta pe parcursul îndeplinirii contractului de servicii. Informaţii detaliate privind reglementările care sunt în vigoare la nivel naţional şi se referă la condiţiile de muncă şi protecţia muncii, securităţii şi sănătăţii în muncă, se pot obţine de la Inspecţia Muncii sau de pe site http://www.inspectmun.ro/Legislatie/legislatie.html .

In cazul unei asocieri, aceasta declaraţie va fi prezentată de către liderul asocierii.

6.1.6 Bugetul proiectului

În întocmirea ofertei financiare, Ofertantul va avea în vedere/ respecta următoarea structură bugetară:

Activitatea	Tip de cheltuială	Număr de unităţi	Valoare totală (fără TVA) (lei)
Proiectarea şi implementare a Sistemului Informatic Managerial	***Total :***		**11.662.986,42**
	11.2. Întreţinere, actualizare şi dezvoltare aplicaţii informatice	1	430.986,42
	11.3. Cheltuieli pentru cablare reţea internă (Data Center)	1	105.000
	9.2. Cheltuieli cu achiziţia de echipamente de protecţie a valorilor umane şi materiale (camera ignifuga si Data Center)	1	35.000
	8.5. Cheltuieli cu achiziţionarea materialelor şi serviciilor de întreţinerea curentă a sediului (camera ignifuga si Data Center)	1	30.000
	6.4. Cheltuieli pentru închiriere servicii de transport (mutare servere)	1	30.000
	8.3. Cheltuieli de arhivare şi securizare documente/informaţii (camera ignifuga si Data Center)	1	40.000
	9.3. Cheltuieli cu achiziţia de echipamente de calcul şi echipamente periferice de calcul	3 servere aplicaţii 2 servere baza de date 1 unitate de stocare 1 rack	1.371.000

		1 scanner A3	
		1 UPS	
		4 scanner A4	
		2.000 token	
	10.2. Cheltuieli cu achiziţia de licenţe	2.000 licenţe semnătură electronică	9.400.000
		10.000.000 pagini	
		remodelare/actualizare fluxuri informatice	
		licenţe sistem de operare servere (5)	
	11.1. Instalare, întreţinere şi reparare echipamente informatice, de comunicaţii, periferice de calcul şi instalaţii, necesare desfăşurării proiectului	1	35.000
	5.1 Cheltuieli cu tipărirea, multiplicarea şi distribuţia de materiale efectuate în cadrul proiectelor finanţate prin PODCA	4100 exemplare – manual	123.000
		1000 exemplare – ghid	63.000
		2000 – ghid format CD	

Notă : Echipamentele propuse în propunerea tehnică şi bugetate în oferta financiară nu vor depăşi per total valoarea de 1.371.000 lei (fără TVA) aferentă liniei bugetare *9.3. Cheltuieli cu achiziţia de echipamente de calcul şi echipamente periferice de calcul.*

6.1.7 Alte cerinţe

Răspunsurile simple de tipul ”OK”/”100%”/„Soluţia răspunde la cerinţă” sau simpla conversie a cerinţei în răspuns (eventual schimbând timpul verbului) nu sunt acceptate şi se va considera că oferta nu răspunde cerinţelor minime obligatorii.

Arhitectura sistemului propus in oferta va evidenţia componentele solicitate în cadrul capitolelor 4.2 – ”Infrastructură de susţinere a lucrului cu fluxuri informatice”, 4.3 – ”Infrastructura de susţinere a activităţii administrative IT” şi 4.4 – ”Infrastructură software de bază” din prezentul document într-un mediu de producţie, cât şi un mediu de test constituit din soluţiile de management a documentelor (utilizând minim 2 nuclee) şi fluxuri de integrare (utilizând minim 2 nuclee), precum şi sistemul relaţional de baze de date aferent (utilizând minim 2 nuclee).

Totodată ofertantul va trebui să detalieze şi lista licenţelor propuse în oferta tehnică, specificând în clar numele licenţei de la producător, ediţia, producătorul, cantitatea şi unităţile de licenţiere specifice producătorului (de exemplu „User” sau „Processor Core”, etc.), precum şi corelarea acestora cu cerinţele Caietului de Sarcini. Lista licenţelor trebuie să cuprindă toate licenţele propuse de ofertant, în caz contrar oferta va fi declarată neconformă.

Tot în cadrul acestei secţiuni, ofertantul va trebui să prezinte lista echipamentelor hardware specificând în clar identificatorul unic producător (part-number) asociat fiecărui echipament, numărul de echipamente ofertate pentru fiecare tip de echipament, configuraţia acestora, precum şi corelarea acestora cu cerinţele din Caietul de sarcini. Nu se acceptă echipamente scoase din fabricaţie (End of life - EOL). Se acceptă livrarea doar de echipamente noi.

Toate documentele referite care sunt parte a ofertei vor fi nominalizate individual în cuprinsul ofertei precizând numărul paginii la care poate fi regăsit.

Ofertantul va include specificaţiile tehnice ale tuturor produselor software/ echipamentelor hardware, consumabilelor de proces şi, după caz, ale instalaţiilor/ utilajelor tehnice prevăzute în ofertă, sub formă de fişe tehnice din care să rezulte îndeplinirea cerinţelor funcţionale precizate

în Caietul de sarcini, respectiv documentele oficiale care provin de la producători şi/sau rapoartele de încercări/ testări emise de laboratoare de încercare sau organisme de certificare şi inspecţie, din cadrul cărora să rezulte modul de îndeplinire a parametrilor solicitaţi, precum şi condiţiile de vânzare, garanţie şi punere în funcţiune a acestora.
Oferta va include capitol separate de: înţelegere a proiectului; plan de testare de nivel înalt; metodologie de dezvoltare agila, iterativa; procedura de management a incidentelor, procedura de management al schimbărilor; cuprins/opis cu documentaţiile referite, referinţa la pagini in cadrul ofertei/documentelor; documentaţii tehnice, condiţii de vânzare, de garanţie, de suport si de punere in funcţiune; plan de intervenţie.
Ofertele vor include toate informaţiile şi documentele (în original sau în copie) despre certificări de calitate şi conformitate cu standardele relevante şi, respectiv cu normele şi recomandările Uniunii Europene pentru echipamente - cel puţin în ceea ce priveşte securitatea şi interoperabilitatea electrică şi electrostatică, securitatea operatorului uman, emisiile sonore şi de radiaţii, ergonomia şi fiabilitatea etc.
Documentele relevante vor fi emise exclusiv de către autorităţile tehnice şi de certificare independente recunoscute şi consacrate (în afara cazului în care uzanţele sau normele aplicabile admit declaraţia pe propria răspundere a producătorului, sau altele asemenea). Ofertantul va prezenta pentru toate produsele ofertate copii după certificatele emise de instituţiile acreditate să elibereze respectivele certificări. Neprezentarea acestor documente va conduce la descalificarea ofertei ca neconformă.
Ofertele vor include cheltuielile aferente tipăririi, multiplicării şi distribuţiei de material efectuate în cadrul proiectului cu de finanţare PO DCA, luându-se în calcul 4100 (exemplare) de manuale, 1000 (exemplare) ghid-uri şi 2000 (bucăţi) discuri optice (CD).

Notă:
Conţinutul materialelor va fi pus la dispoziţie de către Prestatorul şi agreat de către Achizitor, Prestatorul având următoarele obligaţii :

- *realizarea concepţiei grafice – a imaginii vizuale a materialelor*
- *machetarea textelor*
- *pregătirea pentru tipar*
- *tipărirea materialelor*

7. Garanţia în cadrul proiectului

7.1 Garanţie software

Se vor include în Ofertă servicii de garanţie software pentru Sistemul Informatic Integrat e-ANFP după cum urmează:

- Toate componentele şi sub-componentele proiectului produse de tip COTS (”Commercial off-the-shelf”) precum şi certificatele aferente semnăturii electronice calificate vor avea o perioadă de suport de la producător de minim 12 luni.
- Perioada de garanţie pentru toate configurările şi dezvoltările din cadrul componentelor Sistemului va fi de minim 36 de luni de la recepţia finală.

Serviciile de garanţie prestate vor include minim următoarele:

- Diagnosticarea, izolarea si remedierea defectelor software semnalate de către ANFP;
- Asistenta cu instalarea de actualizări si noi versiuni de programe puse la dispoziţie de către producătorii de software tip „commercially available off-the-shelf” inclus in cadrul ofertei/Sistemului e-ANFP care vor putea fi aplicate fără sa afecteze funcţionarea Sistemului sau sa necesite noi dezvoltări ale componentelor Sistemului.

- Asistenta acordata ANFP pentru aplicarea corecţiilor ca urmare a remedierii defectelor semnalate.

Serviciile de garanţie software din cadrul proiectului vor fi disponibile in toate zilele lucrătoare (8x5) prin intermediul unui sistem de help-desk si trebuie sa garanteze remedierea defectelor software semnalate de ANFP conform următorului tabel de gravitate (SLA):

Nivel de gravitate	Descriere	Reacţie iniţială a Ofertantului Câştigător (ore)	Timp total de soluţionare a defectului software (zile lucrătoare)
1	Defect major, sistemul nu este funcţional	1	1
2	Defect mediu, unele funcţii sau componente ale sistemului nu sunt funcţionale	4	2
3	Defect minor, unele funcţii sau componente ale sistemului sunt afectate dar funcţionale	8	4

Se va include în ofertă planul detaliat privind garanţia software asigurata in cadrul proiectului care sî includă etape, activităţi, actori, termene, proceduri/fluxuri de lucru.

7.2 Garanţie hardware

Se vor include în Ofertă servicii de garanţie hardware pentru toate echipamentele oferite, astfel:

- Perioada de garanţie pentru echipamentele incluse în capitolul 4.5 – ”Infrastructură hardware” din prezentul document trebuie sa fie de minim 36 luni de la achiziţionarea acestora;
- Pentru orice alt echipament ofertat se vor prevede (minim) 12 luni de garanţie de la achiziţionare.

Serviciile de garanţie hardware pentru componentele din cadrul proiectului, oferite la Sediul ANFP, vor fi disponibile în toate zilele lucrătoare (5x8) şi vor fi solicitate prin intermediul unui sistem de help-desk (pus la dispoziţia proiectului de către Ofertantul câştigător). Ofertantul câştigător va trebui sa se prezinte la fata locului pentru constatarea defecţiunii in maxim 4 ore de la semnalarea acesteia de către Achizitor, diagnosticarea defecţiunii se va face in maxim 8 ore de la constatarea acesteia, iar înlocuirea sau repararea componentelor hardware defecte se va face în decurs de maxim 20 zile calendaristice de la diagnosticarea defecţiunii. Se va include în ofertă planul detaliat privind garanţia hardware asigurata in cadrul proiectului care va conţine etape, acţiuni, proceduri de lucru, termene şi actori implicaţi.

8. LOGISTICA SI PLANIFICARE

8.1 Locul de derulare al contractului: România, Bucureşti şi în locaţia situată la maxim 400 km de Bucureşti

8.2. Durata Contractului:

Durata prezentului contract este de 12 de luni de la data semnării contractului dar nu mai târziu de 25.11.2015 şi va fi coroborată cu perioada de implementare a proiectului, putând fi prelungită, prin act adiţional, în funcţie de prelungirea perioadei de implementare a proiectului.

8.3 Recepţia

Operaţiunile recepţiei implică:
- recepţia calitativa si cantitativa a serviciilor prestate;
- certificarea serviciilor prestate;
- identificarea documentelor şi/sau materialelor elaborate;
- constatarea eventualelor neconcordanţe faţă de propunerea tehnică;
- constatarea eventualelor deficienţe ale serviciilor prestate.

Operaţiunile precizate mai sus fac obiectul unui Proces verbal de recepţie întocmit de către Achizitor, semnat atât de către acesta cât şi de Prestator.
Prestatorul are obligaţia de a remedia deficienţele semnalate, în termen de 10 zile lucrătoare de la data luării la cunoştinţă a Procesului verbal de recepţie.

Recepţia cantitativă
Pentru toate produsele, recepţia cantitativă se va face la data livrării pentru fiecare tip de echipament şi pachet software şi va consta în:
a) verificarea cantitativă, inclusiv starea generală aparentă, modul de ambalare şi starea
b) ambalajelor;
c) verificarea concordanţei cu certificatul de garanţie;
d) verificarea existenţei documentaţiei tipărite sau pe CD/DVD pentru toate produsele;
e) verificarea existenţei licenţelor, kit-urilor şi CD/DVD-urilor pentru produsele software aferente echipamentelor livrate;
f) verificarea existenţei licenţelor, kit-urilor şi CD/DVD-urilor pentru pachetele software care fac parte din soluţia ofertată;
g) încheierea procesului verbal de predare/primire, semnat de ambele părţi.

Recepţia calitativă
Pentru toate echipamentele şi pachetele software solicitate sau/şi care fac parte din soluţia ofertată, recepţia calitativă se face la locul livrării, în prezenţa Comisiei de recepţie a achizitorului şi a personalului de specialitate pus la dispoziţie de prestator şi se va consemna în procese verbale de punere în funcţiune.
Recepţia calitativă se face în termen de maxim 7 zile calendaristice, după livrare, şi va constă în:
a) instalarea şi punerea în funcţiune a fiecărui echipament (inclusiv a produselor software aferente (ex: sistem de operare drivere) precum şi a pachetelor software;
b) verificarea configuraţiei produselor livrate, în conformitate cu cerinţele din Caietul de sarcini
c) testarea şi verificarea condiţiilor tehnice specificate de producător;
d) configurarea tuturor produselor software livrate;
e) verificarea funcţionării corespunzătoare a fiecărui echipament şi pachet software;
f) predarea raportului de instalare de către prestator;
g) încheierea procesului verbal de punere în funcţiune, semnat de ambele părţi.

Constatarea în timpul recepţiei a unor deficienţe în funcţionarea produselor sau neconcordanţe între caracteristicile tehnice şi funcţionale din caietul de sarcini şi ofertă şi produsele livrate, atrage după sine obligativitatea prestatorului de înlocuire/remediere a acestora în termen de maxim 10 zile lucrătoare cu produse corespunzătoare, caz în care se va semna un nou proces verbal de punere în funcţiune.
Testarea şi acceptanţa sistemului informatic managerial va cuprinde cel puţin următoarele etape:
- testarea individuală a tuturor echipamentelor care compun sistemul
- testarea individuală a tuturor modulelor noi de aplicaţii software care se vor dezvolta în cadrul contractului
- testarea individuală a tuturor modulelor dezvoltate de către prestator, prin derularea unui program de pilotare a sistemului informatic (inclusiv conţinut)

- testare finală a sistemului (inclusiv a conţinutului dezvoltat, cu încorporarea rezultatelor programului de pilotare)

Acceptanţa sistemului se va realiza prin semnarea raportului final de acceptanţă de către Comisia de recepţie desemnată de Achizitor.
După finalizarea tuturor etapelor parţiale de testare conform contractului, pe baza Proceselor verbale de recepţie parţială, prestatorul va notifica achizitorul şi va solicita întrunirea Comisiei de recepţie în vederea recepţiei finale a sistemului. În termen de maxim 7 zile de la această notificare, Achizitorul va întruni Comisia de recepţie şi, împreună cu reprezentanţii prestatorului, vor efectua recepţia finală a sistemului.

8.4 Modul de prezentare a propunerii tehnice

Ofertantul trebuie să prezinte în cadrul propunerii tehnice descrierea detaliată a metodologiei proprii de prestare a serviciilor (cerinţa minima):

a) Descrierea detaliata a etapelor de derulare, propuse de ofertant, pentru realizarea activităţilor, in vederea îndeplinirii contractului, inclusiv punctele de referinţa, precum si rezultatele si documentele ce trebuiesc prezentate pentru fiecare activitate.
b) Definirea atribuţiilor si responsabilităţilor experţilor pentru ducerea la îndeplinire in cele mai bune condiţii a activităţilor si obţinerea rezultatelor aşteptate. In cazul in care contractul este atribuit unui grup de operatori economici, se descriu input-urile fiecărui membru al grupului precum si distribuirea si interacţiunea sarcinilor si responsabilităţilor dintre ei in derularea contractului.
c) Descrierea facilităţilor suport (resurse tehnice, logistice, administrative, etc) pe care ofertantul le pune la dispoziţie, în scopul realizării activităţilor propuse.

Ofertantul trebuie să prezinte în cadrul propunerii tehnice planul (calendarul) de proiect pentru prestarea serviciilor pe toată durata contractului. Planul de proiect trebuie să conţină toate activităţile pe care le va desfăşura precum şi etapele/subetapele determinante de realizare a activităţilor, dependenţele dintre activităţi, jaloanele de proiect (milestones), rezultatele activităţilor şi alocarea resurselor în vederea prestării serviciilor ofertate astfel încât să fie atinse obiectivele proiectului. Ofertantul trebuie să propună planul de proiect cât mai detaliat posibil şi să răspundă cerinţelor de etapizare şi înscriere în termenele de realizare ale proiectului. În perioada de iniţiere a proiectului, ulterior semnării contractului, planul de proiect poate fi modificat doar cu aprobarea Achizitorului.
Ofertantul trebuie să prezinte în cadrul propunerii tehnice modalitatea în care se va realiza raportarea progresului pentru activităţile din cadrul proiectului. Se va detalia modul de raportare în ceea ce priveşte intervalele de raportare, formularele folosite, conţinutul informaţional al raportării precum şi circuitul de aprobare al raportărilor de progres.
Ofertantul va prezenta în cadrul propunerii tehnice modul în care se va gestiona rezolvarea problemelor care pot să apară pe parcursul proiectului. Se va descrie procesul de management al problemelor şi formularele care vor fi utilizate pentru managementul problemelor, escaladarea şi rezolvarea acestora.
Ofertantul trebuie să prezinte în cadrul proiectului modalitatea (metodologia) prin care se va realiza comunicarea între participanţii la proiect.
Ofertantul va prezenta în cadrul propunerii tehnice planul de acceptanţă care va fi utilizat în cadrul proiectului pentru recepţiile/acceptanţele parţiale şi recepţia/acceptanţa finală. Se va prezenta planul împărţit pe etape precum şi formularele aferente recepţiilor/acceptanţelor parţiale şi recepţiei/acceptanţei finale.
Ofertantul va prezenta în cadrul propunerii tehnice şi modalitatea de tratare a schimbărilor în cadrul proiectului. Se va prezenta procedura de management al schimbărilor precum şi formularele care vor fi utilizate în cadrul acestui proces pe durata proiectului.

Ţinând cont de complexitatea şi durata proiectului, Ofertantul trebuie să ia în considerare necesitatea prestării unui număr corespunzător de zile-om pentru activităţile proiectului prin alocarea experţilor necesari. În vederea atingerii obiectivelor proiectului, prestatorul poate suplimenta numărul de resurse alocat activităţilor pe perioada derulării proiectului.

Strategia abordării
Ofertantul va prezenta pe larg (în cadrul ofertei prezentate) organizarea pe care şi-o propune pentru a-şi desfăşura activitatea în cadrul proiectului, conform cu metodologia propusă.

Ofertantul va prezenta în cadrul propunerii tehnice relaţionarea ofertei cu specificaţiile Caietului de sarcini cu specificarea capitolului/subcapitolului/pagina în care se regăseşte demonstrarea îndeplinirii fiecărei cerinţe, urmărind structura Caietului de Sarcini.

8.5 Modul de prezentare a propunerii financiare

Ofertantul va elabora Propunerea financiara astfel încât aceasta sa furnizeze toate informaţiile solicitate cu privire la preţ.
Ofertanţii trebuie sa prezinte Formularul 21 (Formular de oferta) care reprezintă elementul principal al propunerii financiare. Preţul contractului de achiziţie publica va fi cel rezultat in urma etapei finale a licitaţiei electronice şi va fi ferm pe toată durata de derulare a contractului.
Preturile vor fi fără zecimale.
Preturile din Formularul de oferta nu includ taxa pe valoarea adăugata si vor fi exprimate in LEI cu prezentarea TVA separat. Propunerea financiară trebuie sa includă: Formularul de oferta (Formularul nr.21 din Secţiunea III - Formulare) Centralizatorul de preturi - formular 22- si Graficul de plăţi – formular 23; Preturile vor fi finale si vor cuprinde toate taxele si costurile aferente. Propunerea financiara va fi întocmita pentru toata cantitatea de servicii si produse solicitata prin Caietul de sarcini, cu respectarea tipului de cheltuieli conform bugetului contractului prezentat anterior.
Preturile unitare vor fi fixe şi nerevizuibile pe toata durata de execuţie a contractului.

8.6 Dispoziţii generale

Toate rapoartele, datele, materialele compilate sau produse de Prestator în cadrul acestui contract vor constitui proprietatea Autoritarii contractante a contractului – *Agenţia Naţională a Funcţionarilor Publici*.

Prestatorul va trata toate documentele, datele şi informaţiile cu care va intra în contact sau pe care le va accesa, ca având caracter personal şi confidenţial, şi se va conforma în consecinţă tuturor legilor, normelor şi reglementărilor în vigoare din România. Excepţie vor face documentele din cadrul prezentului dosar de achiziţie publică, aşa cum este definit de prevederile OUG 34/2006 cu modificările şi completările ulterioare. De asemenea, cu excepţia cazului în care este necesar ca Prestatorul să dezvăluie anumite informaţii în scopul executării contractului sau în cazul în care documentele menţionate mai sus au caracter de informaţie de interes public, Prestatorul nu va publica sau dezvălui nici o informaţie fără acordul prealabil scris al AC. În caz de dezacord, primează decizia AC.

Orice documente sau materiale elaborate ori compilate de către Prestator sau de către personalul său salariat ori contractat în executarea prezentului contract, vor deveni proprietatea exclusivă a Achizitorului. După încetarea prezentului contract, Prestatorul nu va utiliza documentele si/sau materialele realizate in prezentul contract în scopuri care nu au legătură cu prezentul contract fără acordul scris prealabil al Achizitorului.

Prestatorul nu va publica articole referitoare la obiectul prezentului contract, nu va face referire la aceste servicii în cursul executării altor servicii pentru terţi şi nu va divulga nicio informaţie furnizată de Achizitor, fără acordul scris prealabil al acestuia.
Orice rezultate ori drepturi, inclusiv drepturi de autor sau alte drepturi de proprietate intelectuală ori industrială, dobândite în executarea prezentului contract vor fi proprietatea exclusivă a Achizitorului, care le va putea utiliza, publica, cesiona ori transfera aşa cum va considera de cuviinţă, fără limitare geografică ori de altă natură, cu excepţia situaţiilor în care există deja asemenea drepturi de proprietate intelectuală ori industrială.
Este înţelegerea părţilor că exercitarea drepturilor conferite prin prezentul Contract şi îndeplinirea obligaţiilor aferente se vor face în deplină conformitate cu dispoziţiile legale relevante, în special în materia respectării mediului concurenţial normal şi a legislaţiei privind drepturile de autor şi drepturile conexe.
Toate produsele software incluzând know-how–ul şi documentele asociate, furnizate de Prestator în cadrul prezentului Contract şi dezvoltate anterior intrării în vigoare a prezentului Contract sunt şi vor rămâne proprietatea Prestatorului sau a terţelor părţi care le-au dezvoltat, către Achizitor fiind transferate drepturile de utilizare.
Drepturile de autor pentru codul sursă al produselor dezvoltate în cadrul prezentului proiect vor fi transferate Achizitorului.
Achizitorul primeşte dreptul de utilizare perpetuă, neexclusivă, irevocabilă şi netransferabilă asupra produselor furnizate.
Acordurile de licenţiere nu vor include niciun fel de clauză limitativă suplimentară faţă de prevederile caietului de sarcini.