

AUTORITATEA CONTRACTANTA

Caiet de sarcini
pentru

OFICIUL NAȚIONAL
AL REGISTRULUI COMERȚULUI

Nr. înregistrare: 70915
Data: 21.12.2019

implementarea unui "Sistem Informatic pentru îmbunătățirea capacității de publicare a actelor operatorilor economici, de colaborare între angajați și de asigurare a securității și monitorizării sistemului informatic integrat ce susține procesele de furnizare a serviciilor publice aflate în responsabilitatea Oficiului Național al Registrului Comerțului"

72200000-7 Servicii de programare și de consultanță software (Rev.2)

30211300-4 Platforme informatice

48000000-8 Pachete software și sisteme informatice

72240000-9 Servicii de analiză și de programare de sisteme

72262000-9 Servicii de dezvoltare software (Rev.2)

72590000-7 Servicii informatice profesionale

48900000-7 Diverse pachete software și sisteme informatice

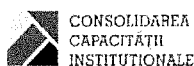
51612000-5 Servicii de instalare de echipament de procesare a informațiilor (Rev.2)

80533100-0 Servicii de formare în informatică

48820000-2 Servere

32420000-3 Echipament de rețea (Rev.2)

32570000-9 Echipament de comunicații



Proiect cofinanțat din Fondul Social European prin
Programul Operațional Capacitate Administrativă 2014-2020!



Cuprins

1	Date generale	5
1.1	Structura organizatorică	5
1.2	Locații implementare proiect	5
1.3	Legislația privind organizarea și funcționarea instituției	5
1.4	Descrierea instituției	6
2	Obiectivul achiziției	11
2.1	Obiectivul general	11
2.2	Scopul proiectului	12
2.3	Situația actuală (Sisteme existente)	13
3	Descrierea noului sistem informatic	43
3.1	Rezultate așteptate	43
3.2	Utilizatorii noului sistem informatic	47
4	Cerințe privind soluția tehnică	53
4.1	Cerințe generale	53
4.2	Cerințe funcționale	56
4.3	Arhitectura generală a sistemului	66
4.4	Descrierea nivelului tehnic al sistemului	80
4.5	Cerințe de livrare și implementare	204
4.6	Organizarea și coordonarea proiectului	205
4.7	Riscuri identificate	223
4.8	Cerințe specifice	226
4.9	Evaluarea performanței Contractantului	227
5	Cerinte experti cheie	228
5.1	Structura echipei de proiect	228
5.2	Responsabilitățile experților cheie	229
5.3	Cerinte minime obligatorii ale experților cheie	233
6	Modalitatea de întocmire a ofertei	238
7	Criterii de atribuire	240

7.1	Descrierea modalitatii de punctare a factorului de evaluare "Pretul ofertei"	241
7.2	Descrierea modalitatii de punctare a factorului de evaluare "Propunerea tehnică – Capabilitati solutie tehnica"	241
7.3	Descrierea modalitatii de punctare a factorului de evaluare "Propunerea tehnica - Experița profesionala a personalului"	244
7.4	Descrierea modalitatii de punctare a factorului de evaluare "Propunerea tehnică - Demonstrarea unei metodologii adecvate de implementare a contractului"	246
8	Cerinte pentru sesiunea demonstrativa	246
9	Drepturi de proprietate intelectuala	249
10	Modalitatea de înlocuire a personalului de specialitate nominalizat pentru îndeplinirea contractului.	250
11	Modalitatea de plată	250
12	Informatii finale	252
	Anexa 1 - Lista locațiilor semnificative la nivelul proiectului – ONRC, ORCT București și ale ORCT Brașov ..	254
	Anexa 2 – Indicatori de performanta pentru realizarea activitatilor din contract	255

Cuprins figuri:

Figură 1	Arhitectura hardware ONRC (mediu de productie)	25
Figură 2	Distributia aplicatiilor si bazelor de date pe servere	26
Figură 3	Arhitectura fizica ORCT Bucuresti	32
Figură 4	Arhitectura fizica ORCT Medii si Mici	35
Figură 5	Utilizatorii interni ai sistemului	48
Figură 7	Utilizatori externi ai sistemului	52
Figură 8	Descrierea generală a arhitecturii a BERC	57
Figură 9	Schema generală flux de publicare Buletinul Electronic al Registrului Comertului	59
Figură 10	Arhitectura generala a sistemului	67
Figură 11	Arhitectura logica subsistem BERC	70
Figură 12	Arhitectura logica Subsistem Colaborare	71
Figură 13	Arhitectura logica propusa subsistem BERC	72
Figură 14	Schema de baza a subsistemului tehnic de procesare, stocare si integrare a datelor	76
Figură 15	Schema de baza a subsistemului tehnic de monitorizare generala a datelor	77
Figură 16	Schema de baza a subsistemului tehnic de securitate si audit	78
Figură 17	Niveluri arhitecturale	80



Abrevieri și denumiri

Termen	Explicație
AC	Autoritatea contractantă
AMPOC	Autoritatea de Management pentru Programul Operațional Competivitate
ACP	Autoritate de Certificare și Plată
BPI	Buletinul Procedurilor de Insolvență
EC	Comisia Europeană
G2B	Government to Business
G2C	Government to Citizen
G2G	Government to Government
MCSI	Ministerul Comunicațiilor și Societății Informaționale
MFP	Ministerul Finanțelor Publice
MFE	Ministerul Fondurilor Europene
ONRC	Oficiul Național al Registrului Comerțului
OIPSI	Organism Intermediar pentru Promovarea Societății Informaționale
ORCT	Oficiul Registrului Comerțului de pe lângă Tribunale
RCCC	Registrul Comerțului Central Computerizat al Oficiului Național al Registrului Comerțului
RC	Registrul Comerțului
BPI	Buletinul Procedurilor de Insolvență
RL	Registrul Litigiilor
SAE	Sistem de Arhiva Electronică
SOA	Service Oriented Architecture
SE	Sistemul Existent (sistemul informatic existent al ONRC)
BPEL	Business Process Execution Language – limbaj de definire a proceselor de afacere
UE	Uniunea Europeană
SNADR	Strategia Națională pentru Agenda Digitală România 2020
TIC	Tehnologia Informației și Comunicații

1 Date generale

Prezentul caiet de sarcini conține cerințele generale ale Oficiului Național al Registrului Comerțului (ONRC) în vederea atribuirii contractului având ca obiect achiziționarea unui sistem informatic, compus din produse hardware, software și servicii de dezvoltare software, în vederea atingerii obiectivelor sale strategice, prevăzute în legislația aplicabilă și în strategiile sectoriale.

1.1 Structura organizatorică

Oficiul Național al Registrului Comerțului (ONRC) este o instituție publică cu personalitate juridică, organizată în subordinea Ministerului Justiției, finanțată integral de la bugetul de stat prin bugetul Ministerului Justiției.

În subordinea ONRC sunt organizate 42 birouri teritoriale, fără personalitate juridică, care funcționează pe lângă tribunale.

1.2 Locații implementare proiect

Proiectul va fi implementat la nivel național, în 2 centre de date, și anume:

- la unul din sediile din București ale Oficiului Național al Registrului Comerțului (ONRC/ORCT București), considerat site principal;
- la sediul ORCT Brașov, considerat site secundar.

și implică toate cele 42 birouri ale registrului comerțului teritoriale (ORCT) precum și sediile birourilor teritoriale care funcționează pe lângă ORCT.

Adresele locațiilor menționate sunt prezentate în **Anexa 1**.

În afara birourilor teritoriale existente, se pot deschide și alte birouri teritoriale în orașele mari din diferite județe, unde numărul persoanelor supuse obligației de înregistrare în registrul comerțului este relativ mare.

1.3 Legislația privind organizarea și funcționarea instituției

Funcționarea și organizarea Registrului Comerțului și Buletinul Procedurilor de Insolvență sunt reglementate de următorul cadru juridic:

- la nivel național: www.onrc.ro/index.php/ro/legislatie/legislatie-nationala
- la nivel european: www.onrc.ro/index.php/ro/legislatie/legislatie-europeana

Registrul litigiilor

În afara actelor normative menționate anterior, Codul de procedură civilă, Codul Civil, Codul de Procedura Penală, codul Penal, Codul Muncii.



1.4 Descrierea instituției

Viziunea și misiunea ONRC

Viziunea ONRC este de a contribui la dezvoltarea mediului de afaceri din România, prin oferirea de servicii publice de calitate, flexibile și orientate către nevoile specifice ale solicitanților.

Misiunea principală a Oficiului Național al Registrului Comerțului (ONRC) constă în prestarea serviciului public de ținere a registrului comerțului și de efectuare a publicității legale a actelor și faptelor întreprinzătorilor, precum și efectuarea procedurii de citare și publicitate a procedurilor de insolvență.

Valori ale ONRC

- a) **Orientarea către solicitanții de servicii publice** – ONRC este o instituție publică total dedicată solicitanților de servicii, adaptându-se la particularitățile activităților comerciale ale fiecăruia, astfel încât înregistrarea datelor întreprinzătorilor să fie făcută cu acuratețe;
- b) **Accesibilitatea serviciilor** – ONRC caută continuu noi mijloace pentru a face serviciile "să vină mai aproape de solicitant" și pentru a spori promptitudinea prestației sale;
- c) **Transparență** – transparența operațiunilor în raport cu mediile de business și guvernamentale este un deziderat constant al ONRC.

Factorii cheie ai dezvoltării ONRC

1. **Digitalizarea serviciilor destinate mediului de afaceri (G2B) pe baza identității electronice**, condiție a autentificării on-line a utilizatorilor externi;
2. **Creșterea accesibilității serviciilor**, prin dezvoltarea serviciilor destinate mediului de afaceri (G2B) online, ca alternativă la serviciile de ghișeu;
3. **Integrarea cu aplicații de e-Payment în arhitectura de sistem a ONRC** în vederea facilitării plăților on-line;
4. **Implementarea practicilor europene cu privire la serviciile publice;**



Proiect cofinanțat din Fondul Social European prin
Programul Operațional Capacitate Administrativă 2014-2020!



5. **Respectarea prevederilor legislative cu privire la înregistrarea întreprinzătorilor și editarea Buletinului Procedurilor de Insolvență;**
6. **Creșterea calității serviciilor**, în întâmpinarea nevoii crescânde a mediului de afaceri pentru servicii mai accesibile;
7. **Asigurarea securității** în condițiile creșterii continue a disponibilității datelor pentru asigurarea confidențialității și continuității serviciilor on-line;
8. **Asigurarea interoperabilității interinstituțională** (juridic, organizațional, semantic, tehnic);
9. **Instruirea prealabilă a resurselor umane** pentru a îmbunătăți interacțiunea operatorilor umani cu noile servicii;
10. **Creșterea eficienței interne a ONRC**, prin implementarea unei infrastructuri IT moderne care să suporte serviciile destinate mediului de afaceri (G2B) și serviciile destinate altor instituții guvernamentale (G2G) precum și prin implementarea/automatizarea unor procese IT necesare exploatării eficiente a acestei infrastructuri.

Strategia ONRC

1. În planul serviciilor destinate mediului de afaceri (G2B):

- Atragerea de noi solicitanți de servicii, prin prestații prompte, personalizate și promovarea unor tarife accesibile;
- **Accesibilitate în furnizarea serviciilor**, inclusiv prin asigurarea disponibilității on-line a acestora;
- Dezvoltarea de servicii "user centric" (servicii cu valoare adăugată);
- Protejarea datelor transmise de solicitanți.

2. În planul serviciilor cu alte instituții guvernamentale (G2G):

- Identificarea permanentă de noi oportunități de **colaborare cu instituții publice centrale și județene** pentru promovarea intereselor comune (furnizarea de servicii cu valoare adăugată, elaborarea de propuneri legislative și norme metodologice, etc.);



Proiect cofinanțat din Fondul Social European prin
Programul Operațional Capacitate Administrativă 2014-2020!



- Creșterea permanentă a numărului de protocoale de colaborare de schimb de date.

3. În plan intra-instituțional:

a. La nivel managerial:

- Creșterea posibilităților de **control și monitorizare internă**;
- **Evaluarea periodică a fluxurilor de lucru** și de transmitere a informațiilor precum și identificarea oportunităților pentru optimizarea acestora.

b. În plan tehnologic:

- Evaluarea și re tehnologizarea permanentă a infrastructurii IT&C de suport, în scopul **derulării eficiente atât a serviciilor publice, cât și a activităților interne**;
- Asigurarea securității datelor preluate/procesate/ transmise;
- **Creșterea interoperabilității interinstituționale** la nivel de back-office/ front-office.

c. În domeniul resurselor umane:

- Managementul eficient al posturilor;
- Fidelizarea angajaților, prin politici adecvate și atractive;
- Posibilități sporite de perfecționare profesională, prin asigurarea accesului la programe de instruire ;
- **Optimizarea comunicării intra-instituționale** pe orizontală (atât în cadrul ONRC, cât și ORCT), precum și pe verticală (ONRC-ORCT).

d. În plan economico-financiar:

- Gestiunea eficientă a resurselor materiale și financiare:
 - optimizarea proceselor de angajare, lichidare, ordonanțare și plată a cheltuielilor;

- planificarea anuală a bugetului și investițiilor pe baza analizelor de execuție și a prognozelor;
 - corelarea proceselor de achiziții publice cu nevoile reale;
 - gestionarea corespunzătoare a patrimoniului.
- Identificarea de noi pârgii pentru minimizarea costurilor

Atribuțiile ONRC sunt reglementate, în principal, de Legea nr. 26/1990 privind registrul comerțului, republicată, cu modificările și completările ulterioare, precum și de Regulamentul de organizare și funcționare a Oficiului Național al Registrului Comerțului și a oficiilor registrului comerțului, aprobat prin Ordinul ministrului Justiției nr. 1.082/C/2014, cu completările și modificările ulterioare.

Astfel, în conformitate cu prevederile cap. 1 din Regulamentul de organizare și funcționare a Oficiului Național al Registrului Comerțului și a oficiilor registrului comerțului de pe lângă tribunale, ONRC este organizat pe 2 niveluri:

- **nivel național**, reprezentat de Oficiul Național al Registrului Comerțului ce funcționează în subordinea Ministerului Justiției și
- **nivel local**, reprezentat de cele 42 de Oficii ale registrului comerțului funcționează pe lângă tribunale (ORCT) sunt organizate în fiecare reședință de județ, în subordinea ONRC fără personalitate juridică

ONRC are atribuțiile care îi revin potrivit dispozițiilor Legii nr. 26/1990 privind registrul comerțului, republicată, cu modificările și completările ulterioare, ale Legii nr. 31/1990 privind societățile, republicată, cu modificările și completările ulterioare, ale Legii nr. 359/2004 privind simplificarea formalităților la înregistrarea în registrul comerțului a persoanelor fizice, asociațiilor familiale și persoanelor juridice, înregistrarea fiscală a acestora, precum și la autorizarea funcționării persoanelor juridice, cu modificările și completările ulterioare, ale Ordonanței de urgență a Guvernului nr. 44/2008 aprobată, cu modificări și completări, prin Legea nr. 182/2016 privind desfășurarea activităților economice de către persoanele fizice autorizate, întreprinderile individuale și întreprinderile familiale, cu modificările și completările ulterioare, ale Legii nr. 85/2014 privind procedurile de prevenire a insolvenței și de insolvență, cu modificările și completările ulterioare, ale Legii nr. 151/2015 privind procedura insolvenței persoanelor fizice, ale Ordinului Ministrului Justiției nr. 2.594/C/2008 pentru aprobarea Normelor metodologice privind modul de ținere a registrelor comerțului, de efectuare a înregistrărilor și de eliberare a informațiilor, precum și cele stabilite prin alte acte normative cu incidență în domeniul său de activitate.

Principalele funcții ale Oficiului Național al Registrului Comerțului și ale oficiilor registrului comerțului de pe lângă tribunale, în conformitate cu dispozițiile Legii nr. 26/1990 privind registrul comerțului, republicată, cu modificările și completările ulterioare, și ale Regulamentului de organizare și funcționare a Oficiului Național al Registrului Comerțului și a oficiilor registrului comerțului de pe lângă tribunale, aprobat Ordin al M.J. nr. 1082/C/2014 cu modificările și completările ulterioare, sunt:

- **funcția de ținere a registrului comerțului;**
- **funcția de eliberare de înscrisuri și de informare;**
- **funcția de arhivare a înscrisurilor în baza cărora se efectuează înregistrările în registrul comerțului;**
- **funcția de asistență pentru persoanele fizice și juridice supuse înregistrării în registrul comerțului;**
- **funcția de editare și publicare a Buletinului procedurilor de insolvență.**

Cât privește **funcția de ținere a registrului comerțului** exercitată de oficiile registrului comerțului de pe lângă tribunale aceasta se poate detalia astfel:

- **înregistrarea tuturor persoanelor juridice supuse obligației de înregistrare, a sucursalelor înființate de acestea, precum și a persoanelor fizice autorizate, întreprinderilor individuale și întreprinderilor familiale care desfășoară activități economice, cu sediul social/sediul profesional pe raza teritorială a tribunalului;**

- **evidența datelor din documentele de înregistrare ale persoanelor supuse înregistrării, precum și arhiva oficială a documentelor cu caracter constitutiv sau modificator ale acestora, cea de publicitate legală;**

- **transmiterea datelor în vederea înregistrării fiscale a contribuabililor și obținerii codului unic de înregistrare de la Ministerul Finanțelor Publice, precum și a informațiilor din cazierul fiscal, în condițiile legii;**

- **eliberarea certificatului de înregistrare și a certificatului de înscriere de mențiuni, după caz, precum și a certificatelor constatatoare emise în baza declarațiilor-tip pe propria răspundere, conform Legii nr. 359/2004, cu modificările și completările ulterioare, și transmiterea acestor declarații către autoritățile publice competente;**

- **transmiterea cererilor de înregistrare a documentului care atestă dreptul de folosință asupra spațiului cu destinație de sediu social și de eliberare a certificatului pentru spațiul cu destinație de sediu social alături de actele doveditoare ale dreptului de folosință către**

administrațiile finanțelor publice, în vederea emiterii certificatelor pentru spațiul cu destinație de sediu social și a adeverințelor privind înregistrarea documentului care atestă dreptul de folosință asupra spațiului cu destinație de sediu social.

Cât privește **serviciile publice oferite** de ONRC, acestea pot fi grupate, în principal, astfel:

- **asistență acordată persoanelor interesate pentru înregistrarea în registrul comerțului;**
- **înregistrarea în registrul comerțului, furnizarea de informații din registrul comerțului și eliberarea de copii;**
- **publicare și furnizare BPI, furnizarea de informații din BPI, de certificate constatatoare, de rapoarte istorice și eliberarea de copii.**

2 Obiectivul achiziției

2.1 Obiectivul general

Obiectivul general al proiectului este îmbunătățirea capacității administrative a ONRC prin asigurarea suportului informatic pentru procesul de publicare legală a actelor operatorilor economici, prin asigurarea unui cadru colaborativ între angajați și prin întărirea securității și disponibilității sistemelor informatice ce susțin procesele de furnizare a serviciilor publice din responsabilitatea ONRC.

Beneficiile urmarite prin implementarea proiectului sunt următoarele:

- simplificarea și reducerea barierelor administrative și a birocratizării excesive, aferente proceselor și reglementărilor, din perspectiva cetățenilor și a angajaților mediului de afaceri;
- reducerea timpului de procesare a datelor în vederea furnizării serviciilor, cu o reducere corespunzătoare a costurilor;
- suport tehnologic sigur și scalabil;
- asigurarea securității datelor și controlul accesului la toate resursele sistemului;
- asigurarea disponibilității ridicate (24 x 7) a serviciilor;
- administrarea și operarea la costuri reduse a infrastructurii și componentelor soluției.

Pentru atingerea obiectivului general mai sus menționat ONRC își propune extinderea Sistemului Informatic Integrat (SII) cu următoarele subsisteme informatice:

1. Subsistemul informatic „Buletinului Electronic al Registrului Comerțului” (SSIBERC) ce va permite extinderea și consolidarea sistemului de publicitate legală a actelor. Acest subsistem va fi utilizat de cel puțin 500 de angajați ai ONRC iar serviciile online vor fi accesibile publicului larg, mediului

- de afaceri și autorităților publice prin intermediul portalului ONRC și a unei aplicații mobile dezvoltate pentru platformele cele mai populare (cel puțin Android și iOS);
2. Subsistemul informatic de tip "Colaborativ" (SSICO) ce va fi implementat în vederea sprijinirii angajaților ONRC în abordarea problemelor, pe activități, în vederea unificării activităților necesare efectuării de sarcini zilnice și periodice, gestionării proceselor interne și a răspunsurilor către mediul de afaceri și administrația publică;
 3. Sisteme informatice de monitorizare a performanțelor și asigurarea securității Sistemului Informatic Integrat al ONRC;

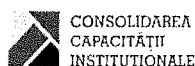
2.2 Scopul proiectului

Achiziția de produse hardware, software și servicii de dezvoltare software în vederea implementării sistemului informatic ce va asigura îmbunătățirea capacității de publicare a actelor operatorilor economici, de colaborare între angajați și de asigurare a securității și monitorizării sistemului informatic integrat al ONRC.

Astfel, prin implementarea proiectului „**Îmbunătățirea capacității de publicare a actelor operatorilor economici, de colaborare între angajați și de asigurare a securității și monitorizării sistemului informatic integrat ce susține procesele de furnizare a serviciilor publice aflate în responsabilitatea Oficiului Național al Registrului Comerțului**”, scopul ONRC este de:

- Reducere a timpului de efectuare a publicității legale;
- Desfasurare a activității în mod unitar la nivelul ONRC și a celor 42 de oficii teritoriale ale registrului comerțului de pe lângă tribunale;
- Îmbunătățire a capacităților instituției de a furniza consecvent servicii care să satisfacă cerințele solicitanților (persoane juridice, persoane fizice, instituții publice) coroborat cu reglementările în vigoare prin crearea unui cadru colaborativ bazat pe tehnologii de ultimă generație;
- Îmbunătățire continuă a calității și a disponibilității serviciilor furnizate;
- Creștere a credibilității și transparenței instituției;
- Creștere a eficienței și eficacității interne;
- Aliniere la standardele europene.
- Se urmărește deschiderea de noi orizonturi privind modalitățile de furnizare a serviciilor publice și optimizarea proceselor decizionale și a fluxurilor de lucru în cadrul ONRC, în concordanță cu principiile debirocratizării, maximizării transparenței și integrității, creșterii calității serviciilor furnizate.

Proiectul este finanțat prin Programul Operațional Capacitate Administrativă 2014-2020, Axa prioritară 2 - Administrație publică și sistem judiciar accesibile și transparente, cod 119317, cod SIPOCA 456.



Proiect cofinanțat din Fondul Social European prin
Programul Operațional Capacitate Administrativă 2014-2020!

2.3 Situația actuală (Sisteme existente)

Începând cu data de 06 februarie 2012, ONRC utilizează la nivel național, atât la sediul central, cât și la sediile celor 42 de birouri ale registrului comerțului de pe lângă tribunale (ORCT) organizate în subordinea ONRC, inclusiv sediile birourilor teritoriale care funcționează pe lângă ORCT, un nou sistem informatic integrat, pentru asigurarea de servicii on line destinate comunității de afaceri prin intermediul unui portal dedicat.

Sistemul informatic integrat ONRC este rezultatul proiectului "Servicii on-line (de e-Guvernare) oferite de ONRC pentru comunitatea de afaceri prin intermediul unui portal dedicat", derulat în perioada 2009 - 2012, scopul fiind acela de a crea beneficii atât pentru utilizatori (cetățeni și mediul de afaceri), cât și pentru administrația publică.

Beneficiarii direcți ai proiectului sunt reprezentați de următoarele categorii:

- Solicitanții de servicii publice:
 - persoane juridice - servicii destinate mediului de afaceri - "Government to Business" (G2B);
 - persoane fizice - servicii destinate persoanelor fizice - "Government to Citizen" (G2C)
 - instituții publice - servicii destinate instituțiilor guvernamentale - "Government to Government" (G2G)
- Instituțiile publice colaboratoare, cu care ONRC dezvoltă relații de tip G2G

Beneficiarii indirecti ai proiectului sunt următorii:

- Administrația publică, datorită eficientizării furnizării serviciilor publice și contribuției proiectului la reducerea birocrăției;
- Angajații companiilor, datorită eliminării timpului alocat deplasării la sediile ONRC precum și reducerii costurilor aferente utilizării serviciilor instituției.

Oferta de servicii a ONRC în raport cu segmentele mai sus menționate este după cum urmează:

Servicii destinate mediului de afaceri (G2B)

- Înregistrarea tuturor persoanelor juridice supuse obligației de înregistrare, a persoanelor fizice autorizate și asociațiilor familiale, care desfășoară activități economice
- Înscrierea de mențiuni pentru toate persoanele juridice, persoane fizice autorizate și asociații familiale, care au fost supuse înregistrării
- Eliberarea de certificate constatatoare, extrase de registru și alte înscrisuri pentru comercianți

- Editarea Buletinului Procedurilor de Insolvență în care se publică citațiile, convocările și notificările actelor de procedură efectuate de instanțele judecătorești, practicienii în insolvență și alte persoane interesate
- Furnizarea de statistici cu privire la comercianți
- Punerea la dispoziție de informații legale despre firme din registrul central al comerțului
- Asigurarea liberului acces la informații de interes public.

Servicii destinate instituțiilor guvernamentale (G2G)

- Colaborarea cu autoritățile și instituțiile publice responsabile pentru elaborarea, actualizarea și utilizarea unor nomenclatoare unitare pe plan național
- Colaborarea cu autoritățile și instituțiile publice implicate în constituirea și autorizarea funcționării comercianților, pentru simplificarea procedurilor specifice
- Obținerea și asigurarea evidenței acordurilor privind folosirea denumirii firmei
- Editarea Buletinului Procedurilor de Insolvență în care se publică citațiile, convocările și notificările actelor de procedură efectuate de instanțele judecătorești, practicienii în insolvență și alte persoane interesate
- Punerea la dispoziție de informații legale despre firme din registrul central al comerțului
- Furnizarea de statistici cu privire la comercianți
- Asigurarea liberului acces la informații de interes public.

Servicii destinate persoanelor fizice (G2C)

- Punerea la dispoziție de informații legale despre firme din registrul central al comerțului
- Furnizarea de statistici cu privire la comercianți
- Asigurarea liberului acces la informațiile de interes public.

Prin intermediul portalului de servicii online se asigură următoarele servicii:

Secțiunea G2B și G2C:

- **Servicii on-line specifice Registrul Comerțului**
 - Informarea inițială on-line a solicitanților despre categoriile de informații/ servicii furnizate de ONRC;
 - Asistența acordată solicitanților prin intermediul portalului;
 - Formulare accesibile on-line;
 - Atenționarea profesioniștilor privind situația firmei;
 - Furnizarea de informații on-line cu privire la stadiul dosarului;
 - Publicarea lunară a publicațiilor statistice de sinteză;

- Publicitatea pe internet a informațiilor / documentelor prevăzute de lege;
 - RECOM on-line - furnizarea de informații la zi din bazele de date privind profesioniștii înregistrați la Registrul Comerțului – cu un grad de complexitate ridicat prin introducerea plății on-line;
 - Verificarea și rezervarea on-line a disponibilității firmei;
 - Verificarea și rezervarea disponibilității emblemei;
 - Verificarea unicității sediului social și asociatului;
 - Completarea on-line și offline și transmiterea electronică a tuturor cererilor / formularelor (înmatriculări, mențiuni, cereri de informații și documente etc.) utilizate în activitatea registrului comerțului, inclusiv a documentelor doveditoare, necesare pentru susținerea cererilor, documente și informații ce vor fi încărcate în baze de date specifice, utilizând tehnologii hardware și software moderne și performante – cu un grad de complexitate ridicat prin introducerea plății on-line;
 - Furnizarea de statistici on-line personalizate, pe baza datelor înregistrate în registrul comerțului central computerizat - RCCC (informații la zi și din istoric);
 - Furnizarea de informații privind istoricul firmei, deșus prin portal „furnizare informatii la zi, privind istoricul firmei, statistici”, inclusiv plăți on-line;
 - Eliberarea de copii semnate electronic cu certificat digital calificat din arhiva electronică de documente constituită din dosarele comercianților – cu plata on-line;
 - Plăți on-line;
 - Atenționarea profesioniștilor, prin mijloace electronice, asupra unor acte normative cu incidență în relația cu registrul comerțului;
 - Actualizarea datelor de contact firmă (telefon, fax, e-mail, web-site).
- **Servicii on-line specifice Buletinului Procedurilor de Insolvență (BPI)**
- Transmiterea electronică automată din sistemul judiciar și din alte sisteme (ex. practicieni în insolvență) în baza BPI, în format electronic, cu semnătură electronică, a actelor de procedură gestionate în cadrul publicării BPI și informațiilor din baze de date;
 - Completarea și transmiterea on-line, cu semnătură electronică, a formularelor, a actelor de procedură și a informațiilor pentru publicare în BPI, inclusiv plata on-line;
 - Asistență BPI acordată solicitanților la completarea și transmiterea on-line a actelor de procedură și formularelor BPI;
 - Transmiterea electronică automată din bazele BPI în sistemul judiciar și în alte sisteme (ex. practicieni în insolvență), în format electronic, cu semnătură electronică, a dovezilor de publicare și informațiilor aferente;

- Acces on-line la informațiile BPI gratuite prin extinderea categoriilor și criteriilor de selectare disponibile utilizatorilor;
- Înștiințarea profesioniștilor, prin mijloace electronice, asupra unor acte normative cu incidență în relația cu BPI (newsletter pe adresa de e-mail, mesaj pe cont personal);
- Furnizare on-line a publicației BPI prin extinderea criteriilor de selectare disponibile utilizatorilor, inclusiv plata on-line;
- Completarea și transmiterea on-line, cu semnătură electronică, a comenzilor pentru abonament BPI și a cererilor de furnizare informații, inclusiv plata on-line;
- Furnizarea on-line de informații din bazele de date ale BPI;
- Publicarea lunară a situațiilor statistice de sinteză din BPI.

Secțiunea G2G

- **Servicii specifice Registrul Comerțului**
 - Gestiunea denumirii de firma pentru care este nevoie de acordul Secretariatul General al Guvernului;
 - Transmiterea electronică a actelor spre publicare în Monitorul Oficial;
 - Transmiterea electronică a datelor și declarațiilor tip pe proprie răspundere către ministerele avizatoare;
 - Transmiterea electronică automată de date către Institutul Național de Statistică, Garda Financiară etc. (16 instituții)
 - Transmiterea electronică de informații către Ministerul Finanțelor Publice - DGTI (date și documente) necesare înregistrării în registrul comerțului (CUI și informații din cazierul fiscal);
 - Transmiterea electronică de informații și înștiințări către Administrațiile Financiare.
- **Servicii specifice BPI**
 - Transmiterea electronică automată din sistemul judiciar și din alte sisteme (ex. practicieni în insolvență) în baza BPI, în format electronic, cu semnătură electronică, a actelor de procedură gestionate în cadrul publicării BPI și informațiilor baze de date;
 - Completarea și transmiterea on-line, cu semnătură electronică, a formularelor, a actelor de procedură și a informațiilor pentru publicare în BPI, inclusiv plata on-line;
 - Asistență BPI acordată solicitanților la completarea și transmiterea on-line a actelor de procedură și formularelor BPI;
 - Transmiterea electronică automată din bazele BPI în sistemul judiciar și în alte sisteme

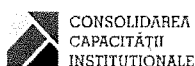
(ex. practicieni în insolvență), în format electronic, cu semnătură electronică, a dovezilor de publicare și informațiilor aferente;

- Acces on-line la informațiile BPI gratuite prin extinderea categoriilor și criteriilor de selectare disponibile utilizatorilor;
- Furnizarea on-line a publicației BPI prin extinderea criteriilor de selectare disponibile utilizatorilor, inclusiv plata on-line;
- Completarea și transmiterea on-line, cu semnătură electronică, a comenzilor pentru abonament BPI și a cererilor de furnizare informații, inclusiv plata on-line;
- Furnizarea on-line de informații din bazele de date ale BPI;
- Publicarea lunară a situațiilor statistice de sinteză din BPI.

Obiectivele specifice ale proiectului de implementare au fost:

- Facilitarea accesului utilizatorilor (cetățeni, mediul de afaceri și administrația publică) și creșterea celerității în furnizarea serviciilor prin punerea la dispoziția acestora a serviciilor publice prin mijloace electronice, on-line, oferind un număr de 34 servicii publice on-line prin intermediul unui portal dedicat, dintre care 24 servicii publice on-line nou create în cadrul proiectului implementat;
- Creșterea numărului de utilizatori ai serviciilor publice on-line oferite de ONRC, estimându-se un ritm anual de creștere de 5% a numărului de utilizatori în perioada ulterioară implementării proiectului, atingându-se un procent de 25% în al cincilea an;
- Eficientizarea fluxului de informații în relațiile cu instituțiile avizatoare și cele guvernamentale cu care ONRC are încheiate protocoale de colaborare - 16 instituții publice vor beneficia de reducerea timpului necesar obținerii informațiilor din registrul central al comerțului conform acordurilor inter-instituționale încheiate;
- Creșterea gradului de instruire a personalului ONRC în vederea utilizării noii infrastructuri TIC implementate, prin instruirea unui număr de 100 persoane, atât la nivel central cât și local;
- Implementarea unui serviciu de plăți on-line (e-payment) pentru gestionarea completă a serviciilor electronice comerciale oferite de ONRC, asigurându-se cel mai înalt nivel de complexitate al noului sistem informatic.;
- Implementarea unei infrastructuri IT&C moderne, care să deservească în mod optim derularea activităților specifice ONRC (ex.: creșterea performanțelor și securității sistemului, monitorizarea sistemului informatic, etc.), vizându-se dotarea cu infrastructura IT&C moderna a celor 43 de locații în care ONRC oferă servicii publice.

Activitatea instituției este aproape complet informatizată și este susținută 24x7 prin intermediul sistemului



Proiect cofinanțat din Fondul Social European prin
Programul Operațional Capacitate Administrativă 2014-2020!



informatic integrat (SII) al ONRC, instituția fiind dotată cu echipamentele, produsele software și serviciile informatice aferente necesare desfășurării activității.

Sistemul informatic al ONRC are, în principal, următoarele caracteristici:

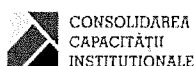
- este suportul de baza al întregii activități desfășurate la nivel local și central al ONRC;
- este unitar – folosește aceeași metodologie, aceleași proceduri de lucru, nomenclatoare, structuri de date și programe la toate oficiile registrului comerțului teritoriale;
- furnizează direct, din datele înregistrate în registrul computerizat, actele eliberate solicitanților privind soluționarea cererilor;
- asigură accesul partajat și controlat la baza de date atât pentru introducerea datelor cât și pentru furnizarea rapoartelor;
- este dotat cu sisteme de protecție fiind permis accesul numai persoanelor autorizate din cadrul sistemului registrului.

Sistemul informatic integrat (SII) al ONRC este un sistem cu o viziune și abordare integrată, distribuit teritorial și ierarhizat pe 2 nivele:

- **nivel central** care asigură în timp real:
 - centralizarea datelor înregistrate;
 - publicarea informațiilor conform prevederilor legale;
 - depunerea/eliberarea documentelor on-line prin intermediul portalului de servicii online;
 - interconectarea cu alte sisteme informatice la nivel național/local (G2G);
 - administrarea la nivel teritorial;
- **nivel teritorial** care gestionează întregul proces de înregistrare a profesioniștilor – inclusiv comunicația cu alte instituții pe plan local, în vederea efectuării înregistrărilor, eliberarea de certificate constatatoare și furnizarea de informații.

Sistemul informatic integrat al ONRC conține următoarele componente:

- **Componenta Registrul Comerțului**, distribuită teritorial și ierarhizată pe 2 nivele:
 - **nivelul central**, care asigură centralizarea, corelarea și administrarea informațiilor de la nivel teritorial, în timp real;
 - **nivelul teritorial**, care gestionează întregul proces de înregistrare a comercianților – inclusiv comunicația cu alte instituții pe plan local, în vederea efectuării înregistrărilor, eliberarea de certificate constatatoare și furnizarea de informații.



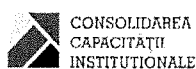
Proiect cofinanțat din Fondul Social European prin
Programul Operațional Capacitate Administrativă 2014-2020!

- **Baza de date** a registrului comerțului, la nivel local și la nivel central, se structurează în 2 componente:
 - baza de date cu informațiile la zi ale persoanelor fizice și juridice înregistrate în registrul comerțului, supusă frecvent interogărilor și prelucrărilor statistice;
 - baza de date de arhivă conținând istoricul firmei cu datele inițiale de la înmatriculare și toate mențiunile ulterioare, supusă interogărilor și prelucrărilor statistice.
- **Componenta Registrul Litigiilor**, care este un sistem centralizat, utilizat la nivel național de ONRC și ORCT-uri.
- **Componenta Buletinul Procedurilor de Insolvență**, care este un sistem centralizat, utilizat la nivel național de ONRC și ORCT-uri.

Pe lângă componentele descrise, la nivel central există și următoarele sub-sisteme:

- a. **Sistemul de arhivare electronică (SAE) a documentelor**, cuprinzând imaginea în format electronic (.PDF) a cererilor de înregistrare și a documentelor care au stat la baza înregistrărilor care sunt scanate și indexate la nivel local și apoi transmise la nivel central; acest sistem este supus interogărilor utilizatorilor din ORCT
- b. **Bazele de date financiar contabile și pentru managementul resurselor umane** sunt formate din două componente:
 - componenta "resurse umane și calcul salarii" se constituie numai la nivel central și este formată din înregistrări în tabele FOXPRO care sunt supuse prelucrărilor și interogărilor, generându-se documente, declarații către autorități și către ordonatorul principal de credite, precum și diverse statistici în format DOC și XLS. Componenta "resurse umane" are o subcomponentă ce include foaia colectivă de prezență care se generează local și se transmite la sediul central;
 - componenta "financiar contabilă" se constituie din subcomponente la nivel local unde se realizează înregistrarea încasărilor și facturarea clienților în baza notelor de calcul, evidența materialelor, obiectelor de inventar și mijloacelor fixe, înregistrarea diverselor documente și a plăților între subunități, și se generează balanța de verificare. Baza de date este transmisă la sediul central unde se verifică datele înregistrate, se centralizează balanțele de verificare și se generează documente, declarații către autorități și către ordonatorul principal de credite, se fac plăți pentru furnizori, precum și pregătirea de statistici în format DOC și XLS.

Sistemul este dezvoltat pe tehnologii Oracle și Java. Aplicațiile care fac parte din Sistemul Informatic Integrat al ONRC (SII) sunt următoarele:



Proiect cofinanțat din Fondul Social European prin
Programul Operațional Capacitate Administrativă 2014-2020!



www.poca.ro

- Registratura Locație (REG)
- Registrul Litigiilor (RL)
- Registrul Comerțului (RC)
- Buletinul Procedurilor de Insolvență (BPI)
- Portalul Serviciilor Online al instituției ONRC (include servicii online RC și BPI)
- Nomenclatoare (centrale – RC+RL, BPI și locale)
- Antecalcul (TAX)
- Publicare date pentru alte instituții (prin intermediul portalului)
- Sistem de securitate internă (central și local) și externă (Aplicația Centralizată de Management Utilizatori - ACMU)
- Raportare Analitică

Aria de acoperire geografică și funcțională a sistemului informatic al ONRC

Locatiile, sistemele și aplicațiile care fac parte din Sistemul Informatic Integrat sunt următoarele:

- Locatii:
 - Sediul central al ONRC Bucuresti
 - Sediile ORCT din tara si din Bucuresti (42 locatii)
 - Birourile teritoriale ale ORCT
- Aplicatii SII:
 - Registratura Locatie (RG)
 - Registrul Litigiilor (RL)
 - Registrul Comerțului (RC)
 - Buletinul Procedurilor de Insolventa (BPI)
 - Portalul Serviciilor Online al institutiei ONRC
 - Nomenclatoare (RC+RL, BPI)
 - Antecalcul
 - Publicare date catre alte institutii
 - Sistem de securitate internă (central și local) și externă (Aplicația Centralizată de Management Utilizatori - ACMU)
 - Raportare Analitica
- Alte aplicatii istorice (implementate anterior proiectului e-Guvernare):
 - Casierie – aplicatie ce ruleaza la nivel central și local (FOXPro)
 - CAPTIVA – aplicatie de arhivare ce ruleaza la nivel local și central (EMC Captiva)



[Handwritten signatures]

- SAE (Sistemul de Arhivare Electronica) – aplicatie ce ruleaza la nivel central (WebSphere AS, DB2 Content Manager, Java, UDB DB2)
- Clienti/ facturi – aplicatie din suita ERP ce ruleaza la nivel central si local (FOXPro) si care administreaza din punct de vedere contabil clientii ONRC generand facturi si monitorizand stadiul acestor facturi.
- Aplicatii externe:
 - Obținere CUI – MFP
 - Obținere cazier fiscal – MFP
 - Monitorul Oficial
 - ECRIS - MJ
 - SEN - „Platformă pentru integrarea serviciilor de e-guvernare în Sistemul Electronic Național” din cadrul Ministerului Comunicațiilor și Societății Informaționale reprezentate de PCU și OneStopShop
 - Autoritati certificate digitale calificare

Infrastructura hardware

În fiecare ORCT funcționează rețele locale proprii, cablare structurată voce-date, în general.

Principalele echipamente din dotarea fiecărui ORCT:

LAN

- două servere de baze de date cu sisteme de operare Linux (RedHat, Fedora etc.), Samba, NFS, etc.;
- un server de comunicații (Internet) cu sistem de operare Linux (RedHat, Fedora etc.) pe care sunt instalate: server de mail, proxy, server HTTP etc.;
- un server/o stație de lucru dedicat/dedicată cu sistem de operare Windows Server/Windows XP pentru sistemul de arhivare electronică a documentelor;
- stații de lucru cu sistem de operare Windows XP Professional și Windows Vista Ultimate, Windows 7, Windows 8.x, Windows 10 Professional;
- echipamente de rețea (dulapuri de conexiuni, switch-uri);
- echipamente de comunicație (routere CISCO);
- alte echipamente: imprimante, scanere, inscripționatoare DVD, switch-uri KVM, copiatoare etc.

DMZ

- Infrastructura SII

La sediul ORCT este implementată o arhitectură bazată pe un firewall (un cluster cu 2 noduri), care împarte rețeaua în trei zone:

- zona demilitarizată (DMZ) – în care sunt amplasate echipamentele SII;
- rețeaua internă care cuprinde serverele interne (file servere și baze de date), stații de lucru, imprimante, scanere, echipamente active de rețea (switch-uri) – care nu sunt accesibile din exterior sau din ORCT, ci numai din rețeaua internă, având adrese IP din clase private;
- zona rețelei virtuale private (VPN) a sistemului registrului comerțului.

La sediul central al ONRC există o rețea locală proprie, cablare structurată voce-date, cat. 6.

Principalele echipamente din dotarea ONRC sunt următoarele:

LAN si DMZ

- servere de rețea locală și baze de date cu sisteme de operare Linux (RedHat) și SGBD FoxPro și Oracle;
- servere care asigură servicii Internet și Intranet (servere de mail, DNS, web etc.) cu sisteme de operare Linux (Red Hat);
- servere dedicate pentru aplicații/soluții;
- servere de baze de date;
- servere pentru sistemul de arhivare electronică a documentelor;
- servere pentru Buletinul Procedurilor de Insolvență;
- echipamente de rețea: dulapuri de conexiuni, switch-uri;
- echipamente de comunicație (routere CISCO);
- stații de lucru cu sistem de operare Windows XP Professional și Windows Vista Ultimate, Windows 7, Windows 8.x, Windows 10 Professional;
- alte echipamente: imprimante, scanere, inscripționatoare DVD, switch-uri KVM, copiatoare etc.

DMZ-uri SII

- Infrastructura SII.

La sediul central este implementată o arhitectură bazată pe un firewall (un cluster cu 2 noduri), care împarte rețeaua ONRC în mai multe zone:

- zona demilitarizată (DMZ) – în care sunt amplasate echipamentele (în principal servere) care trebuie să fie accesibile din exterior și din ORCT (din Internet și Intranet);

- DMZ-uri infrastructura SII;
- rețeaua internă care cuprinde serverele interne (file servere și baze de date), stații de lucru, imprimante, scanere, echipamente active de rețea (switch-uri) – care nu sunt accesibile din exterior sau din ORCT, ci numai din rețeaua internă, având adrese IP din clase private;
- zona rețelei virtuale private (VPN) a sistemului registrului comerțului;
- zona rețelei virtuale private (Extranet VPN) cu instituțiile publice;

Infrastructura de comunicații

În sistemul registrului comerțului sunt instalate două tipuri de comunicații:

- în cadrul sistemului registrului comerțului: între ONRC și ORCT precum și cele între birourile teritoriale și biroul ORCT de care aparțin și ONRC;
- comunicații Internet – cu alte instituții și clienți.

Comunicațiile în cadrul sistemului registrului comerțului sunt necesare, în principal, pentru:

- transmisia permanentă de informații și documente de la ORCT către ONRC, inclusiv a informațiilor necesare obținerii codului unic de înregistrare (CUI) și a cazierului fiscal de la Ministerul Finanțelor Publice (MFP);
- difuzarea de documente, adrese, aplicații, manuale etc., în special prin tehnologia web (intranet);
- acces la sistemul informatic integrat (SII);
- acces la sistemul de arhivare electronică a documentelor (SAE);
- intervenții tehnice și configurări realizate de la distanță de către Serviciul AIC, DTI din cadrul ONRC, pe echipamentele din cadrul ORCT;

Comunicațiile Internet sunt necesare, în principal, pentru:

- acces la site-ul www.onrc.ro, la serviciile SII oferite prin portal.onrc.ro, la site-ul Buletinului procedurilor de insolvență www.buletinulinsolventei.ro, www.bpi.ro;
- schimb de informații și documente cu alte instituții;
- comunicarea cu furnizorii și prestatorii de servicii;
- realizarea update-urilor la sisteme de operare, produse software, drivere, semnături la produsele antivirus, produse legislative, etc;
- acces la informații necesare în activitatea instituției;
- comunicarea cu clienții serviciilor ONRC;

Comunicațiile în cadrul sistemului registrului comerțului sunt realizate prin rețeaua virtuală privată (VPN) a registrului comerțului implementată, în baza H.G. nr. 1213/2005, prin Serviciul de Telecomunicații

Speciale. Toate comunicațiile sunt criptate (prin protocolul IPSec) utilizând modulul de criptare din router-
ele CISCO instalate în toate locațiile.

Pentru BPI și înregistrarea hotărârilor judecătorești în registrul comerțului, altele decât cele în materia
insolvenței, trebuie activată rețeaua de comunicații VPN – ONRC/ORCT – instanțe judecătorești,
Ministerul Justiției, alte structuri din sistemul judiciar, prin STS.

Fiecare locație are 2 conexiuni VPN :

- o conexiune principală, în majoritatea locațiilor pe fibră optică;
- o conexiune de backup pe diferite medii de comunicație.

La aceasta rețea virtuală privată sunt conectate și birourile teritoriale ale ORCT.

Comunicațiile Internet

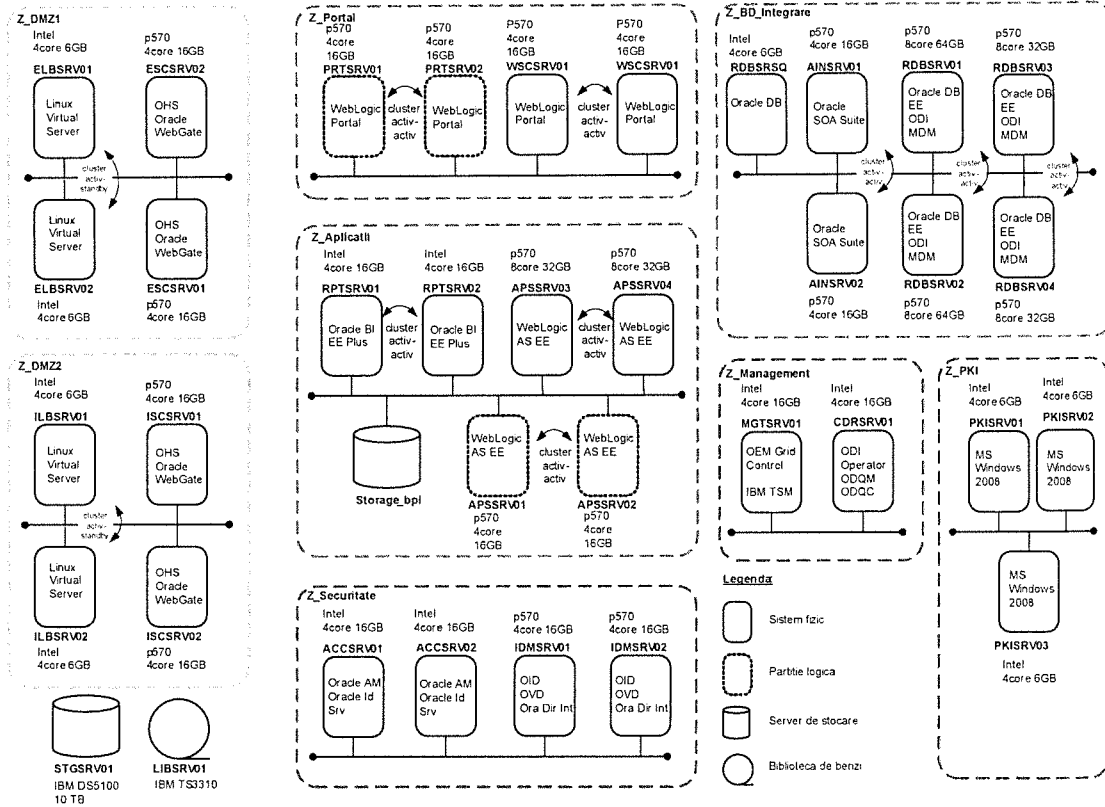
Sunt asigurate de diferiți furnizori de servicii Internet, selectați prin licitații publice:

- ONRC are două conexiuni permanente pe fibră optică (principală și de backup);
- ORCT București are o conexiune permanentă;
- celelalte ORCT au conexiuni permanente pe medii fizice diferite (fibră optică, linie
telefonică închiriată) cu rate de transfer optime activității.

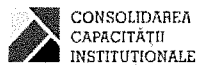
Birourile teritoriale nu au conexiuni Internet proprii, utilizând comunicațiile Internet de la sediul ORCT de
care aparțin.

Diagrama următoare prezintă sistemele plasate în locația ONRC, mediul de producție:

Arhitectura hardware – ONRC (Mediu de productie)



Figură 1 Arhitectura hardware ONRC (mediu de productie)

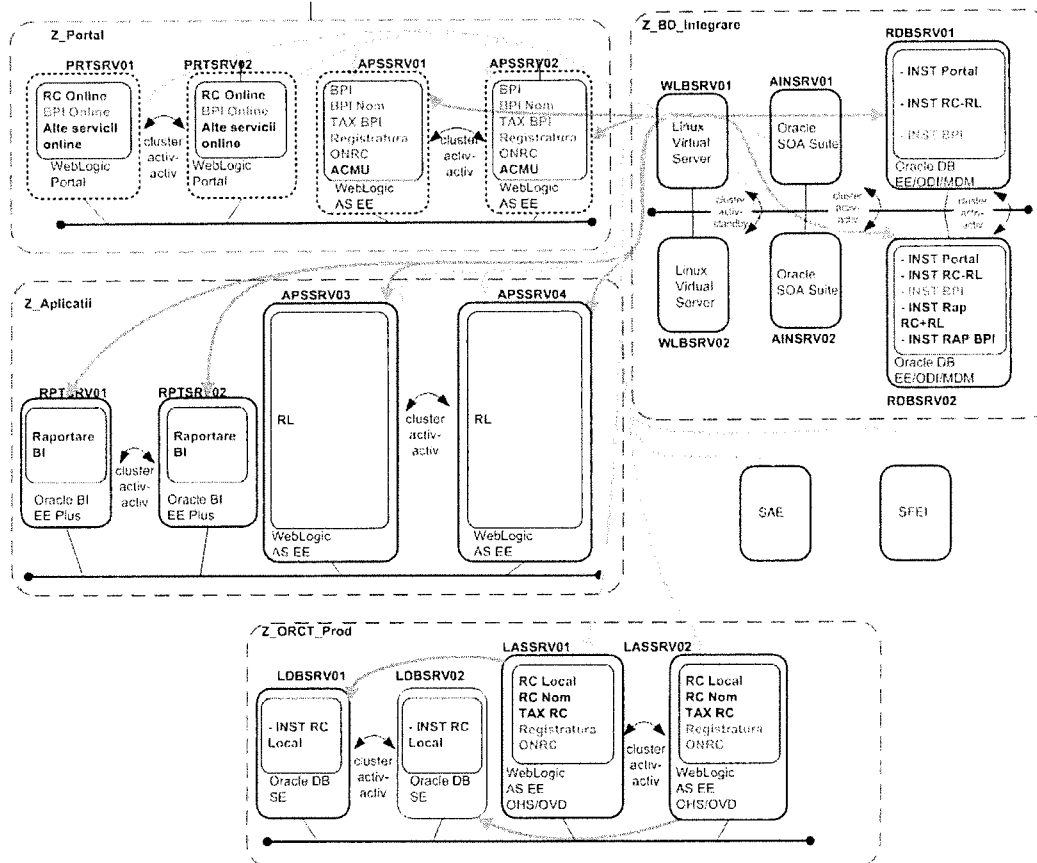


Proiect cofinanțat din Fondul Social European prin
Programul Operațional Capacitate Administrativă 2014-2020!



Handwritten signatures and marks at the bottom of the page.

ONRC – Distribuția aplicațiilor și a bazelor de date pe mașini

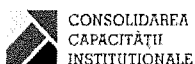


Figură 2 Distribuția aplicațiilor și bazelor de date pe servere

Zona	Denumire,	Rol	Platforma hardware	Sistem de operare	Software
Z_DMZ1	ELBSRV01	Load Balancer acces din internet și extranet și utilizatori și sisteme. Nod activ.	Intel 4core 6GB	Linux	Linux Server Virtual
Z_DMZ1	ELBSRV02	Load Balancer acces din internet și extranet și utilizatori și sisteme. Nod stand-by.	Intel 4core 6GB	Linux	Linux Server Virtual



Zona	Denumire,	Rol	Platforma hardware	Sistem de operare	Software
Z_DMZ1	ESCSRV01	HTTP Server si verificare acces pentru utilizatori din Internet	p570 4core 16GB	AIX	Oracle HTTP Server Oracle WebGate
Z_DMZ1	ESCSRV02	HTTP Server si verificare acces pentru utilizatori	p570 4core 16GB	AIX	Oracle HTTP Server Oracle WebGate
Z_DMZ2	ILBSRV01	Load Balancer acces utilizatori din Intranet. Nod activ.	Intel 4core 6GB	Linux	Linux Virtual Server
Z_DMZ2	ILBSRV02	Load Balancer acces utilizatori din Intranet. Nod stand-by.	Intel 4core 6GB	Linux	Linux Virtual Server
Z_DMZ2	ISCSRV01	HTTP Server si verificare acces pentru utilizatori din Intranet.	p570 4core 16GB	AIX	Oracle HTTP Server Oracle WebGate
Z_DMZ2	ISCSRV02	HTTP Server si verificare acces pentru utilizatori din Intranet.	p570 4core 16GB	AIX	Oracle HTTP Server Oracle WebGate
Z_PORTAL	PRTSRV01	Server aplicatie portal pentru utilizatori Internet.	partitie logica p570 4core 16GB	AIX	Oracle WebLogic Portal
Z_PORTAL	PRTSRV02	Server aplicatie portal pentru utilizatori Internet.	partitie logica p570 4core 16GB	AIX	Oracle WebLogic Portal
Z_PORTAL	WCSRV01	Server de test aplicatii interne pentru servicii portal.	p570 4core 16GB	AIX	Oracle WebLogic Server Enterprise Edition
Z_PORTAL	WCSRV02	Server de test aplicatii interne pentru servicii portal.	p570 4core 16GB	AIX	Oracle WebLogic Server Enterprise Edition

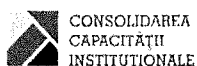

 CONSOLIDAREA
 CAPACITĂȚII
 INSTITUȚIONALE

Proiect cofinanțat din Fondul Social European prin
 Programul Operațional Capacitate Administrativă 2014-2020!





Zona	Denumire,	Rol	Platforma hardware	Sistem de operare	Software
Z_Aplicatii	RPTSRV01	Server de raportare pentru aplicatiile interne	Intel 4core 16GB	Linux	Oracle Business Intelligence Enterprise Edition Plus
Z_Aplicatii	RPTSRV02	Server de raportare pentru aplicatiile interne	Intel 4core 16GB	Linux	Oracle Business Intelligence Enterprise Edition Plus
Z_Aplicatii	APSSRV01	Server aplicatii interne pentru servicii portal BPI si Taxe.	partitie logica p570 4core 16GB	AIX	Oracle WebLogic Server Enterprise Edition
Z_Aplicatii	APSSRV02	Server aplicatii interne pentru servicii portal BPI si Taxe.	partitie logica p570 4core 16GB	AIX	Oracle WebLogic Server Enterprise Edition
Z_Aplicatii	APSSRV03	Server aplicatii interne pentru utilizatorii interni. Aplicatiile centrale de Registratura, RC si RL.	p570 8core 32GB	AIX	Oracle WebLogic Server Enterprise Edition
Z_Aplicatii	APSSRV04	Server aplicatii interne pentru utilizatorii interni. Aplicatiile centrale de Registratura, RC si RL.	p570 8core 32GB	AIX	Oracle WebLogic Server Enterprise Edition
Z_Aplicatii	storage	Server de stocare de 4.5TB.	N/A	Linux	N/A
Z_DB_Integrare	RDBSRV03	Server de baze de date ce va prelua parte din datele din productie.	Intel 4core 6GB	Linux	Oracle Database Enterprise Edition Oracle Real Application Clusters

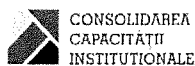


Proiect cofinanțat din Fondul Social European prin
 Programul Operațional Capacitate Administrativă 2014-2020!





Zona	Denumire,	Rol	Platforma hardware	Sistem de operare	Software
Z_DB_Integrare	RDBSRV04	Server de baze de date ce va prelua parte din datele din productie.	Intel 4core 6GB	Linux	Oracle Database Enterprise Edition Oracle Real Application Clusters
Z_DB_Integrare	AINSRV01	Server servicii web si procese.	p570 4core 16GB	AIX	Oracle Service Bus Oracle BPEL Process Manager Oracle Business Activity Monitoring
Z_DB_Integrare	AINSRV02	Server servicii web si procese.	p570 4core 16GB	AIX	Oracle Service Bus Oracle BPEL Process Manager Oracle Business Activity Monitoring
Z_DB_Integrare	RDBSRV01	Server baza de date centrala si integrare la nivel de date. Instanta SIIHQ1 VIRT.IP:	p570 8core 64GB	AIX	Oracle Database Enterprise Edition Oracle Real Application Clusters Oracle Partitioning Oracle Advanced Security Oracle Data Integration Suite Oracle Master Data Management
Z_DB_Integrare	RDBSRV02	Server baza de date centrala si integrare la nivel de date. Instanta SIIHQ2. VIRT.IP:	p570 8core 64GB	AIX	Oracle Database Enterprise Edition Oracle Real Application Clusters Oracle Partitioning Oracle Advanced Security Oracle Data Integration Suite Oracle Master Data Management


 CONSOLIDAREA
 CAPACITĂȚII
 INSTITUȚIONALE

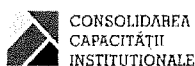
Proiect cofinanțat din Fondul Social European prin
 Programul Operațional Capacitate Administrativă 2014-2020!



Handwritten signatures and marks at the bottom of the page.



Zona	Denumire,	Rol	Platforma hardware	Sistem de operare	Software
Z_DB_Integrare	RDBSRVQ	Server de baze de date utilizat pentru Ad-Hoc queries pe baza de date centrala.	Intel 4core 6GB	AIX	Oracle Database Enterprise Edition
Z_Securitate	ACCSRV01	Server politici de acces la resurse. Server primar.	Intel 4core 16GB	Linux	Oracle Access Manager Access Server Oracle Identity Server
Z_Securitate	ACCSRV02	Server politici de acces la resurse. Server secundar.	Intel 4core 16GB	Linux	Oracle Access Manager Access Server Oracle Identity Server
Z_Securitate	IDMSRV01	Server director si management identitati. Server primar.	p570 4core 16GB	AIX	Oracle Virtual Directory Oracle Internet Directory Oracle Directory Integration Platform
Z_Securitate	IDMSRV02	Server director si management identitati. Server secundar.	p570 4core 16GB	AIX	Oracle Virtual Directory Oracle Internet Directory Oracle Directory Integration Platform
Z_Management	MGTSRV01	Server management sisteme	Intel 4core 16GB	Linux	Oracle Enterprise Manager Grid Control IBM Tivoli Storage Manager
Z_Management	CDRSRV01	Server pentru controlul datelor replicate	Intel 4core 16GB	Linux	Oracle Data Integrator Operator



Handwritten signatures and initials: JH, AGS, Des, dk, and another signature.



Zona	Denumire,	Rol	Platforma hardware	Sistem de operare	Software
Z_PKI	PKISRV01	Server solutie PKI	Intel 4core 6GB	Windows 2008 Enterprise Edition	Window 2008 Server Enterprise Certification Authority cu rolurile de Agent de inrolare Certification Authority cu functia de Agent de Recuperare a Cheilor (Key Recovery Agent). (Enrollment Agent)
Z_PKI	PKISRV02	Server solutie PKI	Intel 4core 6GB	Windows 2008 Enterprise Edition	Windows 2008 Server Enterprise Certification Authority cu functia de Agent de Recuperare a Cheilor (Key Recovery Agent).
Z_PKI	PKISRV03	Server solutie PKI	Intel 4core 6GB	Windows 2008 Enterprise Edition	Window 2008 Server Enterprise Certification Authority cu functia de OCSP Server
-	STGSRV01	Server stocare externa	IBM DS5100 10 TB	N/A	N/A
-	LIBSRV01	Biblioteca de benzi	IBM TS3310	N/A	N/A

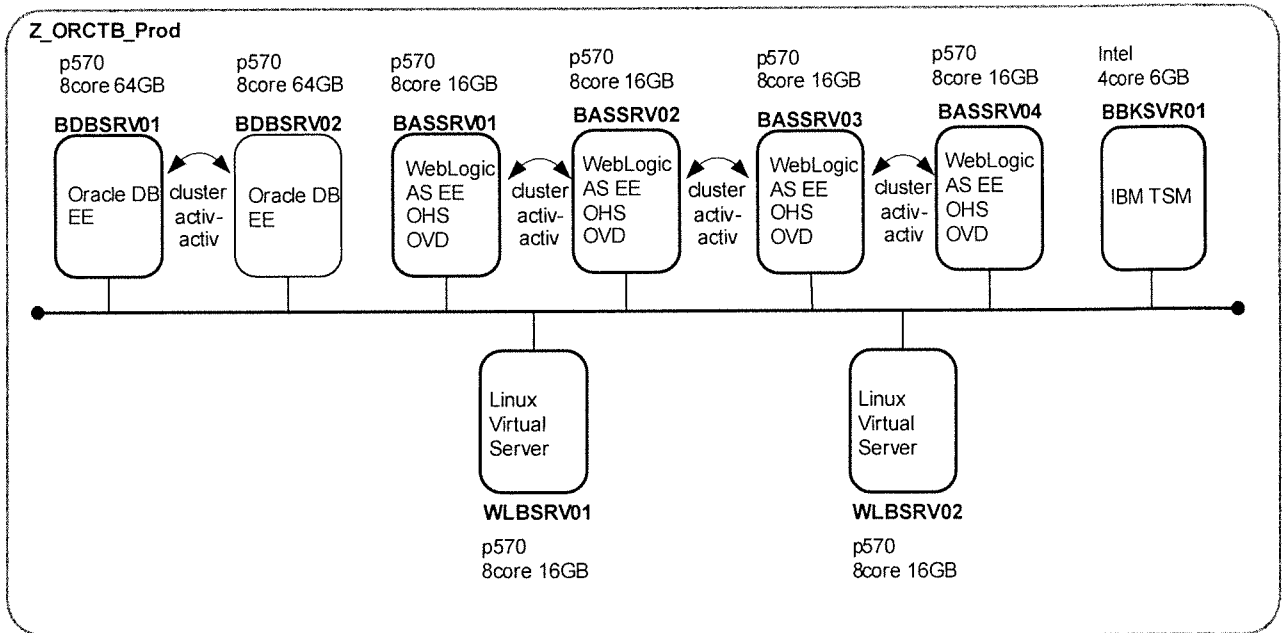
Diagrama urmatoare prezinta sistemele plasate in Bucuresti, mediul de productie:



Proiect cofinanțat din Fondul Social European prin
Programul Operațional Capacitate Administrativă 2014-2020!



Arhitectura fizica – Locatia ORCT Bucuresti

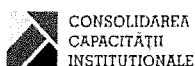


Figură 3 Arhitectura fizica ORCT Bucuresti



[Handwritten signatures]

Zona	Denumire, IP	Rol	Platforma hardware	Sistem de operare	Software
Z_ORCTB_P rod	BDBSRV01	Server baza de date si integrare la nivel de date. In cluster cu BDBSRV02.	p570 8core 64GB	AIX	Oracle Database Enterprise Edition Oracle Real Application Clusters Oracle Partitioning Oracle Advanced Security
Z_ORCTB_P rod	BDBSRV02	Server baza de date si integrare la nivel de date. In cluster cu BDBSRV02.	p570 8core 64GB	AIX	Oracle Database Enterprise Edition Oracle Real Application Clusters Oracle Partitioning Oracle Advanced Security
Z_ORCTB_P rod	BASSRV01	Server de aplicatie pentru aplicatiile locale (RC, RL, Antecalcul, REG). In cluster cu serverele BASSRV02, BASSRV03, BASSRV04.	p570 8core 16GB	AIX	Oracle WebLogic Server Enterprise Edition Oracle HTTP Server Oracle Virtual Directory
Z_ORCTB_P rod	BASSRV02	Server de aplicatie pentru aplicatiile locale (RC, RL, Antecalcul, REG). In cluster cu serverele BASSRV01, BASSRV03, BASSRV04.	p570 8core 16GB	AIX	Oracle WebLogic Server Enterprise Edition Oracle HTTP Server Oracle Virtual Directory
Z_ORCTB_P rod	BASSRV03	Server de aplicatie pentru aplicatiile locale (RC, RL, Antecalcul, REG). In cluster cu serverele BASSRV01, BASSRV02, BASSRV04.	p570 8core 16GB	AIX	Oracle WebLogic Server Enterprise Edition Oracle HTTP Server Oracle Virtual Directory



Proiect cofinanțat din Fondul Social European prin
Programul Operațional Capacitate Administrativă 2014-2020!





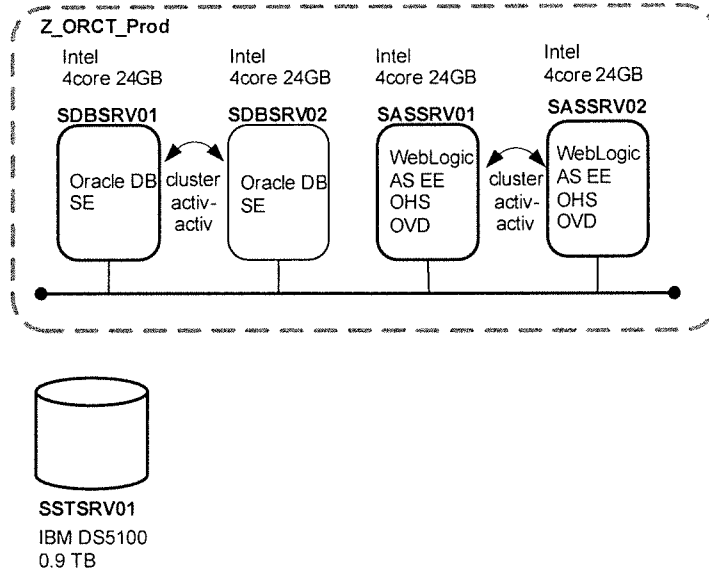
Zona	Denumire, IP	Rol	Platforma hardware	Sistem de operare	Software
Z_ORCTB_P rod	BASSRV04	Server de aplicatie pentru aplicatiile locale (RC, RL, Antecalcul, REG). In cluster cu cu serverele BASSRV01, BASSRV02, BASSRV03.	p570 8core 16GB	AIX	Oracle WebLogic Server Enterprise Edition Oracle HTTP Server Oracle Virtual Directory
Z_ORCTB_P rod	WLBSRV01	Load Balancer acces servicii web. Nod activ. In cluster cu WLBSRV02.	Intel 4core 6GB	Linux	Linux Server Virtual
Z_ORCTB_P rod	WLBSRV02	Load Balancer acces servicii web. Nod stand-by. In cluster cu WLBSRV01.	Intel 4core 6GB	Linux	Linux Server Virtual
Z_ORCTB_P rod	BBKPSRV01	Server de backup centralizat pentru infrastructura din ORCT Bucuresti.	Intel 4core 6GB	Linux	IBM Tivoli Storage Manager
Z_ORCTB_P rod	BSTSRV01	Server de stocare externa	IBM DS5100 10 TB	N/A	N/A
Z_ORCTB_P rod	BLISRV01	Biblioteca de benzi	IBM TS3310	N/A	N/A


 CONSOLIDAREA
 CAPACITĂȚII
 INSTITUȚIONALE

Proiect cofinanțat din Fondul Social European prin
 Programul Operațional Capacitate Administrativă 2014-2020!



Arhitectura fizică – Locatii ORCT Medii si Mici



Figură 4 Arhitectura fizică ORCT Medii si Mici

Zona	Denumire , IP	Rol	Platforma hardware	Sistem de operare	Software
Z_ORCT_Prod	SDBSRV 01	Server baza de date si integrare la nivel de date.	Intel 4core 24GB	Linux	Oracle Database Enterprise Edition Oracle Real Application Clusters Oracle Partitioning Oracle Advanced Security
Z_ORCT_Prod	SDBSRV 02	Server baza de date si integrare la nivel de date.	Intel 4core 24GB	Linux	Oracle Database Enterprise Edition Oracle Real Application Clusters Oracle Partitioning Oracle Advanced Security

Zona	Denumire , IP	Rol	Platforma hardware	Sistem de operare	Software
Z_ORCT_ Prod	SASSRV0 1	Server de aplicatie pentru aplicatiile locale (REG, RC si Taxe)	Intel 4core 24GB	Linux	Oracle Server Edition Oracle HTTP Server Oracle Virtual Directory WebLogic Enterprise
Z_ORCT_ Prod	SASSRV0 2	Server de aplicatie pentru aplicatiile locale (REG, RC si Taxe)	Intel 4core 24GB	Linux	Oracle Server Edition Oracle HTTP Server Oracle Virtual Directory WebLogic Enterprise
Z_ORCT_ Prod	SSTSRV0 1	Server de stocare externa	IBM DS5020 0.9 TB	N/A	N/A

Infrastructura Software

Aplicatii existente

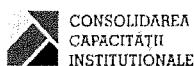
În sistemul informatic sunt utilizate mai multe categorii de produse software.

La nivelul ORCT:

- sisteme de operare:
 - o pe servere: Linux (RedHat, Fedora etc.) ;
 - o pe stații de lucru – Windows XP Professional, Windows Vista, Windows 7, Windows 8.x, Windows 10 Professional;
- pachete software antivirus pe fiecare stație de lucru și pe serverul de mail;
- pachete de tip Office: MS Office, Open Office;
- EMC Captiva – pentru sistemul de arhivare electronică a documentelor;
- alte pachete software pe stații de lucru: Adobe Acrobat Standard (pentru semnare electronică a documentelor pdf), Total Commander, Win Rar, Corel Draw etc.

La nivelul ONRC:

- sisteme de operare:
 - o pe servere: IBM AIX cu HACMP, Linux (RedHat, Fedora etc.) cu Samba, NFS, etc.; Windows 2000 Server, Windows 2003 Server;
 - o pe stațiile de lucru: Windows XP Professional, Windows Vista, Windows 7, Windows 8.x, Windows 10 Professional;



Proiect cofinanțat din Fondul Social European prin
Programul Operațional Capacitate Administrativă 2014-2020!



(Handwritten signatures)

- servere de baze de date (sisteme de gestiune de baze de date): Oracle Database 11g, Oracle RAC, IBM DB2, IBM DB2 Content Manager (ultimele două pe serverele de la sistemul de arhivare electronică a documentelor);
- servere web: apache, IBM HTTP server;
- servere de aplicații: Oracle Application Server 11g, WAS Network Deployment,
- software pentru back-up sisteme;
- software pentru dezvoltare aplicații: Oracle Developer Suite;
- produse Quest pentru monitorizare și replicare baze de date Oracle;
- servere ce asigură diverse servicii Internet: email, web, dns, nfs etc.;
- pachete software antivirus pe fiecare stație de lucru și pe serverul de mail;
- pachete de tip Office : MS Office, Open Office;
- servere pentru sistemul de arhivare electronică a documentelor: Captiva 5.x;
- alte pachete software pentru dezvoltare aplicații, procesare documente: Adobe Acrobat Standard (pentru semnare electronică a documentelor pdf), Macromedia, Adobe Acrobat Professional, produse Macromedia etc.

Aplicațiile care fac parte din Sistemul Informatic Integrat al ONRC (SII) sunt enumerate mai jos, împreună cu infrastructura tehnologică utilizată:

- **Registratura Locatie (RG)**
 - Nivelul de persistenta
 - RDBMS: Oracle 11g (RAC)
 - Nivelul aplicatie
 - Hibernate 3
 - Hibernate annotations
 - Spring 3.0.5
 - JBPM 4.4
 - Jasper Reports
 - Nivelul de prezentare
 - Wicket 1.4.6
 - WEBDAV
 - HTML/CSS
 - Weblogic Portal 11g
 - Nivelul de integrare date si procese
 - Oracle Streams
 - Apache CXF WS
 - Oracle ESB
 - Middle Tier
 - Weblogic Server 11g

- **Registrul Litigiilor (RL)**

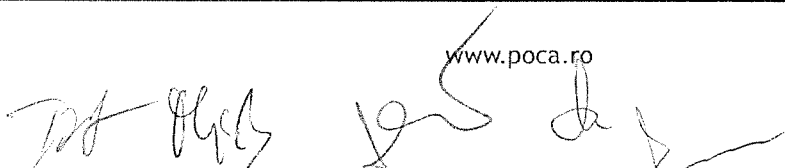
- Nivelul de persistenta
- RDBMS: Oracle 11g (RAC)
- Nivelul aplicatie
- Hibernate 3
- Hibernate annotations
- Spring 3.0.5
- JBPM 4.4
- Jasper Reports 4.0.1
- Nivelul de prezentare
- Oracle ADF
- HTML/CSS
- Weblogic Portal 11g
- Nivelul de integrare date si procese
- Oracle Streams
- Apache CXF WS
- Oracle ESB
- Middle Tier
- Weblogic Server 11g

- **Registrul Comertului (RC)**

- Nivelul de persistenta
- RDBMS: Oracle 11g (RAC)
- Nivelul aplicatie
- IBATIS
- Spring 3.0.5
- BIRT Reports
- Nivelul de prezentare
- HTML/CSS
- Oracle ADF
- Weblogic Portal 11g
- Nivelul de integrare date si procese
- Oracle Streams
- JAX -WS
- Oracle ESB
- Middle Tier
- Weblogic Server 11g

- **Buletinul Procedurilor de Insolventa (BPI)**

- Nivelul de persistenta



- RDBMS: Oracle 11g (RAC)
 - Nivelul aplicatie
 - Hibernate 3
 - Hibernate annotations
 - Spring 3.0.5
 - JBPM 4.4
 - Jasper Reports
 - Nivelul de prezentare
 - Wicket 1.4.6
 - WEBDAV
 - HTML/CSS
 - Weblogic Portal 11g
 - Nivelul de integrare date si procese
 - Oracle Streams
 - Apache CXF WS
 - Oracle ESB
 - Middle Tier
 - Weblogic Server 11g
-
- **Portalul Serviciilor Online al institutiei ONRC**
 - Nivelul de persistenta
 - RDBMS: Oracle 11g (RAC)
 - Nivelul aplicatie
 - Hibernate 3
 - Hibernate annotations
 - Spring 3.0.5
 - JBPM 4.4
 - Jasper Reports
 - Nivelul de prezentare
 - Specificatia Portlet 286 (implementarea Weblogic)
 - Wicket 1.4.6
 - WEBDAV
 - HTML/CSS
 - Nivelul de integrare ata si procese
 - Oracle Streams
 - Apache CXF WS
 - Oracle ESB
 - Middle Tier
 - Weblogic Portal 11g
 - **Antecalcul**

- Nivelul de persistenta
 - RDBMS: Oracle 11g (RAC)
 - Nivelul aplicatie
 - Hibernate 3
 - Hibernate annotations
 - Spring 3.0.5
 - JBPM 4.4
 - Jasper Reports
 - Nivelul de prezentare
 - Wicket 1.4.6
 - WEBDAV
 - HTML/CSS
 - Weblogic Portal 11g
 - Nivelul de integrare date si procese
 - Oracle Streams
 - Apache CXF WS
 - Oracle ESB
 - Middle Tier
 - Weblogic Server 11g
-
- **Publicare date catre alte institutii**
 - Oracle ESB
 - Oracle 11g Database
-
- **Sistem de securitate interna (central si local) si externa (Aplicatia Centralizata de Management Utilizatori - ACMU)**
 - Oracle Identity Manager 11g
 - Oracle Access Manager 11g
 - Oracle Web Gate
-
- **Raportare Analitica**
 - Oracle Business Intelligence Suite Enterprise Edition 11g
-
- **Aplicatia de acces utilizatori**
 - Oracle ADF
 - Oracle Weblogic 11g
 - Oracle Database 11g



- **Replicare masiva de date**
 - SharePlex for Oracle

Infrastructura tehnologică utilizată de catre SAE (Sistemul de Arhivare Electronica)

- WebSphere AS
- DB2 Content Manager
- Java
- UDB DB2

În **ONRC** sunt implementate politici IT referitor la următoarele domenii:

- Securitatea informatiei si controlul accesului;
- Disponibilitatea sistemelor ;
- Proceduri de backup / restore;
- Plan de continuitate;
- Arhivarea datelor.

Securitatea informatiei si controlul accesului

Având în vedere faptul ca informațiile registrului comerțului sunt informații publice, măsurile de asigurare a securității s-au concentrat, până în prezent, în special pe asigurarea funcționării continue a sistemului informatic, de care depinde buna desfășurare a activității instituției.

Securitatea sistemelor informatice la nivelul ONRC este asigurată astfel:

- la nivel fizic – prin reguli de acces fizic la resursele IT (stații de lucru, imprimante, echipamente active de rețea, echipamente de comunicație, firewall);
- prin implementarea unei arhitecturi a sistemului informatic care să asigure protecție maximă la accesele din afara rețelei.
- la nivelul ONRC, prin intermediul unui firewall central, care împarte rețeaua ONRC în zone demilitarizate (DMZ – DeMilitarized Zone), rețea internă, respectiv zona rețelelor virtuale private (VPN și Extranet VPN);
- la nivelul fiecărui ORCT, prin intermediul unui firewall, care împarte rețeaua ORCT în zonă demilitarizată (DMZ – DeMilitarized Zone), rețea internă, respectiv zona rețelei virtuale private (VPN);
- prin controlul accesului utilizatorilor la resursele IT:
- controlul accesului utilizatorilor la nivelul stațiilor de lucru
- controlul accesului la serverul DNS (în DMZ);
- controlul accesului la serverul Internet de mail;

- controlul accesului la serverele web – care găzduiesc site-ul web oficial al instituției – www.onrc.ro, intranet.onrc.ro, portal.onrc.ro, etc (în DMZ-uri);
- controlul accesului la serverele de baze de date interne;
- controlul accesului la imprimante;
- controlul accesului la echipamentele active de rețea (switch-uri) și routere;
- controlul accesului la firewall-uri ;
- prin implementarea de reguli de acces la aplicații și informații: regulile de acces la aplicații și informații sunt stabilite pe baza atribuțiilor angajaților din fișele de post;
- prin programe specifice instalate pe echipamente (stații de lucru, servere) ce asigură protecția antivirus, antispyware;
- prin reguli de acces implementate la nivelul firewall-urilor și router-elor, reguli ce asigură protecția resurselor IT și informații atât în fața acceselor din afara rețelei cât și din interior:
- reguli de acces implementate la nivelul router-ului ce asigură conexiunea Internet
- reguli de acces implementate la nivelul firewall-urilor instalate pe stațiile de lucru.
- prin monitorizarea permanentă a echipamentelor și pachetelor software ce asigură securitatea sistemelor informatice:
- monitorizarea funcționării firewall-urilor;
- monitorizarea funcționării router-elor;
- monitorizarea funcționării pachetului antivirus pe serverul de mail (mail.onrc.ro)
- monitorizarea serverului pentru update-uri la produsele antivirus de pe stații de lucru.

Disponibilitatea Sistemelor / High Availability

Avind în vedere ca asigurarea funcționării continue a sistemului informatic este un obiectiv prioritar în strategia IT a ONRC, au fost implementate soluții pentru asigurarea funcționării continue a echipamentelor critice după cum urmează:

- soluții de tip cluster pentru servere
- echipamente de rezervă, configurate identic cu cele în funcțiune (exemplu : firewall central) ;
- echipamente de rezervă (în special switch-uri) ;

Proceduri de Backup / Restore

La nivelul bazelor de date politica de backup se realizează după cum urmează:

- Baze de date Oracle (utilizate de către SII): salvarea bazelor de date Oracle se realizează periodic pe bandă prin intermediul Tivoli Storage Manager și pe dispozitive de tip SmartBackup cu acces rapid; procedura de backup / restore

- prevede atât full online și offline backup cât și salvări incrementale;
- Baze de date DB2 (utilizate de către sistemul de arhivare electronică): salvarea bazelor de date DB2 se realizează periodic pe bandă prin intermediul Tivoli Storage Manager; procedura de backup / restore prevede atât full offline backup cât și salvări incrementale.

La nivelul sistemului de operare politica de backup se realizează după cum urmează:

- Pentru serverele Intel există platforme de rezervă care pot fi utilizate pentru a înlocui o eventuală mașină defectă;
- Pentru platformele AIX se utilizează configurații de înaltă disponibilitate care permit comutarea rapidă a încărcării de pe un nod defect pe un nod funcțional.

3 Descrierea noului sistem informatic

3.1 Rezultate așteptate

Oficiul Național al Registrului Comerțului, aflat în subordinea Ministerului Justiției, are în vedere derularea de proiecte care să vizeze atingerea obiectivelor sale strategice, prevăzute în legislația aplicabilă și în strategiile sectoriale. În ultimii ani, ONRC a urmărit în mod constant creșterea eficienței și transparenței serviciilor furnizate către terți, în concordanță cu strategia de informatizare a sistemului judiciar și cu strategiile din domeniul e-guvernării.

Buletinul Electronic al Registrului Comerțului

Prin implementarea și dezvoltarea subsistemului informatic Buletinul Electronic al Registrului Comerțului, sub forma unei platforme electronice se urmărește derularea cu celeritate și producerea efectelor scontate a serviciului organizat de Oficiul Național al Registrului Comerțului în îndeplinirea obligației de publicare pe pagina de Internet a instituției a actelor și informațiilor prevăzute în mod expres de lege în sarcina sa, precum și a informațiilor privind mențiunile efectuate din oficiu în registrul comerțului, în baza hotărârilor judecătorești comunicate de instanțele judecătorești sau a altor înregistrări emise de autorități și instituții publice.

Acest instrument electronic, Buletinul Electronic al Registrului Comerțului, va asigura și baza materială necesară punerii în aplicare a viitoarelor prevederi normative privind simplificarea formalităților de asigurare a publicității actelor profesioniștilor.

Astfel, proiectul de lege privind registratorii comerciale și activitatea de înregistrare în registrul comerțului, reglementează, pe lângă înființarea profesiei de registrator comercial și instituirea procedurii de soluționare a cererilor de înregistrare în registrul comerțului și extinderea categoriilor de acte, fapte și mențiuni ale profesioniștilor și ale celorlalte persoane juridice supuse obligației de înregistrare în registrul comerțului, pentru care asigurarea publicității se va realiza de către Oficiul Național al Registrului

Comerțului prin intermediul unei platforme electronice centrale, Buletinul Electronic al Registrului Comerțului.

La data de 14 ianuarie 2010 a intrat în vigoare O.U.G. nr.116/2009 pentru instituirea unor măsuri privind activitatea de înregistrare în registrul comerțului, astfel încât (...) **competența de soluționare a cererilor de înregistrare în registrul comerțului și, după caz, a altor cereri aflate în competența de soluționare a judecătorului delegat aparține, până la reglementarea activității de înregistrare în registrul comerțului efectuată de registratori comerciali directorului oficiului registrului comerțului de pe lângă tribunal și/sau persoanei sau persoanelor desemnate de către directorul general al Oficiului Național al Registrului Comerțului.**

Așadar, având în vedere contextul social economic care impunea, pe de o parte, o decongestionare a activității judiciare prin luarea unor măsuri energice de remediere a supraîncărcării instanțelor și, pe de altă parte, o fluidizare a procedurilor aferente activității comerciale, competența de soluționare a cererilor de înregistrare în registrul comerțului și, după caz, a altor cereri aflate în competența de soluționare a judecătorului delegat a fost preluată, până la reglementarea activității de înregistrare în registrul comerțului, de registratori comerciali, directorul oficiului registrului comerțului de pe lângă tribunal și/sau persoanei ori persoana desemnata de către directorul general al Oficiului Național al Registrului Comerțului.

O.U.G. nr.116/2009 a fost aprobată cu modificări și completări prin Legea nr.84/2010, ulterior fiind modificată de O.U.G. 85/2010.

Ministerul Justiției a elaborat un proiect de lege privind registratorii comerciali și activitatea de înregistrare în registrul comerțului, prin care se propune ca activitatea de registru să se desfășoare sub control administrativ.

Pornind de la aceste legiferări, prin proiectul de lege mai sus amintit se reglementează:

- Procedura de înregistrare în registrul comerțului în baza controlului registratorului comercial sau, după caz, în baza hotărârii instanței judecătorești;
- Profesia de registrator comercial;
- Extinderea categoriilor de acte ale persoanelor supuse obligației de înregistrare în registrul comerțului, pentru care Oficiul Național al Registrului Comerțului asigură efectuarea publicității prin Buletinul Electronic al Registrului Comerțului, organizat ca un instrument electronic;
- Modul de organizare și funcționare a Oficiului Național al Registrului Comerțului și a oficiilor registrului comerțului.

Extinderea categoriilor de acte și informații supuse publicității prin Buletinul Electronic al Registrului Comerțului este în acord și cu prevederile Directivei 2009/101 a Parlamentului European și a Consiliului din 16 septembrie 2009, de coordonare, în vederea echivalării, a garanțiilor impuse societăților în statele

membre, în înțelesul articolului 48 al doilea paragraf din tratat, pentru protejarea intereselor asociațiilor sau terților, care, la art. 3 alin. (5)–(6), conferă statelor membre dreptul de a asigura publicitatea actelor și faptelor profesioniștilor și prin intermediul portalului ONRC.

Subsistemul informatic "Buletinul Electronic al Registrului Comerțului" va asigura pe de-o parte colectarea online sau la ghiseu, procesarea și publicarea datelor și documentelor supuse publicității și pe de alta parte va asigura consultarea online prin intermediul portalului ONRC și a unei aplicații mobile de către publicul larg, mediul de afaceri și autoritățile publice a buletinelor electronice publicate.

Subsistemul Informatic Colaborativ

Un factor determinant în îmbunătățirea proceselor interne și a capacității de furnizare a serviciilor publice îl constituie crearea unui cadru colaborativ (cu precădere pe orizontală între angajații distribuiți teritorial care împartășesc aceeași specialitate / pregătire / responsabilități) care să susțină și să încurajeze partajarea de idei, opinii, abordări, soluții referitoare la problemele profesionale curente. Obiectivul principal al cadrului colaborativ va fi acela de susținere a fluxurilor informaționale și procedurilor formale existente în cadrul organizației și de facilitare a comunicării în cadrul comunităților interne de specialiști în domeniile de interes ale ONRC (juridic, IT, etc).

Totodată, cadrul colaborativ va avea în vedere și susținerea proceselor integratoare la nivelul instituției cum ar fi: gestiunea proiectelor, gestiunea incidentelor software, gestiunea ciclului de viață al aplicațiilor software, etc.

În vederea stabilirii proceselor interne asupra cărora cadrul colaborativ poate avea un impact semnificativ, se va derula o etapă de analiză a sistemului informațional-decizional existent. Pe baza acestei analize vor fi identificate:

1. Comunitățile interne de specialiști (juridic, IT, etc) – a căror colaborare pe orizontală contribuie atât la perfecționarea lor cât și îmbunătățirea calității serviciilor prestate
2. Departamentele care sunt implicate în activități specifice derulate de regulă prin intermediul proiectelor interne
3. Organizarea actuală a echipelor de IT pentru dezvoltarea, administrarea și întreținerea sistemelor informatice ale ONRC
4. Propuneri privind crearea cadrului colaborativ la nivelul instituției având în vedere elementele identificate la punctele 1-3

Rezultatele analizei sistemului informațional-decizional existent vor fi utilizate în cadrul etapei de analiză pentru elaborarea specificațiilor tehnice ale subsistemului informatic de tip "Colaborativ" (SSICO).

Grupul tinta pentru implementarea SSICO îl reprezintă angajații ONRC ce participă în procesele identificate în etapa de analiză a sistemului informațional-decizional existent. Activitățile/procesele avute cu prioritate în vedere de ONRC sunt cele în care pot fi implicați un număr cât mai mare de angajați, distribuiți la nivel teritorial, printre care enumerăm următoarele – fără a ne limita doar la acestea:

- Elaborarea răspunsurilor la solicitări atipice ale operatorilor economici privind înregistrări în registrul comerțului
- Elaborarea răspunsurilor la solicitări atipice ale persoanelor fizice/juridice privind înregistrări în BPI
- Managementul proiectelor interne ONRC (de ex. cu finanțare externă)
- Dezvoltarea / Testarea / Îmbunătățirea aplicațiilor software
- Elaborarea de cerințe funcționale / documentații în vederea achiziționării de servicii / produse

Subsisteme informatice de monitorizare a performanțelor și asigurarea securității SII al ONRC

Din punctul de vedere al tehnologiilor de asigurare a securității și a disponibilității, Sistemul Informatic Integrat al ONRC nu a mai fost actualizat de ceva timp după lansarea acestuia în producție.

În contextul unei evoluții continue a amenințărilor cibernetice, a nevoii de diversificare a serviciilor oferite prin intermediul internetului și de asigurare a unei disponibilități de nivel înalt pentru aceste servicii, ONRC își propune ca prin implementarea acestui proiect să întărească Sistemul Informatic Integrat prin actualizarea/inlocuirea tehnologiilor folosite în prezent și prin instruirea corespunzătoare a personalului de specialitate pentru a face față noilor provocări.

Tendința actuală în crearea sistemelor informatice integrate încorporează elementele de securitate – în special, și cele de monitorizare – în secundar, la toate nivelurile și încă din faza de concepție a sistemului. Astfel, primele elemente le vom avea la nivelul preponderent hardware, care, conform nevoilor specifice generate de subsistemele de business, poate fi împărțit la rândul lui în trei zone relevante, respectiv procesarea datelor, stocarea datelor și interconectarea la nivelul rețelei beneficiarului; propunerea de față adresează aceste zone cu câte un subsistem dedicat.

În continuare, nevoile de securitate și monitorizare se concentrează pe nivelul preponderent software, iar definirea zonelor adresate încearcă nu doar să răspundă cerințelor beneficiarului ci să și maximizeze oportunitățile de dezvoltare ale acestuia în viitorul apropiat – atât din perspectiva sistemelor în sine și tendințelor tehnologice cât și la nivel organizațional – preponderant dpdv împărțire zonala.

Revenind la nivelul hardware, nevoilor de procesare li se răspunde cu o soluție modernă cu trei atribute de bază: putere, densitate și scalabilitate. Puterea este reprezentată de procesoare de ultimă generație, iar densitatea și scalabilitatea rezidă din arhitectura modulară (sasiu + servere); ultimul reper fiind partea

de interconectare privata – între subsistemul de procesare și cel de stocare. De menționat că, la nivel de set – sasiu + servere blade, soluția trebuie să prevadă astfel de seturi pentru fiecare site.

În continuare, nevoilor de stocare li se răspunde cu o soluție completă de stocare ale cărei atribute de bază trebuie să fie disponibilitatea, flexibilitatea și scalabilitatea. Dacă disponibilitatea este asigurată de arhitectura dual-controller în special, și flexibilitatea rezidă din capacitățile de multi-protocol și multiple tipuri de matrici RAID suportate, scalabilitatea rezultă din capacitățile majore de extindere facilă a spațiului de stocare.

Comunicarea între cele două subsisteme de mai sus este reprezentată distinct de subsistemul de interconectare privată, care asigură un acces uniform al nodurilor de procesare atât la zone de stocare cât și către zona de rețea; nivelul de performanță al acestui subsistem nu va trebui să îngreuneze sub nici o formă nivelurile de performanță în procesarea și respectiv stocarea datelor.

Din punctul de vedere al monitorizării performanțelor, relevant pentru proiect sunt trei zone distincte, respectiv dezvoltarea și exploatarea aplicațiilor, accesul la date și serviciile. Acoperirea primelor două zone va aduce beneficiarului vizibilitatea și controlul necesar din punct de vedere al accesului la date și performanțelor pe toată durata de viață a aplicațiilor dezvoltate, ultima zonă conturează o imagine de ansamblu la nivel general de rețea și organizațional, înglobând capacități de monitorizare a traficului și a experienței utilizatorului – sub-zona din ce în ce mai sensibilă în contextual actual de orientare spre consumatorul de drept (cetățeanul) al serviciilor publice.

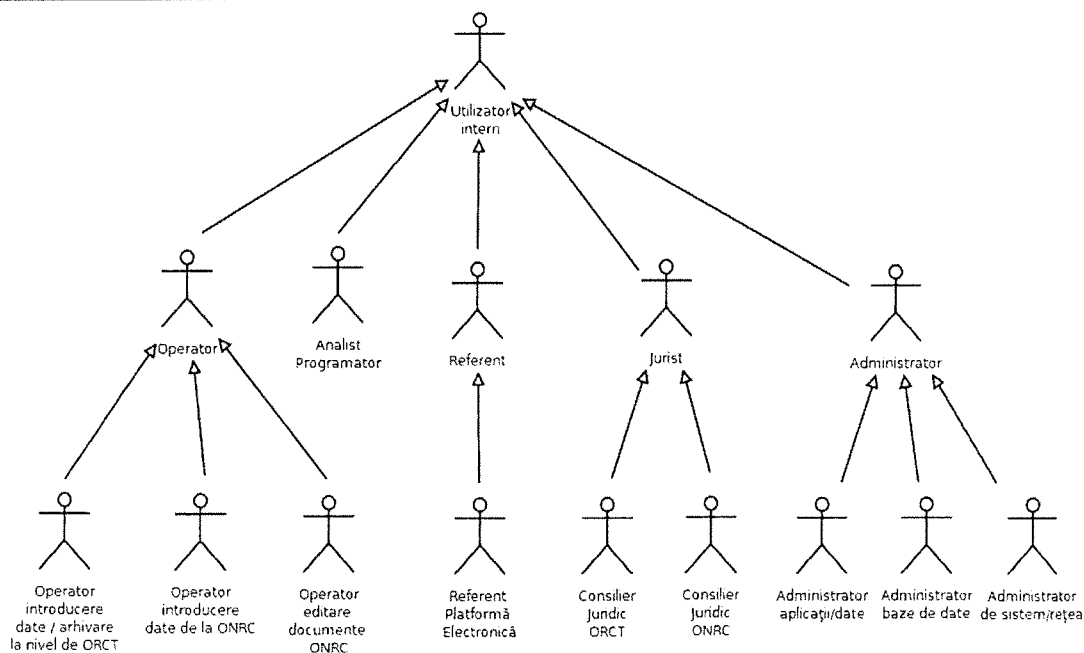
Pentru zona de Securitate și audit, stringentele implică o complexitate sporită, iar această complexitate nu este generată doar de dezvoltarea tehnologică în ansamblu, ci și de multitudinea aplicațiilor și tehnologiilor folosite intern de către beneficiar. Astfel, zonele de adresat în cadrul proiectului sunt: testarea și remedierea securității aplicațiilor, distribuția accesului și protecția serviciilor de aplicație, protecția antimalware și a resurselor la nivel client, analiza reurselor utilizate și managementul datelor de audit.

3.2 Utilizatorii noului sistem informatic

3.2.1 Utilizatori interni (personal ONRC)

Nume User
Operator introducere date/arhivare la nivel de ORCT
Consilier Juridic ORCT
Operator introducere date de la ONRC, după caz

Consilier Juridic ONRC
Operator verificare/validare documente ONRC
Referent subsistem BERC
Administrator aplicații/date
Administrator baze de date
Administrator de sistem/rețea/comunicații/securitate
Specialist IT
Director Platformă electronică/Șef Serviciu Platformă electronică



Figură 5 Utilizatorii interni ai sistemului



Handwritten signatures and marks at the bottom of the page.

Nr. crt.	Cod utilizatori	Denumire	Descriere utilizatori
1	US1	Operator introducere date/arhivare la nivel de ORCT	<ul style="list-style-type: none"> - Preluare/prelucrare acte primite de la profesioniști; - generare si incarcare acte pentru a fi publicate; - trimitere acte la ONRC pentru a fi publicate în BERC; - arhivare acte în Sistemul de Arhivare Electronic.
2	US2	Consilier Juridic ORCT	<ul style="list-style-type: none"> - verifică actele primite de la profesioniști; - verifică datele de identificare ale profesionistului.
3	US3	Consilier Juridic ONRC	<ul style="list-style-type: none"> - verifică actele primite de la ORCT, dupa caz; - verifică datele de identificare ale profesionistului, dupa caz; - verifică corectitudinea numerelor de BERC înainte de publicarea lor în BERC.
4	US4	Operator verificare date la ONRC	<ul style="list-style-type: none"> - verificarea datelor în aplicația BERC al registrului comerțului aferente actelor primite spre publicare.
5	US5	Operator validare documente ONRC	<ul style="list-style-type: none"> - selectarea/validarea actelor în vederea realizării unui BERC; - redactarea actelor care necesită acest lucru, dupa caz; - rularea macro-urilor pentru realizarea buletinului; - redactarea BERC, dupa caz.
6	US6	Referent BERC	<ul style="list-style-type: none"> - gestionarea corespondenței cu clienții; - gestionarea contractelor și a cererilor de furnizare primite de la persoanele interesate; - întocmirea documentelor solicitate ca urmare a încheierii unui contract/protocol de furnizare; - livrarea informațiilor și documentelor pentru care există contract/protocol, clienților.
7	US7	Administrator aplicații / date	<p>Administratorul aplicații/date va avea următoarele atribuțiuni:</p> <ul style="list-style-type: none"> - instalare aplicații; - configurare aplicații; - administrare roluri/grupuri de utilizatori aplicații; - administrare securitate aplicații; - utilizare/configurare module de administrare a aplicațiilor; - gestiunea datelor aplicațiilor; - monitorizarea evenimentelor apărute în exploatarea aplicațiilor; - analiza logurilor/jurnalelor de aplicații.



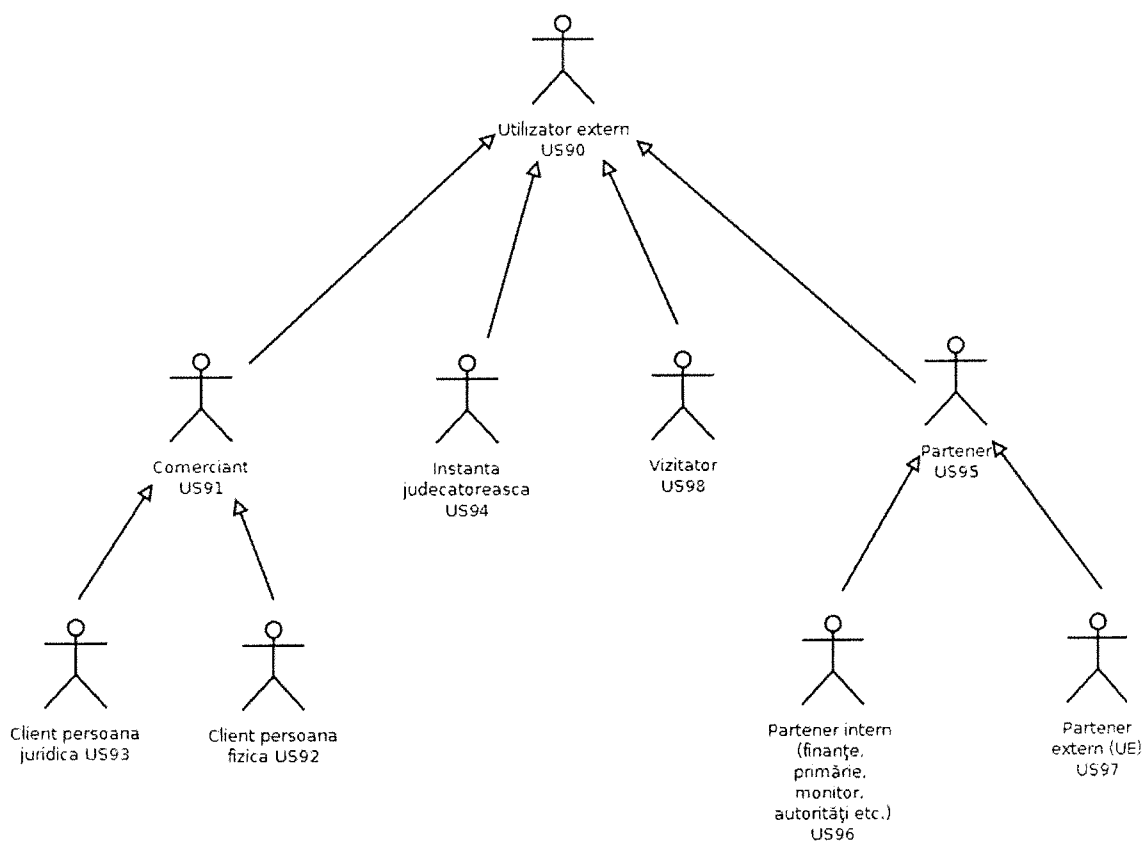
Nr. crt.	Cod utilizatori	Denumire	Descriere utilizatori
8	US8	Administrator baze de date	<ul style="list-style-type: none"> - coordonează actualizarea și asigura protecția bazei de date utilizând mijloace puse la dispoziție de software-ul existent; - administrează și exploatează baza de date; - administrează transmiterea și recepția datelor către diverse baze de date, în temeiul legii sau a acordurilor de cooperare, la termenele și în modalitățile convenite cu instituțiile care țin și gestionează bazele de date respective.
9	US9	Administrator de sistem/rețea/comunicații/securitate	<p>Administrator IT având următoarele atribuții:</p> <ul style="list-style-type: none"> - instalarea sistemelor de calcul si/sau a rețelelor; - configurarea sistemelor de calcul si/sau a rețelelor; - gestiunea utilizatorilor sistemelor de calcul; - monitorizarea evenimentelor apărute în exploatarea sistemelor de calcul/rețelelor; - optimizarea sistemelor de calcul/rețelelor; - instalarea aplicațiilor și a sistemelor software de sistem.
10	US10	Specialist IT	<ul style="list-style-type: none"> - elaborează și participa la elaborarea de noi aplicații și programe informatice, în scopul informatizării și optimizării tuturor activităților desfășurate; - instruește utilizatorii produselor informatice elaborate de Oficiul Național al Registrului Comerțului și răspunde de utilizarea bazelor de date în condiții corecte și strict în limitele autorizate de acces.
11	US11	Director BERC/Șef Serviciu BERC	<p>Coordonează, avizează și controlează activitățile specifice transmiterii și publicării actelor în Buletinul Electronic al Registrului Comerțului;</p> <p>Repartizează cererile de furnizare, comenzile și contractele/protocoale de furnizare informații, precum și orice adresa referitoare la furnizarea informațiilor din BERC după înregistrarea acestora la registratura generala;</p> <p>Coordonează, avizează și controlează activitățile de elaborare instrucțiuni de lucru/norme metodologice, puncte de vedere si/ sau proiecte de acte normative, alte documente, specifice Platformei electronice, efectuare control asupra activității Platformei electronice, alte activități incidente.</p>

3.2.2 Utilizatori externi (grupurile țintă)

Cod User	Nume User
US91	Client persoană fizică
US92	Client persoană juridică
US93	Instanța judecătorească sau asimilat
US94	Partener intern (administrație financiară, primărie, monitor, autorități etc.)
US95	Partener extern (UE)
US96	Vizitator

Nr. crt	Cod utilizator	Denumire	Descriere utilizatori
1.	US91	Profesionist	Persoană înregistrată în Registrul Comerțului
2.	US92	Client persoana fizica	Persoana fizică care intră în relație cu BEREC a ONRC
3.	US93	Client persoana juridica	Persoana juridică care intră în relație cu BEREC a ONRC
4.	US94	Instanța judecătorească saua similat	Instanța judecătorească sau asimilat care emite hotărâri/documente cu impact semnificativ în procesele operaționale ONRC
5.	US95	Partener	O entitate care schimbă informații cu BEREC bazat pe o convenție sau o înțelegere
6.	US96	Partener intern (administrație financiară, primărie, monitor, autorități etc.)	Autorități cu care ONRC are protocoale de colaborare
7.	US97	Partener extern (UE)	Autorități externe cu care ONRC are protocoale de parteneriat în cadrul și în afara UE

Nr. crt	Cod utilizator	Denumire	Descriere utilizatori
8.	US98	Vizitator	Un utilizator cu drepturi limitate care accesează online sistemele ONRC



Figură 6 Utilizatori externi ai sistemului

3.2.3 Managementul utilizatorilor si accesul la sistem

Utilizatorii noului sistem si accesul la aplicațiile acestuia vor fi gestionați folosind solutia existenta pentru managementul accesului, implementata pe baza următoarelor produse: Oracle Internet Directory (server director cu rol de depozit de profiluri de utilizator) si Oracle Access Manager (server management acces).

Aplicațiile noului sistem se vor integra cu soluția de managementul accesului și utilizatorilor, în sensul că vor utiliza profilurile de utilizatori deja existente în cadrul serverului director. Utilizatorii care au acces în noul sistem vor fi diferențiați prin adăugarea unui nou atribut în profilurile stocate în serverul director.

Mecanismele de acces implementate în prezent vor fi reutilizate pentru a securiza și aplicațiile noului sistem. În acest scop, aplicațiile noului sistem vor avea capacitatea de a se integra cu platforma de control acces, permițând autentificarea utilizatorilor de către serverul de control acces. Autentificarea se va realiza pe baza de utilizator și parolă sau pe baza de certificat digital.

Autorizarea utilizatorilor va fi realizată prin mecanismele puse la dispoziție de fiecare aplicație a noului sistem sau prin utilizarea facilităților de autorizare ale serverului de management acces. Accesul la aplicații va fi permis numai utilizatorilor autorizați în acest sens.

4 Cerințe privind soluția tehnică

4.1 Cerințe generale

Soluțiile ce vor fi implementate trebuie să țină cont de următoarele recomandări de abordare a unui sistem informatic modern și deschis:

- abordare unitară, etapizată, folosind metodologii și tehnologii adecvate;
- sisteme pre-integrate - pe cât posibil de la același producător;
- arhitectura modulară și deschisă, bazată pe standarde;
- sistem centralizat cu punct de administrare unic;
- arhitectura tip 'Internet'/'Intranet';

Toate informațiile, cerințele, funcționalitățile prezentate în acest document nu sunt exhaustive. Intenția acestui document este de a furniza o privire de ansamblu asupra proiectului și nu poate fi înțeles ca fiind o descriere detaliată a cerințelor proiectului. Cerințele detaliate ale proiectului vor fi definite în fazele inițiale de implementare a acestui proiect.

4.1.1 Subsistemul Buletinul Electronic al Registrului Comerțului

Subsistemul informatic propus trebuie să fie modular, ușor extensibil și să fie bazat pe următoarele module de soluție:

- componenta portal care să permită definirea și găzduirea tuturor interfețelor cu utilizatorii externi;

- componenta de gestiune conținut și documente care să permită stocarea documentelor în format electronic, regăsirea acestora folosind criterii de selecție bazate pe atribute și arhivarea documentelor electronice conform unor politici de retenție personalizabile;
- componenta de gestiune a bazelor de date pentru stocarea sigură a datelor sub forma unei baze de date relaționale (SGBDR) cu capabilități extinse de replicare și backup;
- componenta server de aplicații care să ofere suport sigur și scalabil de rulare pentru toate modulele proiectului (integrare, gestiune conținut, portal, etc.);
- componenta de integrare aplicații bazată pe standarde deschise care să permită coexistența noului proiect cu aplicațiile deja existente la ONRC;
- componenta de integrare a datelor care să asigure popularea / migrarea datelor utilizând sursele de date existente în ONRC și să permită sincronizarea și consolidarea datelor;

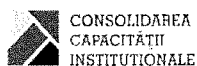
4.1.2 Subsistemul Colaborativ

Subsistemul propus trebuie să fie modular, ușor extensibil și să fie bazat pe următoarele componente funcționale:

- O componenta de colaborare menită să ajute echipele implicate în proiecte să urmărească toate activitățile necesare efectuării de sarcini zilnice și periodice, incluzând dar nu limitat derularea proiectelor, gestionarea proceselor interne de aprobare, crearea documentelor și a fluxurilor de lucru modelate pe procesele de business
- O componenta pentru managementul integrat al cerințelor de business, managementul cazurilor și scenariilor de test, managementul librăriilor de teste manuale, automate, de funcționalitate, performanță, și securitate/integritate a aplicațiilor. Managementul defectelor identificate și menținerea transabilității între defecte, cazuri de testare și cerințe.
- O componenta pentru crearea și managementul testării automate software, care are la baza limbaje de scripting de ultimă generație (Javascript, C sharp, jscript/python, etc) cu suport pentru Continuous integration/continuous delivery și cu posibilitatea de includere de librării externe open-source în crearea testelor automate;
- O componenta de testare a aplicațiilor, pentru măsurarea comportamentului sistemului și a performanței componentelor aplicației sub sarcină cu suport pentru Continuous integration/continuous delivery. Acesta ar permite simularea activității utilizatorilor prin generarea de mesaje între componentele aplicației sau prin simularea interacțiunilor utilizatorului cu interfața de lucru în aplicație, prin intermediul scripturilor create manual sau în mod automat.

4.1.3 Sub sisteme de monitorizare a performanțelor și asigurarea securității SII al ONRC

Modulele avute în vedere pentru construirea subsistemului de monitorizare sunt:



Proiect cofinanțat din Fondul Social European prin
Programul Operațional Capacitate Administrativă 2014-2020!



- Soluții de monitorizare și diagnosticare end to end, incluzând monitorizarea instrumentelor hardware și software, a serviciilor informatice pentru identificare proactivă și reactivă a potențialelor probleme care pot duce la degradarea serviciilor oferite de către ONRC către beneficiari, fie ei direcți sau indirecti, precum și performanța, continuitatea și disponibilitatea fluxului de informații în relațiile cu instituțiile avizatoare și cele guvernamentale
- Modul software pentru monitorizarea performanței tranzacțiilor serviciilor informatice în medii tradiționale, virtualizate sau în cloud, pentru izolarea rapidă a problemelor de performanță prin diagnoza de tip „deep dive” care identifică unitățile de cod cu probleme de performanță cum ar fi metode ale obiectelor din cod sau statement-uri sql. Identifică și agregă tranzacții la nivel de utilizator, server, baza de date și back end.
- Modul software pentru măsurarea în mod proactiv a experienței utilizatorilor prin executarea într-un mod controlat, repetat de tranzacții din locații multiple înainte sau după sistemele de protecție de tip firewall, pentru a identifica disponibilitatea și performanța sistemelor și a aplicațiilor.
- Modul software de diagnosticare care monitorizează starea aplicației în mediile tradiționale, virtualizate sau cloud, funcționând în stările de pre-producție și producție pentru o rapidă diagnosticare a blocajelor în performanța aplicațiilor și aduc o îmbunătățire a calității acestora.
- Instrumente de monitorizare activitatea bazelor de date prin captarea traficului de rețea, generând loguri de audit.

Din perspectiva securității, modulele avute în vedere sunt:

- Componente integrate și performante de asigurare a fiabilității și funcționalității sistemelor și soluțiilor informatice implementate, precum și a securității, prin implementarea de soluții de testare manuală și automată a instrumentelor software dezvoltate intern și/sau extern pentru asigurarea de înaltă calitate, de testare de securitate pentru înlăturarea potențialelor vulnerabilități chiar din stadiile incipiente ale dezvoltării instrumentelor, de testare a performanțelor instrumentelor software pentru eficientizarea fluxului de informații, a managementului procesului de testare, etc;
- Modul software cu capacități de suport și creare de analiză software cu capacitate de raportare detaliată pentru metrici de software cu privire la release-uri, cod sursă, bune practici de programare, și standarde de Securitate în programare, cu capacități de măsurare a performanței echipei de dezvoltare (având în vedere cerințele legale și instituționale cu privire la securitatea sistemelor dar și la complexitatea soluțiilor

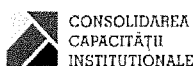
informatică necesare și creșterea complexității atacurilor informatice asupra instituțiilor publice

- Instrumente de analiză a accesului utilizatorilor la aplicațiile web protejând aplicațiile și datele de atacurile cibernetice, cu capacități de învățare în mod dinamic a comportamentului "normal" al aplicațiilor, de actualizată în timp real pentru a oferi o protecție superioară.
- Modul software pentru scanarea dinamică sau statică a codului sursă cu acoperire în cât mai multe tehnologii posibile pentru identificarea vulnerabilităților de securitate și verificarea acestora. Este necesar să facă și recomandări de remediere a vulnerabilităților identificate în urma scanării. Trebuie să prezinte acuratețe mare în identificarea vulnerabilităților și realizarea de recomandări de remediere și reducerea de tip "false-positive". Trebuie să prezinte capacități de actualizare constantă a bazei de date cu noi tipuri de vulnerabilități și să permită identificarea vulnerabilităților de tip "0 day".
- Soluție de securitate pentru detectarea și identificarea vulnerabilităților din cadrul rețelei, monitorizarea activă de detectare a potențialelor breșe de securitate.
- Instrumente de tip firewall la nivel de aplicație, pentru protecția aplicațiilor web, precum și analiza dinamică de malware.
- Instrumente pentru colectarea, agregarea și colectarea de evenimente de securitate, astfel încât să se permită detectarea de incidente care afectează buna desfășurare a serviciilor.
- Instrumente de punere în aplicare și asigurare a securității datelor, prin implementarea de politici care reglementează și restricționează modul în care utilizatorii interni utilizează și transferă date cu caracter confidențial prin instrumente comune, cum ar fi e-mail, imprimare și unități USB și/sau CD
- Instrumente de detectare a atacurilor avansate și cu capacități de transformare a informațiilor despre atacuri în acțiuni de protecție imediate, cu capacități adiționale de inspecție ce pot duce la o largă detectare și descoperire de potențiale atacuri
- Instrumente de captură de date privind interacțiunile interne și/sau externe ale utilizatorilor în raport cu aplicațiile utilizate, de declansarea de alerte privind evenimentele suspecte în timp real, cu capacități în auditare și detectarea fraudelor.
- Instrumente de detectare și remediere automată pentru potențiale atacuri de tip troian și malware, ransomware, cu capacități de creare și implementare de politici proprii, de corelare a indicatorilor proveniți din diverse surse.

4.2 Cerințe funcționale

4.2.1 Subsistemul Buletinul Electronic al Registrului Comerțului

Din punct de vedere funcțional, subsistemul „Buletinul Electronic al Registrului Comerțului” va conține următoarele module dezvoltate customizat pentru ONRC:



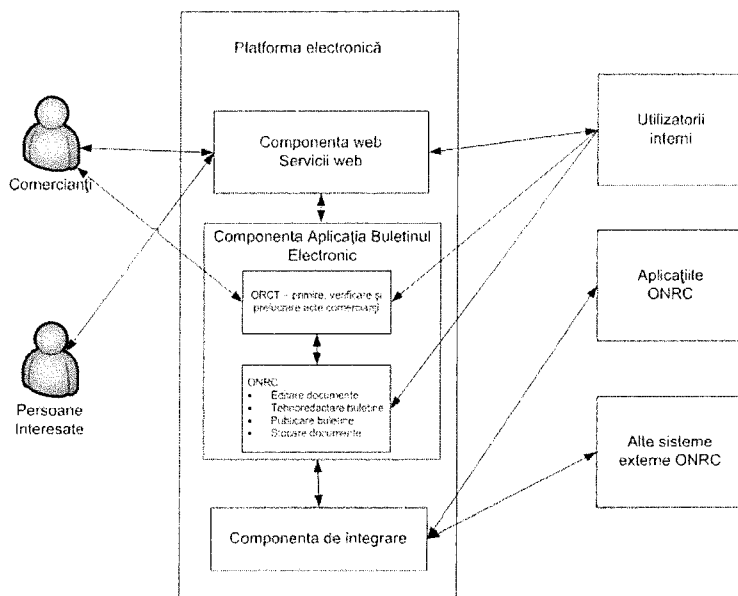
Proiect cofinanțat din Fondul Social European prin
Programul Operațional Capacitate Administrativă 2014-2020!



Handwritten signatures and marks at the bottom of the page.

- Modul web integrat pentru Buletinul Registrului Comerțului, care se integrează în/cu portalul existent pentru oferirea de servicii adiționale online pentru utilizatori cetățeni, mediul de afaceri și administrația publică;
- Un modul software care să permită cu ușurință și profesional prelucrarea și publicarea de informații de interes, cu posibilitate de manipulare, editare și adăugare de conținut în timp real cu capacități de colaborare maritate cu restul funcțiilor din cadrul organizației cu posibilități de afișare automată a proceselor interne;
- O aplicație inovativă pentru echipamente mobile și instrumente de dezvoltare aplicații mobile pentru consolidarea sistemului registrului comerțului. ONRC își propune să furnizeze în premieră servicii de m-governance (soluții care să permită accesul facil și sigur la informație de pe dispozitive mobile, care au o pondere din ce în ce mai importantă în modalitățile identificate de acces al portalului nostru) prin dezvoltarea și integrarea unei aplicații pentru modulul web pentru echipamente mobile pentru oferirea de servicii online, scopul fiind diversificarea și facilitarea metodelor de accesare a resurselor și serviciile ONRC, aducând beneficii pentru utilizatori cetățeni, mediul de afaceri și administrația publică

În continuare este prezentată diagramă arhitecturală de ansamblu ce descrie interacțiunea dintre entitățile implicate.



Figură 7 Descrierea generală a arhitecturii a BEREC

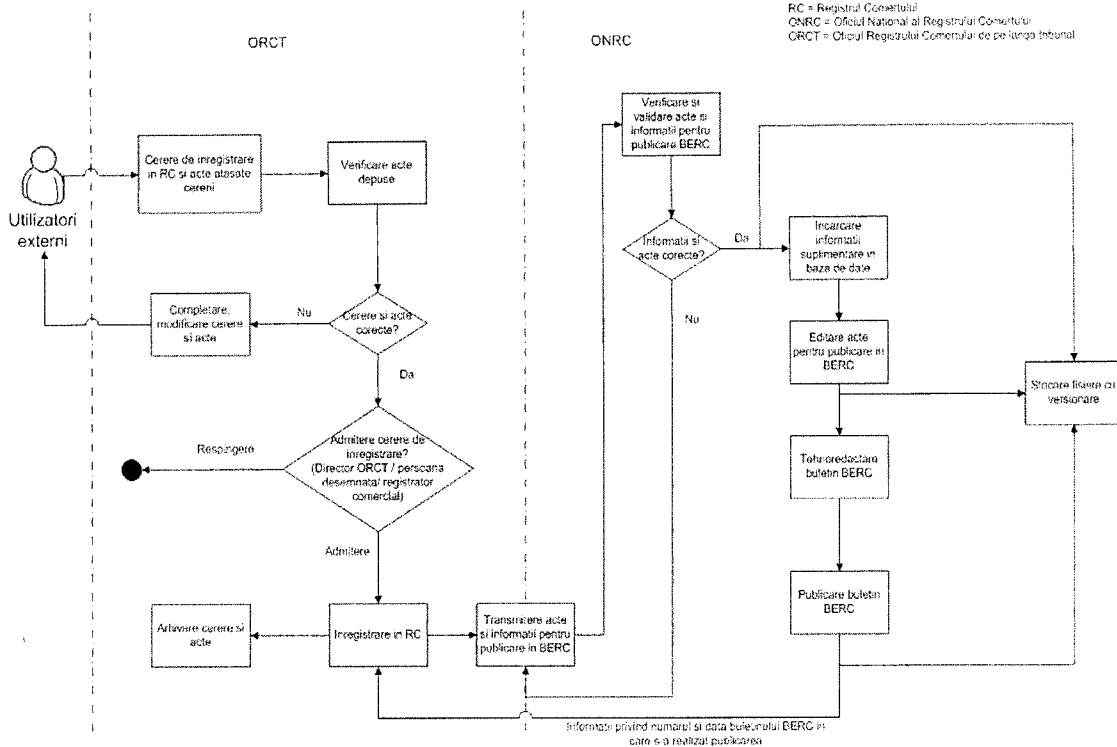
Din punct de vedere procedural, vor exista două nivele de organizare a procesării datelor specifice BEREC:

- nivelul local reprezentat de structurile teritoriale ale ONRC și anume: ORCT (42 locații) și birourile teritoriale ale ORCT; acestea vor prelua actele profesioniștilor și vor proceda la verificarea și pregătirea acestor acte, concomitent cu realizarea înregistrărilor și mențiunilor în registrul comerțului;
- nivelul central reprezentat de ONRC – unde se vor centraliza toate actele profesioniștilor primite de la ORCT-uri, se vor verifica și valida pentru publicarea pe platforma centrală.

În Figură 8 este prezentată schema generală a fluxului de publicare în Buletinul Electronic al Registrului Comerțului.

Pentru atingerea scopului implementării acestui subsistem, realizarea publicității actelor persoanelor supuse obligației de înregistrare în registrul comerțului prin publicarea electronică într-o manieră rapidă și eficientă, este necesar să se țină cont de următoarele aspecte:

- Vor fi reutilizate la maximum, anumite subsisteme/aplicații informatice din cadrul sistemului informatic actual al ONRC prin tehnologii de tip SOA;
- Se vor reutiliza elementele de bună practică și experiența acumulată în implementarea, dezvoltarea și exploatarea Buletinului Procedurilor de Insolvență;
- va permite integrarea sa în cadrul Portalului ONRC prin conceperea sa modulară și prin folosirea serviciilor web și de integrare;
- Întreaga soluție va permite susținerea de servicii online prin furnizarea de informații orientate către clienții persoane fizice sau juridice, publicului larg;
- Componentele soluției, permit extinderea continuă a serviciilor online găzduite de platformă;
- Întreaga soluție obținută să fie în concordanță cu obiectivele generale și specifice stabilite în cadrul proiectului.



Figură 8 Schema generală flux de publicare Buletinul Electronic al Registrului Comerțului

Subsistemul pentru editarea și publicarea Buletinului Electronic al Registrului Comerțului va conține cel puțin următoarele componente funcționale ce vor fi dezvoltate customizat în cadrul acestui proiect:

- Consultare Online a Buletinului Electronic al Registrului Comerțului (COBERC) ce conține 2 module
 - Modulul Portal – interfața web ce va permite accesul persoanelor interesate la Buletinul Electronic al Registrului Comerțului și la informații din bazele de date aferente acestuia din cadrul portalului ONRC;
 - Modulul Mobil – aplicație ce va permite accesul persoanelor interesate la Buletinul Electronic al Registrului Comerțului și la informații din bazele de date aferente acestuia de pe dispozitive mobile;
- Colectare și Elaborare Buletin Electronic al Registrului Comerțului (CEBERC) – interfața ce permite angajaților ONRC să gestioneze procesul de editare, elaborare și publicare a Buletinului Electronic al Registrului Comerțului;
- Integrare (CIBERC) cu aplicațiile registrului comerțului în primul rând, dar și cu alte sisteme interne și externe ONRC;

În continuare vor fi prezentate cerințele funcționale ale fiecărei secțiuni a platformei electronice. De asemenea vor fi enumerate și modul de interacțiune al platformei cu restul componentelor sistemului informatic integrat al Oficiului Național al Registrului Comerțului

Consultare Online a Buletinului Electronic al Registrului Comerțului

Această componenta reprezintă punctul de interacțiune central al subsistemului cu utilizatorii externi, și anume prin intermediul portalului și a aplicației mobile.

Componenta COBERC va fi instrumentul modern care va asigura legătura directă între instituție și publicul larg. Trebuie subliniat faptul că această componentă trebuie gândită și concepută în așa fel încât să permită integrarea facilă în cadrul portalului Oficiului Național al Registrului Comerțului.

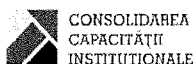
De asemenea această componentă devine principalul instrument de furnizare a serviciilor online asociate realizării publicității actelor comercianților. Privit ca întreg, această componentă va răspunde următoarelor cerințe funcționale și nefuncționale grupate pe diverse categorii:

Interfața grafică

- interfața grafică va fi intuitivă, ușor de utilizat, iar navigarea, rapidă și simplă;
- toate informațiile vor fi prezentate implicit în limba română, însă soluția trebuie să conțină toate elementele de internaționalizare necesare astfel încât să permită extinderea prezentării și la alte limbi de circulație internațională;
- din punct de vedere tehnic / tehnologic această interfață va respecta standardele actuale în domeniu (css, xhtml etc.); respectarea acestor standarde permite extinderea/ modificarea ușoară a acestei interfețe;
- nu va impune utilizarea unui anumit tip de browser de internet.

Securitate

- accesul la serviciile online va fi securizat, fără a exista posibilitatea de a fi accesate în absența autentificării prin metode clasice (nume utilizator, parola, certificate digitale).
- Sa implementeze mecanismele informatice pentru principiile prevazute in cadrul GDPR
 - Principiul legalitatii, corectitudinii și transparenței
 - Principiul limitării scopului
 - Principiul colectării minimului de date pentru atingerea scopului pentru care s-a obținut consimțământul



Proiect cofinanțat din Fondul Social European prin
Programul Operațional Capacitate Administrativă 2014-2020!



www.poca.ro

- Principiul mentinerii datelor actualizate
- Principiul stocării datelor strict pe perioada pentru care s-a obținut consimțământul
- Principiu asigurării securității adecvate datelor astfel încât acestea să fie integre, confidentiale și disponibile
- Principiu responsabilității

Arhitectura componentei

- din punct de vedere arhitectural, întreaga soluție, implicit și componenta web, este construită pe o arhitectură deschisă; pot fi adăugate noi funcționalități sau modificate funcționalitățile existente;
- va permite accesul celorlalte componente ale soluției;
- informațiile vor fi expuse către sisteme externe platformei, prin intermediul serviciilor web; accesul la aceste servicii web făcându-se controlat și securizat.

Administrare

- administrarea portalului web va fi făcută de către administratorii întregului sistem;
- vor fi utilizate politici de securitate pentru administrarea: utilizatorilor, grupurilor/roluri, servicii.

Secțiunea publică – COBERC- funcționalități

- acces la secțiunea publică a publicației Buletinul Electronic al Registrului Comerțului și informații din bazele de date aferente. Aceasta include sumarul buletinelor electronice publicate;
- prezentarea serviciilor platformei electronice;
- furnizarea de informații de interes public.

Secțiunea privată – COBERC- funcționalități

- acces la publicații de tip Buletinul Electronic al Registrului Comerțului și informații din bazele de date aferente;
- plata on-line pentru serviciile de furnizare a publicației și de informații;
- Formulare on-line (web-based) pentru transmiterea actelor persoanelor supuse obligației de înregistrare în registrul comerțului spre publicare în Buletinul Electronic al Registrului Comerțului;
- Statistici și rapoarte.

Serviciile on-line oferite prin intermediul platformei electronice

Prin intermediul platformei electronice vor fi oferite următoarele servicii on-line:

- Buletinul Electronic al Registrului Comerțului (în format PDF);
- Sumarul buletinelor electronice publicate;
- Actele și documentele publicate pentru fiecare persoană supusă obligației de înregistrare în registrul comerțului;
- Plata on-line pentru serviciile de furnizare a publicației și de informații;
- Statistici și rapoarte.

Colectare si Elaborare Buletin Electronic al Registrul Comerțului (CEBERC)

Așa cum s-a menționat, componenta de consultare a platformei electronice va reprezenta principalul instrument de realizare a publicității legale pentru actele persoanelor supuse obligației de înregistrare în registrul comerțului. Logica de business a platformei electronice va fi asigurată însă de componenta de CEBERC. Aceasta va fi răspunzătoare, în mod transparent pentru utilizatorii externi, de toate detaliile legate de primirea, verificarea și gestionarea actelor persoanelor supuse obligației de înregistrare în registrul comerțului, precum și de tehnoredactarea buletinelor propriu zise.

Cerințele la care va răspunde componenta CEBERC, sunt strâns legate de scopul platformei, de a publica actele persoanelor supuse obligației de înregistrare în registrul comerțului prin intermediul componentei COBERC.

Aplicația va răspunde la următoarele cerințe funcționale:

1. trebuie să permită tehnoredactarea buletinelor electronice;
2. trebuie să permită selectarea unor documente și a informațiilor aferente acestora pentru a fi grupate în vederea realizării unui buletin pentru publicare;
3. trebuie să permită semnarea electronică a documentelor și a buletinului electronic, utilizând certificate digitale calificate și certificate digitale interne (emise prin intermediul sistemului PKI implementat la ONRC în cadrul proiectului „Servicii on-line (de e-guvernare) oferite de ONRC pentru comunitatea de afaceri prin intermediul unui portal dedicat”); aplicația va trebui să permită atât semnarea unui document cât și a unui set de documente stocate în unul sau mai multe foldere;
4. trebuie să permită preluarea documentelor ce urmează a fi publicate în buletinul electronic precum și a informațiilor legate de un operator economic din aplicațiile existente ale registrului comerțului;
5. trebuie să permită atașarea documentului editabil și a documentului scanat corespunzător actului operatorului economic care se dorește a fi publicat;

6. trebuie să permită completarea și înregistrarea în baza de date a informațiilor legate de actul operatorului economic care se dorește a fi publicat (care constituie metadescrptorii atașați actelor comercianților);
7. trebuie să permită arhivarea electronică a buletinelor electronice și a actelor publicate;
8. trebuie să fie capabilă să regăsească informațiile legate de actele publicate în buletinul electronic pentru un anumit operator economic;
9. trebuie să fie capabilă să regăsească informațiile legate de un anumit tip de act al operatorilor economici ce face obiectul publicării în BEREC;
10. trebuie să fie capabilă să regăsească informațiile legate de un anumit buletin publicat;
11. trebuie să fie capabilă să gestioneze fluxuri de documente;
12. trebuie să fie capabilă să semnaleze anumite situații predefinite utilizatorilor (de stare inconsistentă, situații speciale, etc);
13. trebuie să permită realizarea unor căutări bazate pe atribute specifice;
14. trebuie să permită stabilirea unor nivele de auditare a operațiunilor efectuate pentru fiecare act al profesioniștilor primit spre publicare;
15. trebuie să permită într-un mod facil și flexibil colectarea informațiilor în vederea furnizării de informații;
16. trebuie să permită realizarea unui istoric al actelor publicate în Buletinul electronic pentru un anumit profesionist;
17. trebuie să permită interconectarea cu aplicațiile necesare din cadrul sistemului informatic integrat al ONRC în vederea atingerii scopului propus, aplicații care vor fi identificate în cursul fazei de analiză;
18. trebuie să permită integrarea cu Portalul ONRC implementat în cadrul proiectului „Servicii on-line (de e-guvernare) oferite de ONRC pentru comunitatea de afaceri prin intermediul unui portal dedicat”;
19. trebuie să permită interconectarea facilă cu alte sisteme informatice, prin utilizarea modularizării și a serviciilor;
20. trebuie să permită realizarea unor rapoarte operaționale și analitice, pe baza informațiilor stocate în bazele de date aferente publicării buletinului electronic.

Principalele rapoarte furnizate vor fi următoarele:

- istoricul actelor publicate pentru un anumit profesionist;
- istoricul acțiunilor efectuate de un utilizator;
- sumarul actelor publicate într-un buletin;
- lista actelor publicate într-un buletin;
- raport statistic cu privire la volumul și tipurile de acte publicate în buletinul electronic într-o anumită perioadă de timp;
- rapoarte cu privire la volumul de acte procesat de utilizatorii interni și la volumul de buletine publicate;
- raport cu privire la volumul de informații furnizat în anumite perioade;
- raport cu privire la numărul abonaților și cu perioadele de abonare.

Integrare (CIBERC)

Componenta de integrare a Buletinului Electronic a Registrului Comerțului va răspunde următoarelor cerințe funcționale:

- Va permite schimbul bidirecțional între subsistemul BERC și aplicațiile registrului comerțului;
- Va permite schimbul bidirecțional între Sistemul de Arhivare Electronică (SAE) și subsistemul BERC;
- Va permite interconectarea și integrarea cu sistemul ERP al ONRC;
- Va permite integrarea cu sistemul electronic de plăți al ONRC;
- Va permite interconectarea cu alte sisteme externe ONRC.

Interconectarea cu sistemele existente interne și externe ONRC

Sistem de arhivare electronică (SAE)

Acest sistem existent în cadrul ONRC va prelua și va arhiva actele primite de la profesionist spre publicare în Buletinul Electronic al Registrului Comerțului. Totodată, va arhiva buletinele electronice elaborate și publicate împreună cu datele relevante aferente procesului de elaborare. Operațiunea de arhivare a actelor primite pentru publicare în buletinul electronic se va efectua în etapa de procesare și verificare de la nivelul fiecărui ORCT, odată cu înmatriculările și mențiunile efectuate în registrul comerțului.

Integrarea cu aplicațiile existente

În momentul în care subsistemul BERC va fi funcțional, va trebui să se integreze cu alte module din cadrul fiecărui ORCT și la nivel de ONRC (registrul comerțului local computerizat, registrul comerțului central computerizat, registratură, taxe etc.).

Pentru a avea acces la datele de identificare ale profesioniștilor (persoanelor supuse obligației de înregistrare în registrul comerțului), integrarea cu aplicațiile de registru devine imperioasă. De asemenea, un capitol important și definitoriu al integrării în interiorul ONRC este integrarea cu modulele de plată electronică și cu modulele financiar – contabile existente.

Integrarea cu Portalul ONRC

Subsistemul BERC trebuie să permită integrarea cu Portalul ONRC. Aceasta s-ar putea să impună unele restricții legate de interfață, componenta web a platformei electronice trebuind să țină cont

de specificațiile portalului în ceea ce privește interfața, pentru a asigura utilizatorului un aspect vizual și funcțional, unitar și coerent.

Interconectarea cu alte sisteme externe ONRC

Subsistemul BERC trebuie să permită interconectarea facilă cu alte sisteme externe ONRC prin folosirea serviciilor web. O astfel de abordare, va permite interconectarea cu alte sisteme – atât interne ONRC cât și externe – datorită modului flexibil de utilizare a datelor și informațiilor din Buletinul Electronic al Registrului Comerțului. De asemenea, această abordare va permite reutilizarea serviciilor pentru cât mai mulți utilizatori.

4.2.2 Subsistemul Colaborativ

Subsistemul Colaborativ trebuie să respecte următoarele cerințe funcționale:

- Sa asigure gestiunea a cel puțin 2 tipuri de proiecte (de ex. proiecte interne de dezvoltare software, proiecte de implementare contracte financiare) cu posibilitatea ulterioară implementării de a gestiona și alte tipuri;
- Sa asigure implementarea a mediului colaborativ de tip Q&A pentru cel puțin 3 comunități interne de specialiști (de ex. referenți registratori, specialiști IT, specialiști arhiva) și să permită unui administrator definirea și configurarea de alte comunități similare. Fluxurile de procesare vor fi implementate pe baza rezultatelor etapei de analiză
- Sa asigure efectuarea deployment-urilor de release-uri ale aplicațiilor dezvoltate în proiect într-un mod integrat cu aplicarea testelor unitare, de integrare și de performanță pe mediul de pre-productie și apoi pe mediul productiv
- Sa includă pentru aplicațiile dezvoltate în cadrul proiectului teste automate (unit tests cel puțin pentru 60% din componentele principale, teste de integrare cel puțin pentru 80% din integrări și teste funcționale pentru cel puțin 20% din scenariile de testare de acceptanță)
- Sa asigure accesul utilizatorilor prin integrarea cu sistemul de gestiunea a identității existent în SII al ONRC

4.2.3 Sub sisteme de monitorizare a performanțelor și asigurarea securității SII al ONRC

Din perspectiva monitorizării Sistemului Informatic Integrat, subsistemul de monitorizare trebuie să respecte următoarele cerințe funcționale:

- Sa asigure monitorizarea performanței rețelei interne a ONRC (la nivel central) în ansamblu, evidențiind interdependențele între aplicații și activele de rețea (servere, instanțe de baze de date) și oferind suport în regim automatizat pentru diagnoza și remediere a blocajelor și/sau penalităților de performanță;
- Sa ofere suport pro-activ din punct de vedere a stringențelor necesare maximizării performanței rețelei pentru dezvoltarea/configurarea aplicațiilor ONRC (la nivel central) pe întregul ciclu de viață al acestora;

- Sa asigure monitorizarea experientei utilizatorilor ONRC (la nivel central) pentru zona de aplicatii web-based si/sau mobile;
- Sa asigure suportul pentru analiza aprofundata si corelata a traficului de retea pentru corelarea nivelului de performanta al aplicatiilor cu aspectele ce tin de securitate cibernetica in cadrul retelei.

Din perspectiva asigurarii securitatii Sistemului Informatic Integrat, subsistemele specializate in asigurarea securitatii trebuie sa respecte urmatoarele cerinte functionale:

- Sa asigure capabilitatile de analiza si testare de securitate a sistemului informatic (ce se va dezvolta in scopul proiectului) coroborate cu capabilitatile de mitigare/remediere a vulnerabilitatilor de securitate evidentiate;
- Sa asigure capabilitatile de protectie a aplicatiilor din cadrul sistemului informatic cat si de redistributie a accesului utilizatorilor catre acestea in scopul maximizarii performantelor serviciilor ONRC;
- Sa asigure capabilitati avansate de protectie antimalware cat si capabilitati avansate de protectie a resurselor la nivelul posturilor de lucru pentru utilizatorii sistemului informatic;
- Sa asigure capabilitati de analiza a accesarii si utilizarii resurselor pentru prevenirea situatiilor de acces si/sau scurgere de informatii neautorizate in/din cadrul sistemului informatic;
- Sa asigure capabilitatile necesare pentru managementul datelor de audit pentru asigurarea unei vizibilitati complete la nivelul infrastructurii aferente sistemului informatic.

4.3 Arhitectura generala a sistemului

Arhitectura aleasă de ONRC, ce trebuie respectată de ofertanți, îndeplinește principiile fundamentale ce stau la baza serviciilor publice, așa cum sunt acestea menționate în Cadru Național de Interoperabilitate. Ofertanții trebuie să aibă în vedere aceste principii atât în oferta depusă cât și în implementarea soluției.

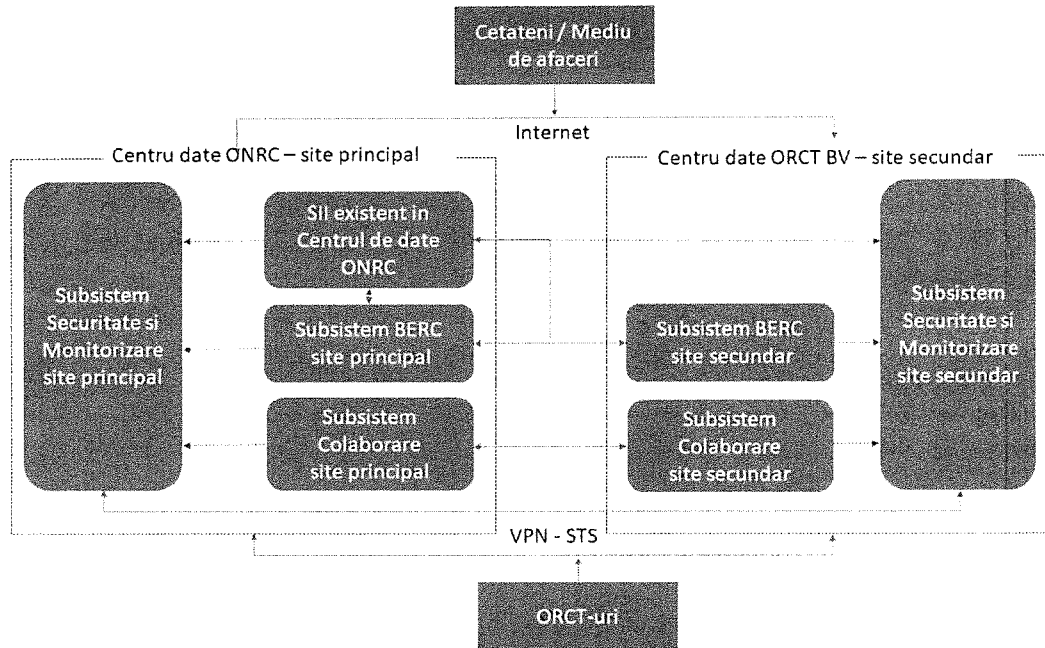
Arhitectura presupune instalarea componentelor soluției în doua centre de date ale ONRC.

Subsistemele BERC si colaborare din cele 2 centre de date trebuie sa fie geo-redundante asigurand astfel inalta disponibilitate nu numai la nivelul unui centru de date ci si in cazul in care centrul principal devine indisponibil.

Subsistemul de securitate si monitorizare trebuie sa acopere atat subsistemele BERC si Colaborare cat si infrastructura hardware/software a SII din centrul de date principal.

ONRC va asigura comunicatia intre cele 2 centre de date.

Cetatenii / Mediul de afaceri vor putea accesa doar componenta online a subsistemului BERC iar angajatii ONRC/ORCT vor avea acces atat la subsistemul BERC cat si la subsistemul Colaborare conform drepturilor de acces asigurate.



Figură 9 Arhitectura generala a sistemului

Scalabilitate, disponibilitate si continuitate

Pentru a asigura o disponibilitate sporită, s-a ales soluția tehnică centralizată și gruparea în cluster atât a serverelor utilizate pentru publicarea web, autentificare, control acces, integrare, bază de date, aplicații cât și a platformelor de colaborare, securitate și monitorizare. Soluția asigură în mod implicit și transparent pentru utilizatorul web (web client), funcția de distribuție a cererilor (load-balancing), permițând totodată o distribuție optimă a solicitărilor către resursele disponibile (cluster activ-activ prin intermediul unui echipament hardware de load-balancing).

Totodată, pentru asigurarea continuității funcționării în caz de dezastru sistemul va fi distribuit în 2 centre de date (centru primar și centru secundar)

În vederea asigurării scalabilității și disponibilității, soluția va respecta următoarele cerințe:

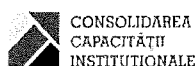
- Să suporte mecanisme de tip clustering (topologie activ-activ și activ-pasiv) la nivelul fiecărui centru de date;
- Să implementeze mecanisme de "disponibilitate ridicată (24/7)" a platformei și aplicațiilor pentru execuția continuă a serviciilor instalate;
- Să implementeze mecanisme de replicare a obiectelor aplicației între serverele aceluiași cluster și între cele 2 centre de date (primar și secundar);
- Să permită ca, în cazul unei întreruperi a funcționării unuia dintre noduri, cererile utilizatorilor să fie preluate automat (și în mod transparent pentru utilizator) de către celălalt nod din cluster;
- Să permită ca, în cazul unei întreruperi a funcționării unui centru de date (de exemplu indisponibilitate acces în internet), cererile utilizatorilor să fie preluate automat (cu impact minim pentru utilizator – la nivelul subsistemelor BERC și Colaborativ) de către centrul de date secundar;
- Să asigure utilizatorii și administratorii sistemului informatic în cazul oricărei defectiuni hardware și/sau software, prin eliminarea totală a punctelor de „single point of failure” din arhitectura sistemului, și, implicit, implementarea mecanismelor de clusterizare/balansare la nivel hardware și software;
- Să permită stoparea temporară a unui nod pentru mentenanță și suport, sistemul în acest timp fiind disponibil pentru activități normale, prin implementarea mecanismelor de cluster;
- Să asigure securitate tranzacțională în cazul apariției unor erori hardware sau software în cluster;
- Să permită reconectarea automată la nodul sau nodurile rămase disponibile după apariția unei defectiuni;
- Să permită upgrade-ul nodurilor existente și adăugarea de noi noduri, dependent de încărcarea sistemului, numărului de utilizatori, numărului de accesări și de complexitatea aplicațiilor;
- Să asigure disponibilitate permanentă 24x7, a serviciilor oferite.

Prestatorul va propune soluția tehnică având în vedere asigurarea continuității și recuperarea în caz de dezastru. Procedurile operaționale furnizate de Prestator vor fi incluse de Beneficiar în planul integrat al ONRC de asigurarea a continuității și recuperare în caz de dezastru.

Fiabilitate și stabilitate

Prin utilizarea unor tehnici avansate de cluster, soluția propusă asigură un nivel relativ ridicat de disponibilitate (availability) și fiabilitate (reliability). Utilizarea tehnicilor avansate de cluster asigură, pe lângă un nivel crescut de scalabilitate și o bună distribuție a cererilor (load balancing), precum și un nivel ridicat de fiabilitate prin creșterea nivelului de toleranță la erori.

În vederea creșterii fiabilității și stabilității soluției, trebuie utilizat un mediu de administrare și monitorizare centrală a aplicațiilor și a bazelor de date. Acest mediu va trebui să respecte următoarele cerințe:



Proiect cofinanțat din Fondul Social European prin
Programul Operațional Capacitate Administrativă 2014-2020!



- Monitorizarea integrată a elementelor de infrastructură legate de rețea, sisteme, aplicații eterogene - Sisteme de operare și aplicațiile Proiectului - din punct de vedere al performanțelor, la nivel de Data Center;
- Măsurarea și colectarea datelor de performanță într-o bază de date pentru analiză și raportare ulterioară;
- Diagnosticarea problemelor ce apar în cadrul soluției;
- Administrare web-based cu capabilități de monitorizare configurabile;
- Posibilitatea de a seta praguri pentru avertizări și alerte critice;
- Alertare via e-mail la evenimente pe o ierarhie de priorități configurabilă;
- Posibilitatea de a oferi grafice de performanță în timp real;
- Posibilitatea de a securiza comunicația între diferite componente ale soluției. Componentele subsistemului de monitorizare/securitate vor comunica intern doar securizat;
- Administrarea arhitecturilor de tip cluster;
- Posibilitatea de a defini mai mulți administratori / utilizatori cu roluri diferite;
- Posibilitatea configurării sistemului de management astfel încât să execute acțiuni corective automate (fără intervenția administratorilor) în cazul detectării de erori sau în cazul degradării performanțelor;
- Existența unor instrumente pentru realizarea operațiilor de backup și recovery pentru baza de date, pentru aplicații, cât și pentru adăugarea de noi noduri în arhitectura de cluster;
- Includerea mecanismelor/sub-componentelor de optimizare a performanțelor componentelor sistemului cu sugerarea operațiunilor ce trebuie efectuate si/sau investigate de către personalul tehnic în acest sens.

Agenții pentru fiecare componentă de infrastructură urmărită nu trebuie să interfereze cu operațiile normale ale componentei respective pentru a nu afecta performanțele acesteia

Extensibilitate

Arhitectura soluției este una deschisă orientată pe servicii (Service Oriented Architecture). Funcționalitățile modulelor vor fi oferite prin intermediul unui set bine definit de servicii, acest lucru favorizând reutilizarea componentelor și asigurând o bună integrare și interoperabilitate cu sistemele externe.

Soluția va fi pregătită pentru eventuale îmbunătățiri și extinderi realizate prin integrarea unor noi module în baza protocoalelor standard de comunicație și prin API (Application Programming Interface), la nivelul aplicațiilor customizate. În mod analog, subsistemul de monitorizare a performanțelor și asigurarea securității trebuie să fie scalabil/extensibil.

Utilizarea serviciilor web (web Services) asigură o interoperabilitate ridicată a soluției, permițând colaborarea cu aplicații bazate și pe platforme heterogene.

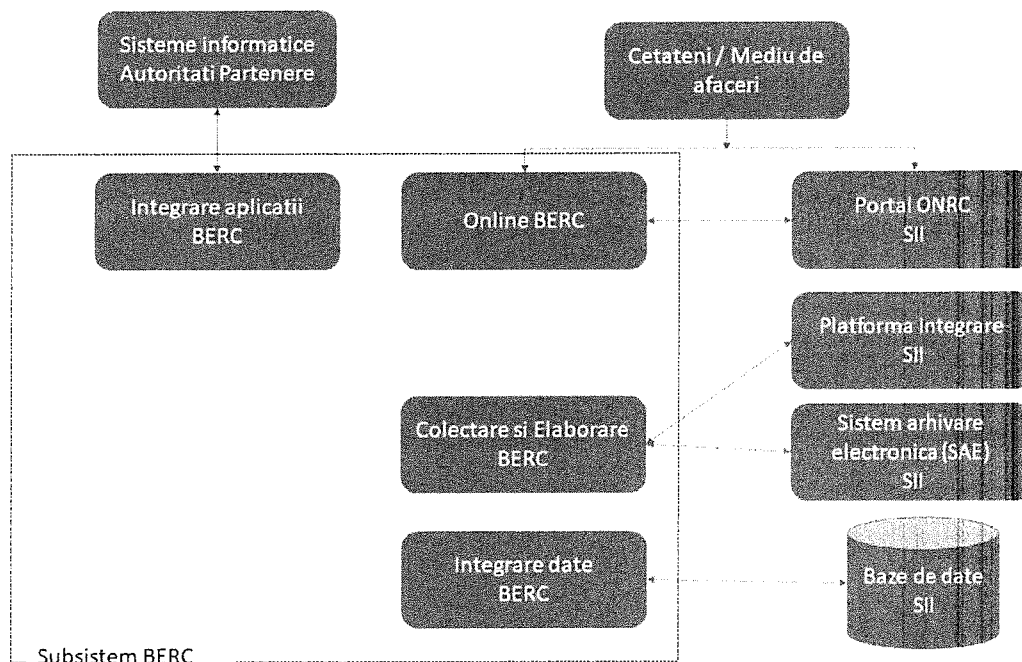
În vederea asigurării extensibilității, soluția va trebui să respecte următoarele cerințe:

- Soluția va avea o arhitectură deschisă bazată pe standarde;
- Soluția va oferi integrarea cu sisteme existente utilizând tehnologii moderne, de tip SOA;
- Soluția trebuie să aibă la bază standarde în domeniu, ca de exemplu: Java 2 Enterprise Edition (J2EE), XML, suport pentru servicii web;
- Soluția va fi flexibilă din punct de vedere al clienților de tip browser, al sistemelor de operare și al suportului pentru bazele de date;
- Soluția va oferi posibilitatea utilizării serviciilor web pentru a expune date și servicii către sistemele externe platformei.

4.3.1 Nivelul funcțional de aplicație

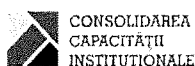
4.3.1.1 Subsistemul Buletinul Electronic a Registrului Comertului

Descrierea logică a interacțiunilor dintre componentele subsistemului BEREC este descrisă în Figură 10.



Figură 10 Arhitectura logică subsistem BEREC

Componenta funcțională de consultare online a BEREC se va integra cu actualul portal al ONRC



Proiect cofinanțat din Fondul Social European prin
Programul Operațional Capacitate Administrativă 2014-2020!



Handwritten signatures and marks at the bottom of the page.

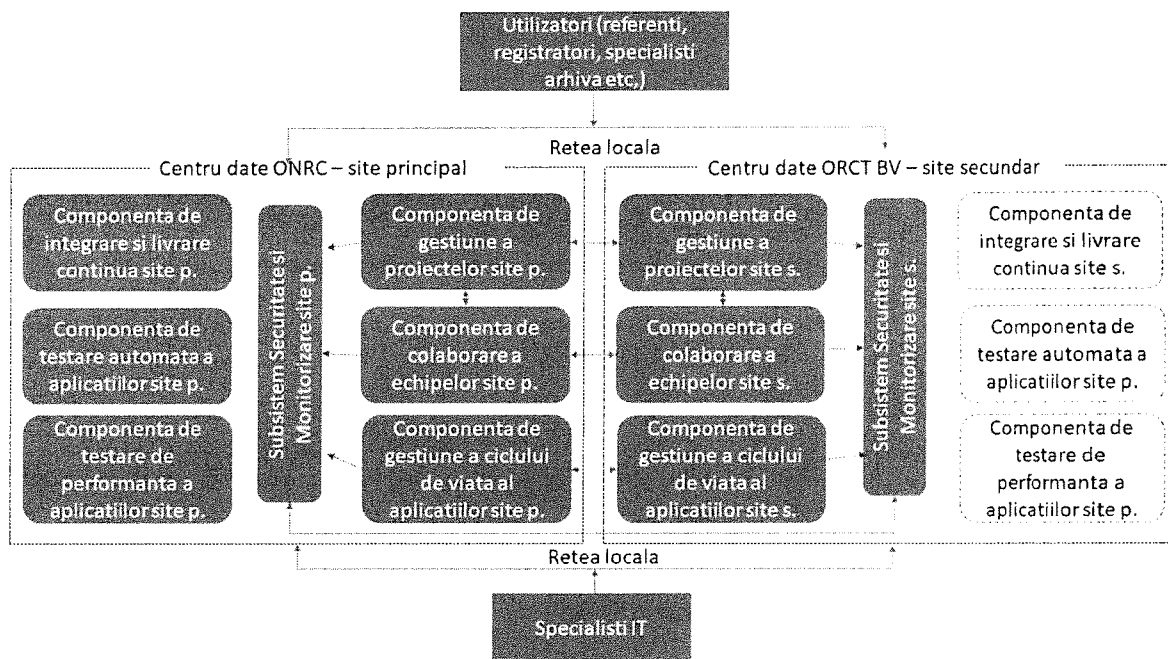
asigurand astfel autentificarea unica a utilizatorilor de portal in vederea accesarii atat a functionalitatilor existente in Portalul ONRC cat si a celor care vor fi furnizate de componenta functionala de consultare online a BEREC.

Pentru integrarea cu aplicatiile existente din cadrul SII al ONRC componenta functionala de Colectare si Elaborare a BEREC va apela serviciile disponibile in cadrul platformei de integrare a SII (bazata pe Oracle Service Bus) prin intermediul careia sunt interconectate aplicatiile SII.

Pentru integrarea la nivel de date componenta de Integrare date a BEREC se va conecta direct bazele de date din cadrul SII.

4.3.1.2 Subsistemul Colaborativ

Descrierea logica a interactiunilor componentelor subsistemului Colaborativ este descrisa in Figură 11



Figură 11 Arhitectura logica Subsistem Colaborare

Asa cum se observa si din Figură 11 componentele functionale ce asigura gestiunea proiectelor, colaborarea echipelor si gestiunea ciclului de viata al aplicatiilor sunt prevazute a functiona georedundanta la nivelul aplicatiei iar componentele ce asigura testarea automata, testarea de performanta

și livrarea/integrarea continuă a aplicațiilor sunt prevăzute a funcționa în site-ul principal, geo-redundantă fiind asigurată la nivelul sistemului de virtualizare.

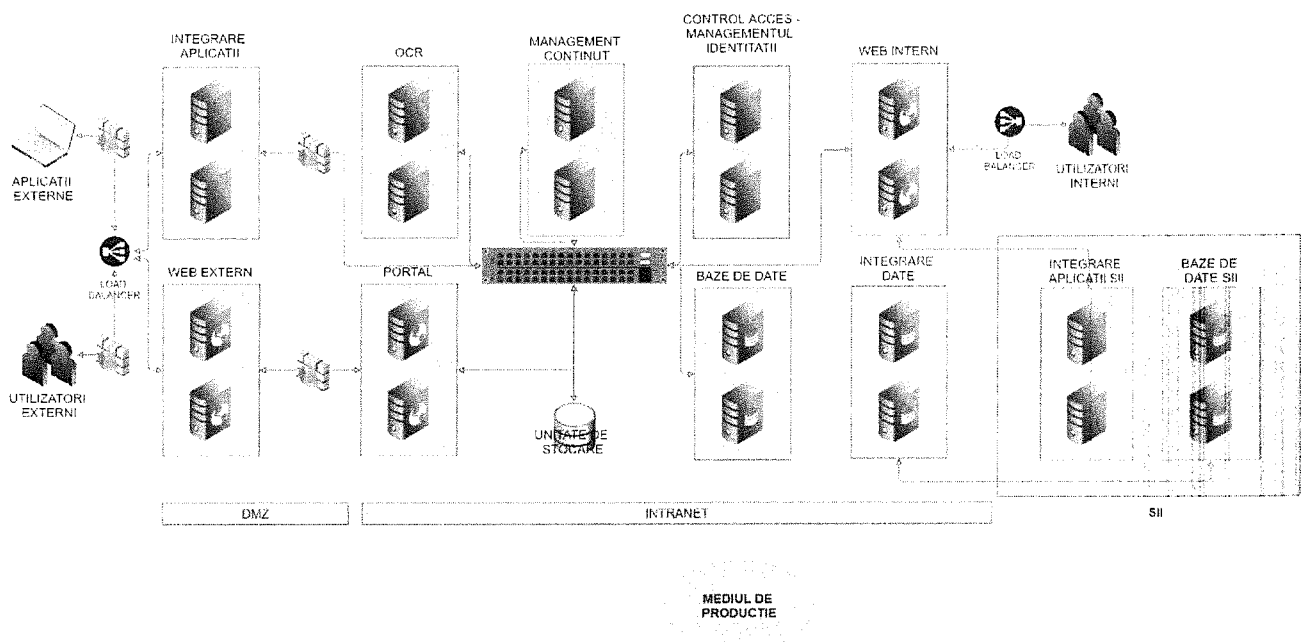
Componentele ce asigură testarea automată, testarea de performanță și livrarea/integrarea continuă a aplicațiilor vor fi configurate astfel încât să țargheze întregul mediu productiv al subsistemului BEREC / Colaborare atât în ceea ce privește testarea de performanță cât și instalarea de noi versiuni ale aplicațiilor customizate.

4.3.2 Nivelul tehnic de aplicație

4.3.2.1 Subsistemul Buletinul Electronic a Registrului Comerțului

Toate serviciile on-line vor fi accesibile prin intermediul componentei Portal și a aplicației mobile dedicate clienților externi.

Arhitectura logică propusă pentru mediul de producție al subsistemului BEREC este prezentată în figură de mai jos:



Figură 12 Arhitectura logică propusă subsistem BEREC

La nivel central sunt create structurile bazelor de date, inclusiv datele de gen nomenclatoare. La nivel central sunt instalate și vor funcționa toate componentele legate de securitatea platformei și aplicațiile interne. În plus, mediul va permite funcționarea componentei de integrare și interconectare cu aplicațiile ONRC precum și cu alte sisteme externe ONRC, dacă este cazul. De asemenea, la nivel central vor fi expuse informațiile către utilizatorii externi și persoanele interesate prin intermediul componentei Portal și a aplicației mobile.

În cadrul sub sistemului BERC se disting următoarele componente tehnice:

- Componenta Portal;
- Componenta server de aplicație;
- Componenta de integrare aplicații;
- Componenta de integrare a datelor;
- Componenta de gestiune a bazei de date;
- Componenta de procesare OCR;
- Componenta de gestiune conținut și documente;
- Componenta de dezvoltare a aplicațiilor mobile prin intermediul careia va fi dezvoltată și aplicația mobilă adresată utilizatorilor externi;

Funcționalitățile de asigurare securitate / monitorizare centralizată (inclusiv backup-restore) sunt furnizate de subsistemul de securitate și monitorizare prezentat în cadrul acestui document.

Accesul la serviciile on-line se va face prin intermediul componentei **server web extern**. Accesul la aplicațiile interne se va face prin accesarea componentei server web găzduit în intranetul ONRC (server web intern). Accesul la serviciile on-line, oferite prin intermediul componentei Portal a platformei, se va face prin intermediul unui cluster de servere web plasat în DMZ-ul ONRC (accesul se va face prin intermediul unei componente specializate hardware și/sau software cu funcționalități de load-balancing).

Componenta Server de Aplicații oferă contextul de rulare pentru componentele soluției: Portal, aplicațiile de editare și elaborare a buletinului, integrare.

Aplicațiile deservind utilizatorii - interni versus externi - vor fi găzduite după cum urmează:

- Utilizatorii interni vor accesa aplicațiile interne instalate pe infrastructura de server de aplicații și gestiune a conținutului.
- Utilizatorii externi vor accesa numai componenta Portal a platformei pentru a obține informații, a vizualiza conținutul buletinelor electronice publicate, pentru a folosi serviciile disponibile.

În această manieră, se va realiza o delimitare strictă a utilizatorilor pe echipamente distincte, care să permită o utilizare judicioasă a resurselor de calcul puse la dispoziție.



Serverul de aplicație destinat componentei Portal va găzdui toate serviciile on-line adresate utilizatorilor externi (din internet).

Aplicațiile interne care vor deservi cu informații buletinele electronice vor rula pe o infrastructură de server de aplicații dedicată. Aplicațiile interne vor fi construite pe baza cerințelor funcționale exprimate în acest document.

Pentru balansarea eficientă a cererilor utilizatorilor vor fi utilizate componente hardware și/sau software de dirijare a încărcării către resursele soluției desemnate să rezolve optim aceste cereri.

Bazele de date utilizate de modulele soluției sunt găzduite de componenta server baze de date, instalat într-un segment de rețea separat. Pentru subsistemul BERC va exista o singură bază de date la nivel central. Totodată, prin intermediul componentei de integrare date se va asigura schimbul de date cu bazele de date din cadrul SII existent al ONRC.

Componenta de integrare aplicații va asigura, în primul rând, atât interoperabilitatea aplicațiilor BERC cu sisteme informatice ale autoritatilor partenere. Aceasta componentă va fi instalată pe un cluster dedicat de servere de aplicații. Integrarea la nivel aplicativ cu SII existent al ONRC va fi realizată prin intermediul componentei existente de integrare din cadrul SII.

Componenta de gestiune a conținutului / documentelor va asigura gestiunea tuturor documentelor și versiunilor acestora pe perioada de la intrare/creare în ONRC până la arhivare.

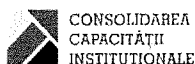
Componenta de procesare OCR va fi responsabilă cu transformarea în format editabil a documentelor din format imagine (PDF, TIFF, JPEG, etc) în vederea reducerii timpilor de editare a buletinului electronic.

Scenarii de utilizare

Utilizatorii interni ai ONRC

- Utilizatorul ONRC/ORCT accesează prin intermediul browser-ului aplicația web;
- Autentificarea și autorizarea utilizatorului este realizată de către serverul de control acces / SSO;
- În funcție de drepturile asociate profilului, utilizatorul poate accesa anumite secțiuni din aplicația web;
- La nivelul fiecărui ecran de lucru utilizatorul poate efectua operații de citire, scriere și ștergere.

Utilizatorii externi



Proiect cofinanțat din Fondul Social European prin
Programul Operațional Capacitate Administrativă 2014-2020!



- Utilizatorii externi ONRC, publicul larg, persoane fizice sau juridice, instituții guvernamentale, care vor accesa componenta on-line a BEREC;
- Autorizarea și accesul se fac pe baza unui cont de utilizator (nume utilizator și parolă); datorită arhitecturii folosite pentru autentificarea utilizatorilor pot fi utilizate și alte soluții (certIFICATE digitale).

4.3.2.2 Subsistemul Colaborativ

Pentru deservirea componentelor functionale evidentiate in cap. 4.2.2 Subsistemul Colaborativ, in cadrul subsistemului Colaborativ au fost incluse următoarele componente tehnice:

- Componenta de gestiune proiecte;
- Componenta de colaborare a echipelor;
- Componenta de gestiune a ciclului de viata al aplicatiilor;
- Componenta de integrare si livrare continua a modificarilor de aplicatii;
- Componenta de testare automata a aplicatiilor;
- Componenta de testare de performanta a aplicatiilor;

Componenta de colaborare a echipelor si cea pentru gestiunea proiectelor sunt destinate utilizarii angajatilor ONRC/ORCT care vor fi implicati in proiecte sau care fac parte din comunitatile de specialisti pentru care se va implementat un cadru de colaborare digitala.

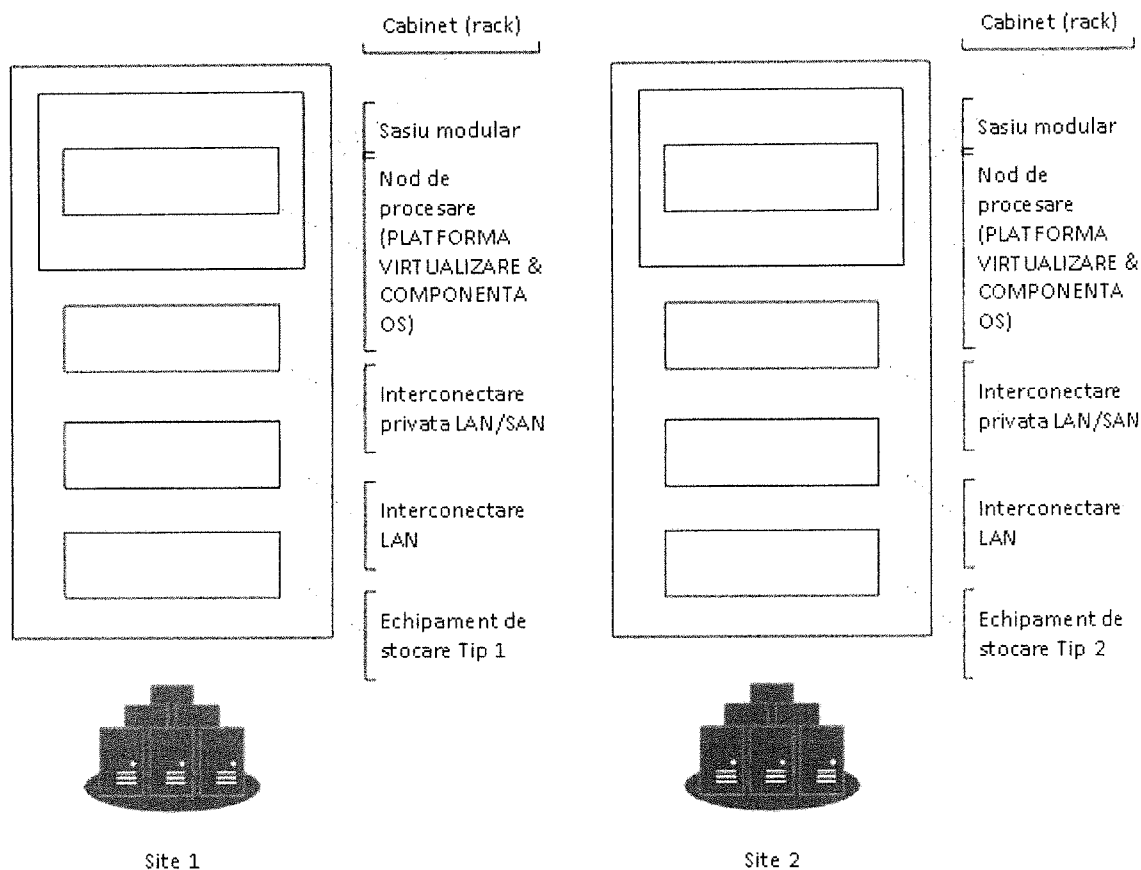
Celealte componente sunt destinate echipelor de specialisti IT pentru administrarea, intretinerea, mentenanta si testarea facila a aplicatiilor software personalizate.

4.3.3 Nivelul tehnic de infrastructura

4.3.3.1 Subsistem tehnic de procesare

Subsistemul tehnic de procesare, stocare si integrare a datelor se compune din:

- Echipamente de tip sasiu modular,
- Echipamente de interconectare private LAN/SAN,
- Echipamente de procesare generala,
- Componenta de virtualizare sistem,
- Componenta de sistem de operare,
- Echipamente de integrare LAN,
- Echipament de stocare de Tip 1,
- Echipament de stocare de Tip 1.

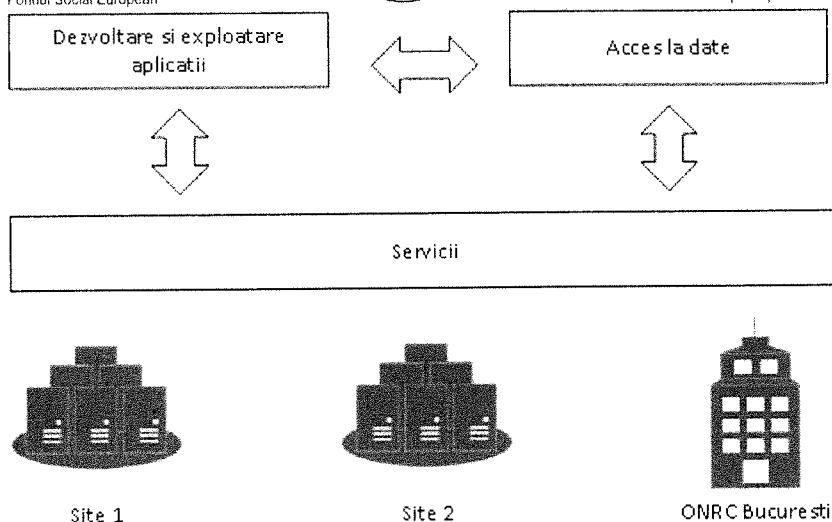


Figură 13 Schema de baza a subsistemului tehnic de procesare, stocare și integrare a datelor

4.3.3.2 Subsistem tehnic de monitorizare generală a datelor

Subsistemul tehnic de monitorizare generală a datelor se compune din:

- Componenta de monitorizare a dezvoltării și exploatării aplicațiilor,
- Componenta de monitorizare a accesului la date,
- Componenta de monitorizare a serviciilor.



Figură 14 Schema de baza a subsistemului tehnic de monitorizare generala a datelor

4.3.3.3 Subsistem tehnic de securitate si audit

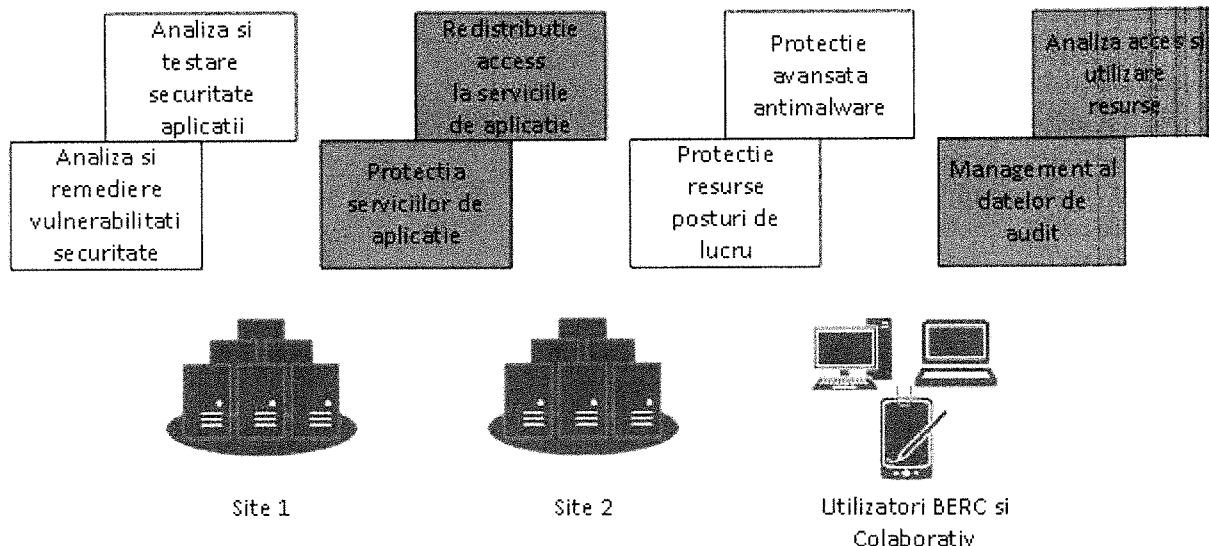
Subsistemul tehnic de securitate si audit se compune din:

- Componenta de analiza si testare de securitate a aplicatiilor,
- Componenta de analiza si remediere a vulnerabilitatilor de securitate,
- Componenta de analiza a accesarii si utilizarii resurselor,
- Componenta de redistributie la serviciile de aplicatie,
- Componenta de protectie a serviciilor de aplicatie,
- Componenta centrala de protective avansata antimalware,
- Componenta de protectie a resurselor la nivel de post de lucru,
- Componenta de management al datelor de audit.



[Handwritten signature]

[Handwritten signature]



Figură 15 Schema de baza a subsistemului tehnic de securitate si audit

4.3.4 Arhitectura n-tier

Din punct de vedere tehnic, componentele funcționale se vor sprijini pe anumite componente tehnice: server de aplicații, sistem de gestiune a bazelor de date, server web, platformă de integrare, etc.

În proiectarea, din punct de vedere tehnic, a sistemului informatic se pleacă de la următoarele premise, care constituie cerințe minimale obligatorii:

- interfața utilizatorului este browserul web – aplicația fiind web-based;
- arhitectura aplicației web trebuie să fie n-tier;
- componenta portal și serviciile on-line trebuie să fie disponibile tuturor categoriilor de utilizatori;

De asemenea, noul sistem va trebui să asigure interfațarea și interconectarea cu:

- Sistemul Informatic Integrat al ONRC;
- Sistemul de arhivare existent în tehnologie Captiva/IBM Content Manager și JAVA;
- Piațele on-line ONRC și modulele economico – financiare.

Aplicațiile software vor fi construite conform principiilor arhitecturii web multi-tier peste următoarele niveluri logice clar separate:

- **Prezentare**

Interfața cu utilizatorul va asigura un meniu cu opțiuni de servicii cu posibilitatea de navigare între opțiuni și sub-opțiuni. Interfața utilizator va fi intuitivă (facilă), informativă, fiabilă, atractivă și stabilă.

- **Business logic**

Modelul de business logic asigură transparența complexității acestuia față de utilizatori, fiind organizat conform următoarelor principii:

- Standardizare;
- Reutilizare;
- Separare clară între nivelul de prezentare și business logic;
- Orientare servicii.

Nivelul de business logic asigură tratarea tuturor regulilor de procesare incluzând fără a se limita la:

- Autentificare și autorizări de securitate;
- Managementul sesiunilor utilizatorilor;
- Reguli de integritate date;
- Reguli de orchestrare servicii;
- Reguli de validare intrări;
- Monitorizarea tranzacțiilor.

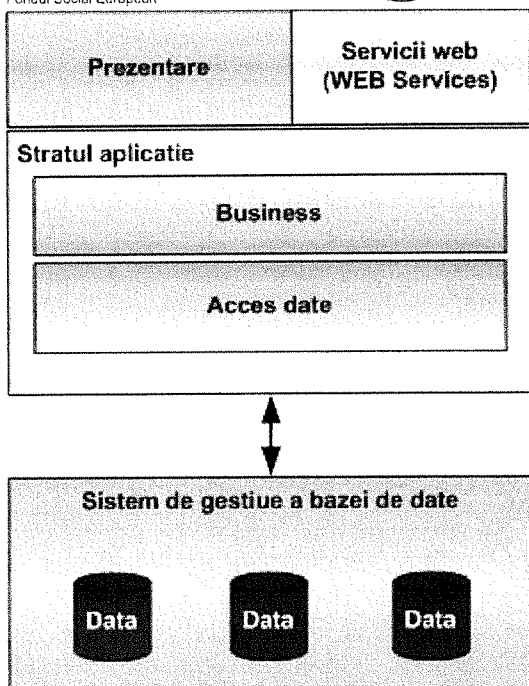
- **Informații și date**

Informația stocată în bazele de date și utilizată în cadrul aplicației prezintă următoarele particularități:

- volum mare de fișiere și documente colectate în vederea publicării împreună cu datele aferente;
- acuratețe ridicată, obținută prin verificarea surselor de intrare, cu raportarea eventualelor neconcordanțe;
- necesitatea de a suporta un proces de analiză complexă;
- diseminare internă.



Handwritten signatures and initials in blue ink.



Figură 16 Niveluri arhitecturale

4.4 Descrierea nivelului tehnic al sistemului

4.4.1 Caracteristici specifice ale subsistemelor tehnice

În elaborarea arhitecturii de sistem, respectiv a specificațiilor tehnice pentru fiecare echipament/categorie de echipamente s-au avut în vedere cerințele specifice pentru fiecare nivel de infrastructură coroborate cu cerințele și provocările de natură tehnică pentru fiecare tip de funcționalitate, astfel încât să se obțină un sistem scalabil ce va oferi totalitatea resurselor tehnice necesare (capacitate, performanță și disponibilitate), fără a impune vreo limitare de natură tehnică.

- Prin implementarea soluției preconizate se dorește obținerea unui set comun de obiective funcționale și operaționale, atât pentru fiecare element/platformă din infrastructură cât și pentru arhitectura globală a proiectului;
- Complexitate redusă a platformelor, în scopul integrării și extinderii cu ușurință, atât din punct de vedere operațional cât și funcțional;
- Complet redundanță la nivelul tuturor elementelor componente, în scopul protejării facile a datelor rezidente și efectuării transparente a operațiunilor de administrare, update, upgrade și înlocuire a componentelor ce se pot defecta;

- Mecanisme native de redundanta locala, integrate cu restul elementelor de infrastructura, pentru protectia continua si completa a aplicatiilor, proceselor si serviciilor deservite in eventualitatea unor defectiuni majore;
- Scalabila in mod transparent pentru aplicatiile, procesele si serviciile deservite, in scopul extinderii ulterioare a solutiei, indiferent de necesitatea scalarii – capacitate, conectivitate si performanta;
- Bazata pe componente standard, in scopul integrarii si extinderii facile a setului de aplicatii/procese/servicii si cerinte existente in infrastructura, precum si cu orice alte noi cerinte viitoare;
- Unelte de administrare integrate si facil de folosit, ce acopera intreaga functionalitate, independente de anumite elemente de infrastructura (sistem de operare, tehnologie de aplicatie, etc), in scopul reducerii eforturilor operationale si costurilor de integrare in infrastructura;
- Functionalitati integrate de securitate, integrate cu restul elementelor de infrastructura, in scopul securizarii complete a accesului si manipularii datelor de catre utilizatori, aplicatii si servicii;
- Mecanisme integrate de agregare a resurselor fizice din infrastructura (procesare, stocare, comunicatie), mecanisme integrate de analiza predictiva si aplicare proactiva de politici asupra resurselor in scopul obtinerii maximului de performanta si eficienta indiferent de aplicatiile si serviciile deservite de platforme, asigurand disponibilitate maxima, timpi de raspuns la incidente si costuri operationale minime;
- Platforme integrate nativ ce vor permite reducerea semnificativa a timpilor de nefunctionare a aplicatiilor si serviciilor, reducerea proceselor operationale, respectiv a timpilor de solutionare a incidentelor, distribuirea uniforma a capacitatilor de procesare, stocare si comunicatie cu imbunatatirea semnificativa a gradului de utilizare relativ la fiecare resursa fizica, diminuarea costurilor operationale.

Sistemele/echipamentele oferite trebuie sa respecte urmatoarele cerinte generale:

- Sistemele si echipamentele livrate trebuie sa fie noi, neutilizate si de ultima generatie. Ele trebuie sa asigure gradul necesar de performanta, fiabilitate si flexibilitate fiind proiectate si destinate pentru aplicatii critice de tip "enterprise level";
- Dispozitivele hardware trebuie sa fie astfel proiectate incat sa poata asigura scalabilitatea sistemului in cazul cresterii ulterioare a necesarului de resurse de calcul;
- Dispozitivele hardware trebuie sa fie compatibile cu caracteristicile retelei electrice din Romania astfel incat sa fie garantata conectarea fara probleme a acestora la reseaua electrica existenta a beneficiarului;
- Toate aceste cerinte sunt dezvoltate la nivel de detaliu in cadrul cererii de oferta. In acelasi timp cerintele nu sunt limitative ofertantii avand libertatea de a le dezvolta si extinde conform solutiei pe care au in vedere sa o propuna si care trebuie să îndeplinească în totalitate cerintele beneficiarului;



- Ofertantii vor avea în vedere că toate cerintele si caracteristicile solicitate explicit pentru Soluția propusa in cadrul cererii de oferta au un caracter minim si obligatoriu.

4.4.1.1 Echipamente de tip șasiu modular

Soluția/componentele oferite trebuie să îndeplinească următoarele **cerințe funcționale generale**:

- Arhitectura soluției propuse trebuie să includă următoarele caracteristici generale de fiabilitate, disponibilitate și ușurință în efectuarea operațiunilor de intretinere/remediere a defectiunilor (Reliability Availability Serviceability-RAS) la nivel de servere sau șasiu:
 - o Componente redundante în interiorul sistemului (surse de alimentare electrică, module de ventilatie, module de procesare, module de comunicare);
 - o Capabilități de auto-testare și rezolvare a defectelor intermitente fără intervenție umană;
 - o Dealocarea "online" și izolarea componentelor defecte ale sistemului (de exemplu discuri, ventilatoare, subsisteme de alimentare cu energie electrică, adaptoare PCI). In momentul reboot-ului componentele defecte vor fi deconfigurate;
 - o Diagnosticarea erorilor în timp real;
 - o Capabilități arhitecturale de prevenire a erorilor.
- Platforma de procesare reprezintă un ansamblu modular pentru suportul procesării, în arhitecturi mixte eterogene dedicat operațiunilor de procesare specifice, format din șasiu modular și module de procesare generala, detaliate in subcapitolele urmatoare.

Echipamentul de tip șasiu modular trebuie sa respecte urmatoarele **cerinte funcționale specifice**:

Caracteristica	Cerinta tehnica minimala
Arhitectura	<ul style="list-style-type: none"> ▪ Componenta de tip șasiu modular pentru suportul procesării centralizate, cu suport inteligent pentru optimizarea, balansarea si integrarea modulelor de procesare, de stocare si a extensiilor de I/O ale acestora, precum și a modulelor de management; ▪ Sasiul trebuie sa suporte interconectarea cu alte sasiuri similare si agregarea resurselor de procesare, stocare si a extensiilor I/O ale acestora intr-o singura platforma unificata, administrabila prin intermediul unui singur set unitar de unelte de management; ▪ Șasiul trebuie configurat pentru instalarea a minim 8 noduri de procesare de tip blade sau similare, optimizate pentru asigurarea densității si puterii de calcul necesare;

	<ul style="list-style-type: none"> ▪ Șasiul va fi echipat cu toate componentele redundante, hot-plug/hot-swap și utilizabile în mod concurrent, pentru alimentare și ventilare, management (inclusiv procesoare de serviciu/management);
<p>Funcționalități performante și</p>	<ul style="list-style-type: none"> ▪ Șasiu fără management local, a cărui administrare să se poată face integrat, la nivelul întregului sistem, prin interfața unică de administrare; ▪ Să nu necesite o configurare inițială și să fie recunoscut automat de aplicația unică de administrare; ▪ Midplane de tip pasiv, capabil să: ▪ Asigure interfețe de tip „10 Gigabit Ethernet” și „40 Gigabit Ethernet” pentru nodurile de procesare; ▪ Asigure minim 2(două) interfețe pentru fiecare server blade; ▪ Asigure o lățime de bandă agregată pentru nodurile de procesare de minim 1,2Tbps;
<p>Interconectare LAN/SAN</p>	<p>Se va face prin 2 dispozitive cu rol de extensie locală a echipamentelor externe pentru accesul unificat în cele două rețele. Cele două dispozitive vor asigura următoarele funcționalități:</p> <ul style="list-style-type: none"> ▪ Failover automat prin acces de tip „active – active” la midplane-ul șasiului și la echipamentele pentru accesul unificat; ▪ Autoconfigurare, prin sincronizarea automată a firmware-ului local cu cel de pe echipamentele pentru accesul unificat; ▪ Fără management local, administrarea acestora făcându-se integrat, la nivelul întregului sistem, prin interfața unică de administrare; ▪ Minim 32 porturi interne de tip „10 Gigabit Ethernet” și 4 (patru) porturi externe de tip „40 Gigabit Ethernet”, capabile FCOE; ▪ Performanță de comutare: minim 960 Gbps; ▪ Funcționalități „Layer 2”: ▪ Minim 1000 VLAN-uri și VSAN-uri; ▪ Suport pentru „jumbo frames” (9216 bytes) pe toate porturile; ▪ La mutarea unei mașini de pe un nod de procesare pe altul conlucrează cu celelalte componente ale sistemului pentru a transfera automat identitatea de rețea a acesteia (adresă MAC, adresă IP, VLAN, QoS, politici de securitate, etc.) în noul context; ▪ QoS:

	<ul style="list-style-type: none"> ▪ Bazat pe standardul IEEE802.1p; ▪ Cozi de servire a pachetelor, in iesire, bazate pe campul COS (Class Of Services) și cu capabilități de priorizare strictă; ▪ Minim 8 cozi hardware per port; ▪ Planificarea porturilor de ieșire prin WRR (Weighted Round Robin);
Surse de alimentare	<ul style="list-style-type: none"> ▪ Surse de alimentare interne în șasiu, de tip „hot-swap”, care să asigure alimentarea redundantă în condiții de încărcare maximă a șasiului; ▪ Redundanță de tip „N+1” și „N+N”, cu capabilități „load-balancing” și „failover”; ▪ Plaja de tensiune operabilă: 200-240V AC; ▪ Plaja de frecvența suportată: 50– 60 Hz; ▪ Echipare minimală: 4 surse; ▪ Puterea minimă per sursă: 2500 W; ▪ Sursele se livrează cu cablu de alimentare tip PDU;
Sistem de ventilație	<ul style="list-style-type: none"> ▪ Sistem de ventilație de tip „hot-swap”, redundant, instalat intern în șasiu; ▪ Flux de aer din fata catre in spate; ▪ Echipare minimală: 8 ventilatoare;
Cerinte constructive	<ul style="list-style-type: none"> ▪ Montabil în rack-uri standard de 19”; ▪ Ofertantul trebuie să livreze un kit cu elementele de fixare/instalare în rack (suportți, șuruburi/captive);
Garanție și suport	<ul style="list-style-type: none"> ▪ Pentru toate elementele și modulele integrate, soluția va include garanție de minim 36 de luni. Suportul și garanția trebuie asigurate în România de producătorul respectivelor echipamente sau prin partener autorizat; ▪ Garanția hardware va fi asigurată cu un SLA (Service Level Agreement) de 8x5xNBD (8 ore pe zi, 5 zile pe săptămână, cel mai târziu a doua zi lucrătoare – Next Business Day), care să garanteze diagnosticarea echipamentului sau modulului defect și înlocuirea acestuia în maxim 3 zile lucrătoare, fără alte costuri; ▪ Se va asigura acces 24x7 în centrul de suport al producătorului, cu posibilitatea raportării problemelor aparute în funcționare și solicitarea rezolvării acestora în funcție de severitate. De

	asemenea se va asigura dreptul de a face update-uri si upgrade-uri software (sistem de operare, firmware, etc).
--	---

4.4.1.2 Echipamente de interconectare privată LAN/SAN

Echipamentele de interconectare privata LAN/SAN trebuie sa respecte fiecare urmatoarele **cerinte functionale specifice**:

Caracteristica	Cerinta tehnica minimala
Arhitectura	Complet redundanta bazata pe cel putin 2 module de comunicatie;
Funcționalități performanțe	<ul style="list-style-type: none"> ▪ Echipamentul va asigura două funcționalități majore: <ul style="list-style-type: none"> ▪ Accesul unificat al nodurilor de procesare generala la rețeaua Ethernet și la storage, prin tehnologia FCoE; ▪ Managementul centralizat al resurselor infrastructurii – noduri de procesare generala (procesoare, memorie, BIOS, adaptoare CNA, interfețe LAN și SAN, etc), șasiu (surse de alimentare, ventilație, dispozitivele de extensie FCoE, etc) – și al componentelor proprii de integrare în rețelele LAN și SAN, printr-o interfață unică de administrare și monitorizare; ▪ Porturi: <ul style="list-style-type: none"> ▪ Cel puțin 40 de sloturi tip „QSFP” si „SFP+”, capabile FCoE, 10 si 40 Gigabit Ethernet, precum si 4, 8, 16G Fibre Channel (FC), pentru conectarea la șasiul de noduri de procesare și la rețeaua Ethernet, precum si la platformele de stocare; ▪ Cel puțin 16 din aceste porturi trebuie să poată funcționa, la alegere, ori in mod FCoE, ori in mod 10 Gigabit Ethernet, ori in mod 4, 8 sau 16G Fibre Channel (FC); ▪ Cel puțin 8 din aceste porturi trebuie să poată funcționa atat ca 40 Gbps Ethernet cat si ca 4x10 Gbps Ethernet (cu transceiver de tip QSFP sau echivalent); ▪ Capacitate de procesare: minim 2 Tbps; ▪ Disponibilitate înaltă; ▪ Cele două echipamente trebuie să poată lucra într-o arhitectură de tip „cluster”, în care software-ul care asigură interfața unică de administrare a sistemului va funcționa în mod „activ – pasiv”; ▪ Interfețele prin care se va face comunicația in interiorul cluster-ului trebuie să fie dedicate, altele decat cele mai sus menționate;

	<ul style="list-style-type: none">▪ Funcționalități „Layer 2”:▪ Minim 1000 VLAN-uri și VSAN-uri per echipament;▪ Suport pentru „jumbo frames” (9216 bytes) pe toate porturile;▪ Rapid Per-VLAN Spanning Tree Plus;▪ IGMP versiune 1, 2 și 3 snooping;▪ EtherChannel bazat pe IEEE 802.3ad cu capabilități avansate de distribuire a traficului, prin funcții de hashing ce iau în calcul informații Layer 2, 3 și 4;▪ La mutarea unei mașini de pe un nod de procesare pe altul conlucrează cu celelalte componente ale sistemului pentru a transfera automat identitatea de rețea a acesteia (adresă MAC, adresă IP, VLAN, QoS, politici de securitate, etc.) în noul context;▪ QoS:▪ Bazat pe standardul IEEE802.1p;▪ Egress queuing, bazat pe COS și cu capabilități de priorizare strictă;▪ Minim 8 cozi hardware per port;▪ Planificarea porturilor de ieșire prin WRR (Weighted Round Robin);
Management	<ul style="list-style-type: none">▪ Centralizat, pentru toate componentele sistemului, printr-o aplicație unică de administrare și monitorizare care va rula în cadrul cluster-ului, în mod „activ – pasiv”;▪ Instanța aplicației (cea „activă”) trebuie să poată administra ambele echipamente pentru acces unificat, minim 16 șasiuri cu noduri de procesare generala și minim 128 de noduri de procesare;▪ Accesul la aplicație trebuie să se poată face din rețeaua IP prin interfață GUI, prin interfață în linie de comandă (CLI) și prin API XML public;▪ Aplicația trebuie să rezide în firmware-ul echipamentelor și să nu necesite un server de management extern;▪ Comunicația dintre aplicație și celelalte componente ale sistemului – șasiu, noduri de procesare, adaptoare unificate de comunicație, dispozitivele de extindere trebuie să se desfășoare automat și să se bazeze pe funcții de „autodescoperire”;▪ Aplicația trebuie să permită provizionarea nodurilor de procesare și a parametrilor lor I/O prin definirea și utilizarea de profiluri;

	<ul style="list-style-type: none"> ▪ Profilurile trebuie să permită crearea unui nivel de abstractizare care să permită decuplarea identității unui nod de procesare (procesor, memorie, BIOS, interfețe LAN și SAN, adrese MAC și WWN), împreună cu drepturile de acces în rețea și stocare necesare (VLAN, QoS, Security, VSAN, Zoning, LUN-uri) de hardware-ul și infrastructura LAN/SAN pe care, la un moment dat, acesta le folosește; ▪ Aplicația trebuie să permită operaționalizarea la cerere a unuia sau mai multor noduri de procesare fizice, prin configurarea automată a unuia sau mai multor noduri de procesare, adaptoare unificate de comunicare, NIC și HBA, dispozitive de extindere a accesului din șasiuri, și a parametrilor necesari accesului în LAN și SAN, pe echipamentele pentru acces unificat, având drept referință un profil definit anterior; ▪ Aplicația trebuie să asigure funcții de inventariere, diagnostic, monitorizare, detecție a erorilor, auditare și colectare de statistici; ▪ Aplicația trebuie să poată exporta configurația întregului sistem, facilitând procese bazate pe ITIL;
Surse de alimentare	<ul style="list-style-type: none"> ▪ Minim 2 surse de alimentare interne, de tip „hot-swap”, care să asigure alimentarea redundantă în condiții de încărcare maximă a șasiului cu transceiver-e; ▪ Redundanță de tip „1+1”, cu capabilități „load-balancing” și „failover”; ▪ Plaja de tensiune operabilă: 100-240V AC; ▪ Plaja de frecvență suportată: 50– 60 Hz; ▪ Se livrează cu 2 cabluri de alimentare de tip PDU;
Sistem de ventilație	<ul style="list-style-type: none"> ▪ Sistem de ventilație de tip „hot-swap”, redundant, instalat intern; ▪ Flux de aer de tip “front to back”; ▪ Echipare minimală: 2 ventilatoare, în configurație redundantă “1+1”;
Cerinte constructive	<ul style="list-style-type: none"> ▪ Montabil în rack-uri standard de 19”; ▪ Dimensiune maxima 1U; ▪ Ofertantul trebuie să livreze un kit cu elementele de fixare/instalare în rack (suport, șuruburi/captive);



Handwritten signatures and marks at the bottom of the page.

Garanție și suport	<ul style="list-style-type: none"> ▪ Pentru toate elementele și modulele integrate, soluția va include garanție de minim 36 de luni. Suportul și garanția trebuie asigurate în România de producătorul respectivelor echipamente sau prin partener autorizat; ▪ Garanția hardware va fi asigurată cu un SLA (Service Level Agreement) de 8x5xNBD (8 ore pe zi, 5 zile pe săptămână, cel mai târziu a doua zi lucrătoare – Next Business Day), care să garanteze diagnosticarea echipamentului sau modulului defect și înlocuirea acestuia în maxim 3 zile lucrătoare, fără alte costuri; ▪ Se va asigura acces 24x7 în centrul de suport al producătorului, cu posibilitatea raportării problemelor aparute în funcționare și solicitarea rezolvării acestora în funcție de severitate. De asemenea se va asigura dreptul de a face update-uri și upgrade-uri software (sistem de operare, firmware, etc).
--------------------	---

4.4.1.3 Echipamente de procesare generală

Echipamentele de procesare generală trebuie să respecte fiecare următoarele **cerințe funcționale specifice**:

Caracteristica	Cerința tehnică minimală
Arhitectura	<ul style="list-style-type: none"> ▪ Nod de procesare generală de tip blade, compatibil cu Șasiul modular pentru suportul procesării centralizate oferit; ▪ Suport multiprocesor pentru minim 2 procesoare fizice;
Procesor	<ul style="list-style-type: none"> ▪ Număr de procesoare instalate: minim 2;
Memorie internă	<ul style="list-style-type: none"> ▪ Tip memorie: DDR4-2400-MHz RDIMM/PC4-19200/dual rank/x4;
Interfețe de rețea	<ul style="list-style-type: none"> ▪ Minim 2x10 Gigabit Ethernet, prin adaptor de tip "Unified": <ul style="list-style-type: none"> ▪ Cu funcționalitate FCOE; ▪ Cu suport pentru failover și load balancing; ▪ Capabil să furnizeze virtualizare la nivel de adaptor un minim de 64 interfețe virtuale LAN și SAN, care să poată fi create dinamic și la cerere, și care să fie văzute de serverul fizic ca dispozitive PCI-e locale, alocabile mașinilor virtuale; ▪ Să suporte procesarea în hardware a protocoalelor pentru virtualizarea rețelelor VXLAN și NVGRE

Stocare	Doua carduri SD conectate la un controller RAID cu suport pentru RAID1;
Acces	<ul style="list-style-type: none"> ▪ Suport pentru acces prin KVM local; ▪ Suport pentru acces de tip „out of band” prin: <ul style="list-style-type: none"> ▪ KVM la distanță, bazat pe IP; ▪ Protocol SSH; ▪ Virtual Media și IPMI (Intelligent Platform Management Interface);
Management	<ul style="list-style-type: none"> ▪ Procesor de management integrat, cu capabilități de monitorizare a componentelor critice local și de la distanță; ▪ La instalare și pentru integrarea în sistem, nodul de procesare nu trebuie să necesite o configurare prealabilă; ▪ Nodul de procesare trebuie să posede o facilitate de „autodesoperire”, prin care este recunoscut și configurat automat de către aplicația unică de administrare a componentelor întregului sistem;
Compatibilitate sisteme de operare	Suport pentru Microsoft Windows Server 2012 R2/2016, VMware vSphere 6.0/6.5, Red Hat Linux 7.x;
Garanție și suport	<ul style="list-style-type: none"> ▪ Pentru toate elementele și modulele integrate, soluția va include garanție de minim 36 de luni. Suportul și garanția trebuie asigurate în România de producătorul respectivelor echipamente sau prin partener autorizat; ▪ Garanția hardware va fi asigurată cu un SLA (Service Level Agreement) de 8x5xNBD (8 ore pe zi, 5 zile pe săptămână, cel mai târziu a doua zi lucrătoare – Next Business Day), care să garanteze diagnosticarea echipamentului sau modulului defect și înlocuirea acestuia în maxim 3 zile lucrătoare, fără alte costuri; ▪ Se va asigura acces 24x7 în centrul de suport al producătorului, cu posibilitatea raportării problemelor aparute în funcționare și solicitarea rezolvării acestora în funcție de severitate. De asemenea se va asigura dreptul de a face update-uri și upgrade-uri software (sistem de operare, firmware, etc).

4.4.1.4 Componenta de virtualizare sistem

Soluția va include o componentă de virtualizare dedicată, bazată pe Hypervisor propriu, fără dependență de un sistem de operare anume. Această soluție va fi instalată direct în platforma de procesare și va beneficia de suportul acestei platforme atât la nivelul capacității de procesare cât și la nivelul opțiunilor de conectivitate și integrare cu restul elementelor fizice de infrastructură.

Componenta de virtualizare sistem trebuie să îndeplinească următoarele **cerințe funcționale specifice**:

Caracteristica

Cerința tehnică minimă

Funcționalități

- Hypervisorul trebuie să fie matur, testat și implementat în infrastructuri de producție complexe și să ofere performanță maximă pentru aplicațiile și serviciile instalate în mașini virtuale indiferent de complexitatea și natura acestora. Nivelul de abstractizare a componentelor fizice din platformele de procesare, stocare și comunicație nu trebuie să adauge complexitate și/sau penalizări de performanță sesizabile în funcționarea aplicațiilor și serviciilor deservite;
- Platforma de virtualizare trebuie să fie compatibilă cu toți producătorii hardware recunoscuți: IBM, Dell, HP, Sun, Intel, iar hypervisorul pe care această platformă se bazează trebuie să fie independent de producătorul sau de metoda de stocare internă/externă disponibilă în platforma de procesare și/sau stocare pe care rulează;
- Platforma de virtualizare trebuie să ofere suport pentru următoarele sisteme de operare instalabile în mașina virtuală: Windows Xp/Vista/7/10/2003/2008/2008 R2/2012 R2/2016, Linux Suse/Red Hat/CentOS, FreeBSD, Solaris, Netware și să permită adăugarea de spațiu de stocare pentru mașinile virtuale prin folosirea următoarelor protocoale: NAS – NFS ; SAN – iSCSI/FC/FCoE, asigurând astfel compatibilitate cu majoritatea tehnologiilor implementate în mod uzual atât în platformele de procesare cât și în platformele de stocare;
- Platforma de virtualizare nu trebuie să depindă de un sistem de operare gazdă a cărui actualizare să afecteze disponibilitatea și funcționalitatea echipamentelor din platforma de procesare, respectiv a mașinilor virtuale care rulează pe aceste echipamente;

- Amprenta pe disc a hypervisor-ului trebuie sa aiba dimensiuni reduse astfel încât instalarea hypervisor-ului să poata fi realizata foarte rapid chiar și prin intermediul rețelei de comunicare, oferind totodată posibilitatea de rulare integrala din mediu de tip USB;
- Platforma de virtualizare trebuie sa ofere suport nativ pentru USB 3.0 și rularea de aplicații grafice (DirectX sau OpenGL2) in masinile virtuale rezidente, respectiv suport pentru accelerarea video in hardware pentru respectivele masini virtuale (suport pentru tehnologia de accelerare video oferita de NVIDIA GRID sau echivalent);
- Platforma de virtualizare trebuie sa ofere suport nativ pentru conectarea pe port serial in orice masina virtuala, prin folosirea unui concentrator serial de retea;
- Componentele virtuale ale platformei sa poata fi modificate cu usurinta permitand astfel crearea de configuratii diferite pentru seturi comune de masini virtuale, precum si crearea de configuratii unitare la nivelul intregii infrastructuri virtuale, atat din prisma elementelor virtuale de procesare si stocare (integrate nativ in platforma sau prin integrarea nativa cu componente terte ale respectivelor platforme de procesare si stocare), cat si din prisma elementelor de comunicare (posibilitatea integrarii directe cu platforma de retea aleasa prin intermediul unor conectori/componente proprietare sau de la producatorul platformei de retea si asigurarea crearii unei retele virtuale unificate la nivelul intregii infrastructuri virtuale);
- Platforma de virtualizare trebuie sa ofere mecanisme nativ integrate pentru adaugarea de resurse de procesare si memorie fara restartarea sistemului de operare din masina virtuala, (in masura in care sistemul de operare suporta aceste facilitati), mecanisme ce pot fi independente de platformele de procesare/stocare/comunicatie sau prin intermediul unor conectori/componente comune respectivelor platforme;
- Prin integrarea nativa cu platformele de procesare, masinile virtuale definite in platforma de virtualizare trebuie sa beneficieze concomitent de suport de multiprocessing simetrica a minim 64 procesoare logice, minim 1 TB de RAM si acces la totalitatea

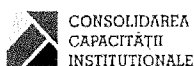
porturilor I/O, resurse adresabile virtual prin abstractizarea resurselor fizice disponibile in infrastructura;

- Resursele virtuale (resurse de procesare, stocare si comunicatie) disponibile la nivelul intregii platforme de virtualizare (prin integrarea nativa cu platformele fizice de procesare, stocare si comunicatie) trebuie sa fie adresabile si configurabile in totalitatea lor prin intermediul unei singure interfete de management si nu prin configurarea separata pentru fiecare echipament disponibil in respectivele platforme;
- Platforma de virtualizare trebuie sa permita agregarea tuturor resurselor fizice (placi de retea, switch-uri de comunicatie integrate in platformele de procesare) si virtuale de comunicatie (switch-uri virtuale) intr-un singur nivel unitar de comunicatie, adresabil la nivelul intregii infrastructuri virtuale indiferent de complexitatea acestora sau a platformelor de procesare si comunicatie ce se integreaza prin intermediul ei. Deasemenea trebuie sa ofere mecanisme automate de evaluare si priorizare continua a accesului masinilor virtuale si aplicatiilor rezidente la resursele de comunicatie disponibile, permitand alocarea si realocarea dinamica a acestor resurse in functie de cerintele de moment sau conform unor politici prestabilite;
- Platforma trebuie sa permita gruparea si organizarea logica a resurselor de procesare in functie de necesitati, precum si izolarea acestor grupari de resurse, respectiv sa asigure flexibilitatea necesara mării cantitatii de resurse disponibile intr-o grupare prin extragerea de resurse din alte grupari. Accesul masinilor virtuale si apartenenta la aceste grupari de resurse trebuie sa se faca atat in mod manual prin interventia unui operator cat si pe baza unor politici dinamice de acces;
- Platforma trebuie sa ofere functionalitati integrate nativ de pornire/repornire a oricarei masini virtuale (indiferent de aplicatiile si serviciile ce ruleaza pe respectivele masini virtuale), in cadrul aceluiasi server sau pe servere diferite, in cazul detectarii nemijlocite a unei probleme de functionare a masinii virtuale au a aplicatiilor si serviciilor ce ruleaza pe aceste masini virtuale. Scenarii posibile ce necesita implementarea nativa a unui astfel de mecanism de recuperare ar putea fi: blocarea sistemului de operare ce ruleaza in masina virtuala, intreruperea cailor de



Proiect cofinanțat din Fondul Social European prin
Programul Operațional Capacitate Administrativă 2014-2020!

- comunicatie catre platformele de stocare, intreruperea cailor de comunicatie catre platforma comuna de management, etc;
- Platforma trebuie sa ofere mecanisme integrate de balansare a incarcarii resurselor fizice si virtuale disponibile in infrastructura si redistribuire a sarcinilor generate de utilizatori, servicii si aplicatii, prin integrarea nativa cu platformele hardware, indiferent de producatorul respectivelor elemente de infrastructura. Aceste mecanisme trebuie sa fie disponibile atat la comanda prin interventia unui operator cat si prin operatiuni automate definite in functie de necesitati, gradul de ocupare al resurselor si/sau pe baza unor reguli/politici prestabilite;
 - Platforma de virtualizare trebuie sa ofere redundanta completa a arhitecturii, atat la nivelul elementelor virtuale distincte (procesoare, memorie, elemente de comunicatie, masini virtuale, etc) cat si la nivelul unor seturi intregi de echipamente de infrastructura (platforma de procesare, platforma de stocare, platforma de comunicatie, etc) prin integrarea nativa cu mecanismele redundante existente in aceste platforme si prin folosirea unor tehnologii native de redundanta, balansare si fail-over aplicabile intregului spectru de functionalitate asigurata (masini virtuale, servicii, aplicatii, platforme de procesare, platforme de stocare, platforme de comunicatie);
 - Platforma de virtualizare trebuie sa permita configurarea spatiului de stocare virtual prin integrarea directa cu platforma de stocare aleasa prin intermediul unor conectori/componente native sau de la producatorul platformei de stocare, mecanism ce va permite extinderea discurilor virtuale fara a fi necesara oprirea masinilor virtuale ce au atasate aceste discuri. Deasemenea prin integrare directa cu platforma de stocare, trebuie sa ofere mecanisme automate de monitorizare a incarcarii I/O si de alocare/reallocare dinamica a resurselor I/O catre masinile virtuale in functie de cerintele acestora (ad-hoc sau conform unei politici prestabilite), realizand astfel o prioritizare inteligenta a accesului aplicatiilor la resursele de stocare;
 - Prin aceleasi mecanisme de integrare (inclusiv la nivelul componentelor apelabile si programabile din cadrul altor platforme, componente de tip API) cu platformele de stocare oferite, trebuie sa permita identificarea si folosirea optima a



Proiect cofinanțat din Fondul Social European prin
Programul Operațional Capacitate Administrativă 2014-2020!

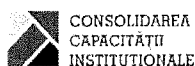


mecanismelor de asigurare a cailor redundante de acces in platformele de stocare si a mecanismelor tertе de protectie a datelor stocate, incluzand volumele adresate direct de platforma de virtualizare, respectiv volumele de date folosite de aplicatii, servicii si utilizatori;

- Integrarea nativa cu platformele de stocare alese trebuie sa permita alocarea dinamica de spatiu catre masinile virtuale, chiar daca acel spatiu nu este fizic disponibil in aceste platforme, permitand functionarea corecta a aplicatiilor si serviciilor ce necesita resurse stricte de spatiu de stocare, respectiv cresterea transparenta a volumelor de date prin adaugarea de resurse fizice de stocare (discuri) doar in momentul cand acestea devin necesare;
- Platforma trebuie sa includa mecanisme proprietare de catalogare si grupare a resurselor disponibile in platformele de stocare, indiferent de tipul, producatorul si numarul acestora (tipuri de discuri, latentă, tipul volumelor si metoda de export aplicata asupra lor), permitand astfel crearea de profile de stocare si asocierea acestor profile cu distribuirea/redistribuirea masinilor virtuale in functie de cereri temporare ale aplicatiilor sau in baza unor politici predefinite;
- Deasemenea trebuie sa includa atat mecanisme automate de evaluare continua a necesarului de resurse I/O cat si mecanisme de pozitionare si repositionare a masinilor virtuale in gruparile de resurse de stocare in functie de cerintele initiale ale aplicatiilor, respectiv in functie de cerintele evaluate in mod continuu. Astfel se obtine o balansare permanenta a distributiei masinilor virtuale proportional cu gruparile de resurse de stocare, indiferent de cerintele de performanta si capacitate de stocare ale respectivelor masini virtuale;
- Trebuie sa integreze nativ mecanisme de agregare a conexiunilor fizice de retea disponibile in platformele de procesare, astfel incat sa poata oferi un sigur nivel virtual si unificat de comunicatie, nivel ce va fi disponibil pentru intregul set de aplicatii si servicii gazduite in platforma de virtualizare. Mecanismele vor fi independente de platformele de procesare si de cele de comunicatii, permitand adaugarea transparenta de functionalitati specifice de comunicatie (management, control si tipuri de protocol suportate)

de la producatori terți. Se va obține astfel implementarea unui set comun de funcționalități, unitar la nivelul arhitecturii de rețea (fizică și virtuală), set ce va permite distribuția inteligentă, dinamică a încărcării pe aceste conexiuni, respectiv redundanța nativă atât la nivelul conexiunilor de rețea fizice/virtuale, cât și la nivelul strict al setului de funcționalități implementate, indiferent de producătorul platformelor de procesare și de comunicație folosite;

- Platforma trebuie să implementeze nativ mecanisme de asigurare dinamică a prioritizării accesului la aplicații și servicii, prin integrarea directă cu platformele de stocare și de comunicație oferite, respectiv prin aplicarea de politici și profile asupra accesării datelor ce constituie mașinile virtuale respective și/sau sunt folosite de către respectivele aplicații, indiferent de locația respectivelor date (rezidente în platforma de stocare sau tranzitate prin mediile de comunicație fizice/virtuale). Se va obține astfel garantarea accesului prioritar la aplicațiile și serviciile critice din infrastructură;
- Platforma va trebui să integreze mecanisme automate de instalare/provizionare a unei întregi imagini preconfigurate de hypervisor, mecanism necesar în cazul adăugării rapide a unui nou server în platformele de procesare virtualizate, precum și mecanisme automate de instalare/provizionare a actualizărilor software la nivelul sistemelor de operare instalate în mașinile virtuale, mecanisme independente de, dar integrate cu funcționalitățile de actualizare native ale respectivelor sisteme de operare;
- Prin integrarea cu resursele de management, platforma de virtualizare trebuie să permită mecanisme integrate de mutare a mașinilor virtuale de pe un server pe altul sau dintr-un datacenter în altul fără oprirea sistemului de operare ce rulează în mașina virtuală și fără întreruperea serviciului oferit de aplicația/aplicațiile din mașina virtuală. Aceleași mecanisme trebuie să permită atât mutarea întregului harddisk virtual concomitent pentru oricare mașină virtuală în cadrul aceluiași datacenter sau între datacenter-e diferite, independent de platforma de stocare folosită și de mecanismele de replicare ale acesteia, precum și extinderea automată a harddisk-urilor virtuale pe măsura ce

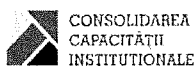


Proiect cofinanțat din Fondul Social European prin
Programul Operațional Capacitate Administrativă 2014-2020!



sistemul de operare și aplicațiile din mașinile virtuale o cer. În acest fel vor deveni posibile scenarii automate, prin politici pre-definite/definibile, de consolidare a mașinilor virtuale pe un număr prestabilit de servere și oprirea automată a serverelor fără activitate sau cu subutilizare a resurselor de procesare;

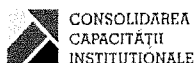
- Tot prin integrarea cu resursele de management, platforma de virtualizare trebuie să permită operațiuni automate, bazate pe politici pre-definite/definibile, de repornire (pe o altă platformă de procesare) a mașinilor virtuale individuale, precum și a seturilor de mașini virtuale ce au fost definite ca deserving o singură aplicație/serviciu sau un sub-set al unei aplicații/serviciu, în eventualitatea unei defecțiuni hardware majore la nivelul platformelor de procesare;
- Platforma trebuie să includă funcționalitate nativă de rulare în paralel a unei mașini virtuale sau a unui set de mașini virtuale ce deservește o singură aplicație/serviciu, pe un număr de minim două echipamente distincte din platformele de procesare. Mecanismul trebuie să folosească tehnologii independente dar integrate cu platformele de procesare și de stocare, asigurând replicarea transparentă și sincronă a conținutului de memorie și a conținutului de disc asociat unei mașini virtuale, respectiv unui set de mașini virtuale, fără introducerea de latență în respectivele platforme sau în funcționarea mașinilor virtuale;
- Platforma trebuie să includă o componentă de administrare și monitorizare dedicată, disponibilă atât la nivelul echipamentelor fizice ce alcatuiesc platformele de procesare, stocare și comunicație cât și la nivelul mașinilor virtuale, ale resurselor virtualizate, aplicațiilor, serviciilor și protocoalelor însumate în infrastructură. În vederea accesului facil la funcțiile de administrare și monitorizare oferite, platforma trebuie să permită acces atât prin consolă locală/la distanță cât și prin browser web și prin platforma de management dedicată;
- Componenta de management și monitorizare a infrastructurii trebuie să permită autentificarea utilizatorilor bazată pe roluri și privilegii distincte de utilizare, prin integrarea cu un serviciu de tip director. De asemenea trebuie să permită crearea facilă de politici



Proiect cofinanțat din Fondul Social European prin
Programul Operațional Capacitate Administrativă 2014-2020!

dinamice de acces la resursele de procesare, precum și de disponibilitate ale acestora;

- Separarea privilegiilor administrative trebuie să se poată face pe orice element disponibil în interfața de administrare (server, utilizator, resursa de procesare, stocare, rețea, etc), permițând astfel crearea de zone/domenii de securitate în funcție de aplicații și/sau roluri funcționale, nu în funcție de elementele disponibile în infrastructura de procesare, stocare și comunicație;
- Platforma de management trebuie să asigure și mecanisme de definire și aplicare a profilurilor standard de configurație pentru serverele ce fac parte din infrastructura virtuală. De asemenea, să permită configurarea de politici de aplicare a acestor profile în funcție de necesitățile de moment sau în concordanță cu politica stabilită în prealabil;
- Componenta de management trebuie să se integreze nativ sau prin intermediul unor conectori/componente cu platforma de procesare și cu platforma de stocare în vederea realizării operațiunilor de backup direct din aceste platforme, precum și pentru crearea rapidă a unor zone izolate atât din punct de vedere al securității cât și al grupurilor de resurse de procesare, stocare și rețea, în scopul testării și dezvoltării;
- Componenta de management trebuie să integreze nativ funcții de monitorizare analitică a integrității și performanței platformei de virtualizare, funcții ce vor permite anticiparea proactivă a problemelor de performanță și disponibilitate. Respectivul mecanism trebuie să se bazeze atât pe modele de utilizare predefinite, cât și pe funcții integrate de auto-învățare, astfel încât să se asigure vizibilitate completă asupra problemelor din infrastructură;
- Trebuie să integreze nativ funcții de administrare și optimizare a spațiului disponibil în platformele de stocare și a gradului de disponibilitate și ocupare a resurselor virtualizate din platformele de procesare și comunicație, astfel încât să balanseze în permanență nevoile curente ale mașinilor virtuale (atât la nivel individual cât și la nivel global) în raport cu resursele fizice din respectivele platforme, eficientizând utilizarea respectivelor resurse fizice;

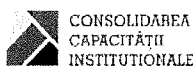


Proiect cofinanțat din Fondul Social European prin
Programul Operațional Capacitate Administrativă 2014-2020!



- Platforma trebuie să integreze un portal de tip dashboard pentru afisarea și analizarea tuturor informațiilor legate de disponibilitate, grad de ocupare a resurselor, metrici de performanță, istoric al acțiunilor administrative și corective, precum și recomandări de optimizare a întregii funcționalități puse la dispoziție de platforma de virtualizare. Portalul trebuie să permită executarea directă de acțiuni corective și administrative asupra elementelor de infrastructură vizate (mașini virtuale, resurse de procesare, stocare și comunicație), acțiuni bazate pe recomandările afișate în portal în urma analizelor efectuate asupra respectivelor elemente;
- Datele monitorizate trebuie să fie automat analizate și exprimate sub formă de metrici de stare, risc și eficiență, permițând identificarea rapidă a potențialelor probleme în infrastructură;
- Platforma trebuie să ofere analize de capacitate și să identifice explicit resursele ce sunt supra-utilizate, ajutând în procesul de redistribuire a sarcinilor de încărcare între elementele platformei în scopul eficientizării rularii aplicațiilor și serviciilor, respectiv să ofere scenarii predefinite de simulare a încărcării pentru a elimina procesele deductive de alocare a resurselor platformei;
- Platforma trebuie să ofere analize automate a proceselor de instalare și configurare a mediului virtualizat, în scopul detectării rapide a eventualelor probleme ce pot apărea datorită configurațiilor defectuoase sau a elementelor noi introduse în infrastructură;
- Trebuie să integreze funcții automate de alertare în cazul depășirii pragurilor optime de funcționare, atât pentru starea tuturor elementelor platformei de virtualizare, cât și pentru metrici de performanță și capacitate;
- Soluția va include garanție de minim 36 de luni. Suportul și garanția trebuie să fie asigurate în România de producătorul respectivei soluții sau prin partenerul autorizat al acestuia;
- Garanția va fi asigurată cu un SLA (Service Level Agreement) de 8x5xNBD (8 ore pe zi, 5 zile pe săptămână, cel mai târziu a doua zi lucrătoare – Next Business Day);
- Se va asigura acces 24x7 în centrul de suport al producătorului, cu posibilitatea raportării problemelor apărute în funcționare și solicitarea rezolvării acestora în funcție de severitate. De

Garanție și suport



Proiect cofinanțat din Fondul Social European prin
Programul Operațional Capacitate Administrativă 2014-2020!



asemenea se va asigura dreptul de a face update-uri si upgrade-uri software.

4.4.1.5 Componenta de sistem de operare

Componenta de sistem de operare trebuie sa respecte fiecare urmatoarele **cerinte functionale specifice**:

Caracteristica	Cerinta tehnica minimala
Cerinte generale	<ul style="list-style-type: none"> ▪ Componenta trebuie sa ofere suport pentru cel putin urmatoarele arhitecturi de processor: <ul style="list-style-type: none"> ○ x86, ○ x86_64 ▪ Componenta trebuie sa ofere suport pentru lucrul cu memoria RAM, astfel: <ul style="list-style-type: none"> ○ x86: minim 16 GB ○ x86_64: minim 1 TB ○ x86_64 ▪ Componenta trebuie sa ofere suport pentru lucrul cu cel putin urmatoarele sisteme de fisiere: <ul style="list-style-type: none"> ○ FAT32 ○ NTFS ▪ Componenta trebuie sa ofere suport pentru lucrul in regim multi-tasking ▪ Componenta trebuie sa ofere suport pentru lucrul cu memoria virtuala (SWAP) ▪ Componenta trebuie sa ofere suport pentru cel putin o tehnologie de virtualizare a resurselor de procesare, stocare si retea ▪ Componenta trebuie sa ofere suport pentru stocarea si replicarea datelor ▪ Componenta trebuie sa ofere suport pentru lucrul cu containere ▪ Componenta trebuie sa ofere suport pentru lucrul cu servere de aplicatie, web si/sau baze de date ▪ Componenta trebuie sa ofere suport pentru controlul accesului si al identitatii, cel putin ACL si OpenLDAP ▪ Componenta trebuie sa ofere suport pentru lucrul la nivel de retea (DNS, DHCP, SDN, VPN, QoS, Firewall, Load Balancing) ▪ Componenta trebuie sa ofere suport pentru accesul de la distanta (Remote Desktop)

	<ul style="list-style-type: none"> ▪ Componenta trebuie sa ofere suport pentru securitate sporita (user/password, tokens, Kerberos, TLS- SSL ▪ Componenta trebuie sa ofere support pentru diagnoza ▪ Componenta trebuie sa include o consola grafica de administrare ▪ Componenta trebuie sa include o componenta de executie automatizata a sarcinilor ▪ Componenta trebuie sa ofere suport pentru lucrul cu browsere de internet
Garanție si suport	<ul style="list-style-type: none"> ▪ Solutia va include garantie de minim 36 de luni. Suportul si garantia trebuie asigurate in Romania de producatorul respectivei solutii sau prin partener autorizat; ▪ Garantia va fi asigurata cu un SLA (Service Level Agreement) de 8x5xNBD (8 ore pe zi, 5 zile pe saptamana, cel mai tarziu a doua zi lucratoare – Next Business Day); ▪ Se va asigura acces 24x7 in centrul de suport al producatorului, cu posibilitatea raportarii problemelor aparute in functionare si solicitarea rezolvarii acestora in functie de severitate. De asemenea se va asigura dreptul de a face update-uri si upgrade-uri software.

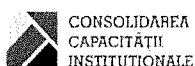
4.4.1.6 Echipamente de integrare LAN

Echipamentele de integrare LAN trebuie sa respecte fiecare urmatoarele **cerinte functionale specifice**:

Caracteristica	Cerinta tehnica minimala
Arhitectura	<ul style="list-style-type: none"> ▪ Complet redundanta bazata pe cel putin 2 module de comunicatie; ▪ Arhitectura de tip „crossbar”, „non-blocking”, capabila sa asigure comunicatii fara pierderi de frame-uri intre oricare doua porturi, la viteza maxima de 10Gbps si 40Gbps, cu o intarziere minima, constanta, care sa nu depinde de lungimea frame-urilor;
Cerinte tehnice generale	<ul style="list-style-type: none"> ▪ Echipamentul va avea caracteristicile unui modul de comunicatie destinat mediului de centru de date, care sa asigure simultan urmatoarele functionalitati: <ul style="list-style-type: none"> ▪ Switch Ethernet Layer 2; ▪ Switch Ethernet Layer 3; ▪ Interfete fizice disponibile: <ul style="list-style-type: none"> ▪ Minim 10 Gigabit Ethernet (cu conector SFP+);

	<ul style="list-style-type: none"> ▪ Minim 40G Ethernet care sa suporte urmatoarele tipuri de transceivere: <ul style="list-style-type: none"> ▪ 40GBase-SR4; ▪ 40GBase-LR4; ▪ 10GBase-SR; ▪ 10GBase-LR; ▪ 10GBase-ER;
Performante	<ul style="list-style-type: none"> ▪ Comutarea la nivel 2: minim 1.4 Tbps si minim 1100 Mpps; ▪ Tabela de adrese MAC de minim 96000 de inregistrari; ▪ Minim 4000 de ID-uri pentru VLAN-uri per switch; ▪ Comutare de tip "Cut-Trough" pentru asigurarea unei latente de comutare a pachetelor port-la-port mai mica de 2 microsecunde; ▪ Procesor de control multi-core;
Functionalitati Layer 2	<ul style="list-style-type: none"> ▪ Incapsulare IEEE 802.1Q; ▪ Rapid Per-VLAN Spanning Tree Plus sau echivalent; ▪ Multiple Spanning Tree Protocol (MSTP) (IEEE 802.1s): minim 64 de instante; ▪ Spanning Tree PortFast, Root Guard si Bridge Assurance; ▪ Virtual Port Channel sau o tehnologie echivalenta care sa permita crearea unui "link-aggregation group" intre doua switch-uri pe de o parte si un alt echipament de tip client (server, switch, router, etc) de partea cealalta; ▪ Link Aggregation Control Protocol (LACP): IEEE 802.3ad; ▪ Posibilitatea balansarii legaturilor din Port Chanel utilizand informatii de nivel 2, 3 si 4; ▪ Suport pentru "Jumbo frames" cu dimensiuni de 9216 bytes pe toate porturile; ▪ Mecanisme de control al inundarii rețelei cu trafic unicast, multicast si broadcast; ▪ Private VLAN, inclusiv pe porturile de tip trunk 802.1Q si EtherChannel; ▪ Suport pentru protocolul LLDP (IEEE 802.3ab); ▪ Suport pentru protocoalele: IEEE 802.3ae, IEEE 802.3z, IEEE 802.1q VLAN, IEEE 802.1ad, IEEE 802.1ba, IEEE 802.3an; 802.1Q VLAN Tagging; 802.1p Class-of-Service (CoS) Tagging for Ethernet frames; 802.1x Port-based network access control;

	<ul style="list-style-type: none"> ▪ Suport pentru protocolul VXLAN si cel puțin 256 Virtual Tunnel End-Points (VTEP);
Funcionalitati Layer 3	<ul style="list-style-type: none"> ▪ Suport pentru urmatoarele protocoale Layer 3: ▪ Open Shortest Path First (OSPF) versiunile 2 si 3; ▪ Border Gateway Protocol (BGP); ▪ RIP v2; ▪ Multicast PIM SM, SSM si MSDP; ▪ Cel puțin 96000 intrari in tabela de routare; ▪ Posibilitatea de a filtra accesul pe interfete dupa informatii despre adresa IP sursa sau destinatie si in acelasi timp si portul TCP/UDP sursa sau destinatie; ▪ DHCP snooping cu posibilitatea de a adauga Optiunea 82; ▪ Facilitatea de a filtra pe un port/VLAN a raspunsurilor la cererile protocolului ARP;
QoS	<ul style="list-style-type: none"> ▪ Layer 2 IEEE 802.1p (CoS); ▪ Configurare QoS per port; ▪ Minim 4 cozi hardware de servire per port; ▪ Posibilitatea de clasificare a traficului bazata pe liste de control al accesului; ▪ Coada cu prioritate stricta; ▪ Weighted Round-Robin (WRR) si Priority Queuing (PQ) pe cozile de iesire;
Management	<ul style="list-style-type: none"> ▪ Suport pentru SPAN si Encapsulated Routed SPAN; ▪ Suport pentru sflow sau echivalent; ▪ Suport pentru revenirea la o configuratie anterioara; ▪ Suport pentru standardul AAA, Tacacs+ si Radius; ▪ Suport pentru interfata XML (Netconf); ▪ Suport pentru monitorizarea utilizarii bufferelor interne; ▪ Suport pentru protocolul SSHv2 si SCP;
Surse de alimentare	<ul style="list-style-type: none"> ▪ Minim 2 surse de alimentare interne, de tip „hot-swap”, care să asigure alimentarea redundantă în condiții de încărcare maximă; ▪ Redundanță de tip „1+1”, cu capabilități „load-balancing” și „failover”; ▪ Plaja de tensiune operabilă: 100-240V AC; ▪ Plaja de frecvența suportată: 50– 60 Hz; ▪ Se livrează cu 2 cabluri de alimentare de tip PDU;



Proiect cofinanțat din Fondul Social European prin
Programul Operațional Capacitate Administrativă 2014-2020!



Sistem de ventilație	<ul style="list-style-type: none"> ▪ Sistem de ventilație de tip „hot-swap”, redundant, instalat intern; ▪ Flux de aer de tip “front to back”; ▪ Echipare minimală: 2 ventilatoare, în configurație redundantă “1+1”;
Cerinte constructive	<ul style="list-style-type: none"> ▪ Montabil în rack-uri standard de 19”; ▪ Ofertantul trebuie să livreze un kit cu elementele de fixare/instalare în rack (suportți, șuruburi/captive);
Garanție si suport	<ul style="list-style-type: none"> ▪ Pentru toate elementele si modulele integrate, solutia va include garantie de minim 36 de luni. Suportul si garantia trebuie asigurate in Romania de producatorul respectivelor echipamente sau prin partener autorizat; ▪ Garantia hardware va fi asigurata cu un SLA (Service Level Agreement) de 8x5xNBD (8 ore pe zi, 5 zile pe saptamana, cel mai tarziu a doua zi lucratoare – Next Business Day), care sa garanteze diagnosticarea echipamentului sau modulului defect si inlocuirea acestuia in maxim 3 zile lucratoare, fara alte costuri; ▪ Se va asigura acces 24x7 in centrul de suport al producatorului, cu posibilitatea raportarii problemelor aparute in functionare si solicitarea rezolvării acestora in functie de severitate. De asemenea se va asigura dreptul de a face update-uri si upgrade-uri la toate componentele software (sistem de operare, firmware, etc).

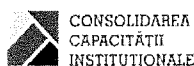
4.4.1.7 Echipament de stocare de Tip 1

În vederea atingerii obiectivelor operationale Solutia trebuie sa includa un sistem de stocare cu arhitectură internă flexibilă, în care nodurile active de control vor fi simultan conectate la toate structurile de tip bus sau loop (SAS loops și similare), pentru a face posibilă arondarea inițială și reconfigurarea ulterioară facilă a alocării discurilor între nodurile de control, între diferitele volume (sau structuri similare), precum și între servicii diferite (SAN/NAS).

Echipamentul de stocare de Tip 1 trebuie sa indeplineasca urmatoarele **specificatii tehnice minimale**:

Caracteristica	Cerinta tehnica minimala
Arhitectura	<ul style="list-style-type: none"> ▪ Platforma unificata de stocare trebuie sa fie echipata cu doua controller-e unificate (SAN/NAS) in acelasi sasiu pentru a putea

	<p>dispune de o configuratie redundanta de tip cluster activ-activ la nivelul echipamentului;</p> <ul style="list-style-type: none"> ▪ Controller-ele trebuie sa fie de tip hot-swap;
Protocol de acces la date	Platforma de stocare trebuie să ofere acces la datele stocate atat prin protocol de tip block (SAN), prin FC (Fiber Channel) si iSCSI, precum si prin protocol de tip file (NAS), prin NFS (v2/v3/v4) si CIFS (SMB2/SMB3);
Memorie	<ul style="list-style-type: none"> ▪ Platforma va include extinderea memoriei cache Read/Write cu discuri in tehnologie SSD, cu o capacitate totala minima de 1 TB (configurata redundat cu minim un disc de tip hot-spare), pentru intreaga platforma, indiferent de marimea volumelor de date accelerate, respectiv de tipul de protocol folosit pentru accesul la accesul la volumele de date accelerate (SAN/NAS);
Nivele RAID	Configurarea si optimizarea matricilor RAID in configuratii cu unul si doua discuri de paritate asociate fiecarui set de discuri componente al unei matrici RAID, precum si posibilitatea de a folosi aceste matrici RAID in mod de replicare integrala de tip mirror;
Conexiuni SAN	<ul style="list-style-type: none"> ▪ Minim 1024 host-uri per platforma de stocare, prin conexiune intermediara de tip Full Fabric; ▪ Pana la 8 host-uri conectate direct la platforma de stocare; ▪ Minim 512 LUN-uri per platforma de stocare;
Dimensiune sistem de fisiere	Minim 256 TB;
Dimensiune LUN exportat	Minim 256 TB;
Hard discuri	<ul style="list-style-type: none"> ▪ Trebuie sa permita utilizarea in paralel a discurilor de tip SAS 6/12 Gbps, NL-SAS 3 Gbps, SSD; ▪ Capacitatile pentru un HDD minim disponibile trebuie sa fie de 2 TB pentru discurile NL-SAS, 600 GB pentru cele SAS, 400 GB pentru cele SSD;
Extensia capacitatii de stocare	Platforma de stocare trebuie să asigure următoarea capabilitate minimă de extensie a capacității de stocare:



Proiect cofinanțat din Fondul Social European prin
Programul Operațional Capacitate Administrativă 2014-2020!



Handwritten signature

Handwritten signature

	<ul style="list-style-type: none">▪ Suport pentru module de expansiune cu discuri de 3,5" respectiv 2,5";▪ Modulele de expansiune trebuie sa se conecteze la echipamentul de stocare prin magistrale de date redundante, cu latime de banda de cel puțin 48 Gbps (SAS 12 Gbps cu 4 cai de acces).
Managementul platformei	<ul style="list-style-type: none">▪ Platforma de stocare trebuie să asigure un sistem de management și monitorizare integrat;▪ Platforma de stocare trebuie să aibă capabilitatea de monitorizare și management a mai multor echipamente din aceeași gamă într-o singură instanță a interfeței, atât pentru serviciile SAN, cât și pentru cele NAS;▪ Platforma de stocare trebuie să asigure provizionarea automată a sistemelor de fișiere;▪ Platforma de stocare trebuie sa asigure monitorizarea performantei si capacitatii platformei de stocare atat la nivel fizic cat si la nivel virtual. Solutia trebuie sa asigure functionalitatile respective atat pentru platforma propusa cat si pentru alte platforme de la acelasi producator;▪ Platforma de stocare trebuie sa includa fara costuri aditionale cel puțin posibilitatea administrării prin intermediul unei interfete web securizate SSL si/sau aplicatie dedicata de management, precum si consola de administrare la distanta SSH/Telnet. Toate functiile native ale sistemului de stocare, precum si functionalitatea licentiata separat trebuie sa fie accesibile in mod integrat prin intermediul acestor unelte de administrare, astfel incat operatiunile de configurare si administrare sa poata fi efectuate indiferent de locatie si de modalitatea de acces;▪ Atat in scop administrativ cat si in vederea accesului la seturile de date, Platforma de stocare trebuie sa permita nativ definirea de utilizatori locali si roluri de utilizare, cu seturi diferite de permisiuni granulare aplicabile actiunilor administrative si/sau seturilor de date. Deasemenea trebuie sa permita integrarea cu un sistem director de tip LDAP, pentru sincronizarea utilizatorilor si a drepturilor de acces la seturile de date partajate de sistem. Pentru sporirea securitatii in mecanismele de autentificare, echipamentul trebuie sa permita integrarea cu un sistem NTP/SNTP pentru sincronizarea informatiilor de timp.



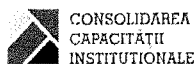
Proiect cofinanțat din Fondul Social European prin
Programul Operațional Capacitate Administrativă 2014-2020!





Mecanismele de export ale volumelor prin intermediul protocolului CIFS trebuie sa beneficieze nativ de suportul integrării echipamentului de stocare cu sistemele de tip director si cu serverele de timp;

- Uneltele de administrare prin interfata web si/sau aplicatie dedicata trebuie sa fie usor de folosit si sa implementeze majoritatea actiunilor administrative (definirea de volume, LUN-uri, exportul seturilor de date indiferent de protocolul folosit pentru export, configurarea functiilor de partajare, optimizare si backup, adaugarea/eliminarea de noduri la/din cluster, definirea relatiilor de replicare, etc) intr-o singura interfata fara a fi nevoie de acces la uneltele in linie de comanda, iar pentru un numar de operatiuni importante de configurare sa puna la dispozitie asistenti de configurare. Uneltele trebuie sa permita atat configurarea si administrarea sistemului curent cat si orice alt sistem existent de la acelasi producator, indiferent de gama si/sau generatie. Deasemenea trebuie sa integreze un panou unificat de afisare a informatiilor legate de performanta (inclusiv gradul de ocupare al procesoarelor, nivel I/O, latenta in functie de protocolul de comunicatie si tipul de export al volumelor, numarul de operatiuni efectuate asupra seturilor de date), informatiilor legate de gradul de ocupare (inclusiv gradul de ocupare per volum de date si tipul de partajare al resurselor), respectiv afisarea informatiilor legate de starea controller-elor, a relatiilor de replicare intre echipamente si a evenimentelor informatonale si/sau de alertare survenite in functionarea oricarui element hardware sau functie software;
- Tot ca parte a uneltelor standard de administrare, Platforma de stocare trebuie sa includa posibilitatea de integrare nativa cu platforma de procesare generala si platforma de procesare specializata astfel incat sa permita definirea volumelor, LUN-urilor, aplicarea politicilor si mecanismelor integrate de optimizare, backup si recuperare, efectuarea operatiunilor de instantiere rapida a seturilor de date ce apartin de masini, analiza si corectarea dinamica a parametrilor de export ai seturilor de date catre platformele de procesare, identificarea si modificarea modului de aliniere logica a partițiilor din sistemele de operare, direct din uneltele de management puse la dispozitie





de platformele de procesare, fara a folosi un alt set de unelte tertе ce nu apartin nici de platforma de stocare, nici de cele de procesare. Astfel se obtine o platforma unitara de management, ce reduce efortul si costul administrativ, indiferent de natura operatiunilor efectuate;

- Platforma de stocare trebuie sa permita accelerarea hardware a operatiunilor ce au loc intre platformele de procesare si sistemul de stocare, prin degrevarea unor procese de la nivelul platformelor de procesare si preluarea lor la nivelul echipamentului de stocare. Aceasta functionalitate trebuie sa permita accelerarea mutarii unei masini intre doua volume de date ale platformelor de procesare si accelerarea efectuarii unei copii identice a unei masini;
- Platforma de stocare trebuie sa includa suport pentru VAAI, VASA si VVols;
- Pentru asigurarea unui nivel optim de disponibilitate operationala, Solutia oferita va permite update si upgrade software si hardware al platformei fara intreruperea serviciilor;
- In scopul alocarii eficiente si dinamice a spatiului de stocare in functie de cerintele previzionate sau de moment, Platforma de stocare trebuie sa includa nativ sau prin licentiere ulterioara, un mecanism de integrare directa la nivelul sistemului de operare ce acceseaza platforma de stocare, mecanism ce va permite executarea direct din sistemul de operare a actiunilor administrative ce privesc definirea de volume si LUN-uri, redimensionarea lor fara pierderea datelor stocate, configurarea si optimizarea parametrilor de conectare la aceste volume indiferent de protocolul folosit in exportul lor. Mecanismul trebuie sa fie disponibil cel putin pentru sistemele de operare de tip server pentru care platforma de stocare trebuie sa ofere suport de conectivitate directa: Windows, Linux, VMware vSphere;
- Ca parte a functiilor de administrare si diagnosticare Platforma de stocare trebuie sa includa standard un mecanism de alertare pe e-mail, configurabil pentru un set specific de adrese e-mail si/sau catre o platforma de suport disponibila la producatorul sistemului de stocare. Deasemenea trebuie sa permita integrarea in unelte dedicate de management al infrastructurilor prin suport complet pentru protocolul SNMP versiunea 2 si 3 si

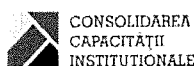

 CONSOLIDAREA
 CAPACITĂȚII
 INSTITUȚIONALE

Proiect cofinanțat din Fondul Social European prin
 Programul Operațional Capacitate Administrativă 2014-2020!



	<p>prin existenta in mod gratuit a descriptorilor si parametrilor platformei astfel incat integrarea sa se faca in mod facil in uneltele de management ce nu au implicit profile definite pentru sistemul specific oferat. Tot in scopul operatiunilor de management si diagnosticare sistemul trebuie sa integreze un set de led-uri ce afiseaza cel putin starea curenta a echipamentului;</p>
Optimizarea capacitatii de stocare	<ul style="list-style-type: none">▪ Platforma de stocare trebuie să aibă capabilitati de tip „Thin Provisioning” (alocarea către nodurile de procesare a unei capacități de stocare mai mare decât cea fizic disponibilă);▪ Platforma de stocare trebuie să asigure rebalansarea datelor pe matricile de discuri în cazul în care sunt adăugate discuri suplimentare;▪ Platforma de stocare trebuie sa includa un mecanism de instantiere a unui set de date disponibil la nivel de volum si/sau LUN, fara copierea datelor in instante multiple, ci prin folosirea unui singur set de date, dar adresabil de catre aplicatii si utilizatori ca instante complet diferite;• Platforma de stocare trebuie sa permita definirea de volume de date pe matrici ce suporta discuri in tehnologii diferite (SSD + SAS + NL-SAS), organizate in matrici cu nivele de protectie RAID diferite (Ex.: masiv format din matrici de discuri SSD in RAID 1 + discuri SAS in RAID 5 + discuri NL-SAS in RAID 6);• Platforma de stocare trebuie sa ofere nativ, fara licentiere ulterioara optiunea de prioritizare si accelerare a accesului la date in mod automat si transparent pentru aplicatiile si utilizatorii ce folosesc aceste seturi de date. Mecanismele de accelerare si prioritizare trebuie sa beneficieze de suportul hardware al unui set dedicat de discuri de mare viteza (SSD). Pentru economisirea spatiului si a costurilor asociate, sistemul trebuie sa permita instalarea lor in acelasi sertar cu un tip mai lent de discuri de la acelasi producator (SAS, spre exemplu). Pentru obtinerea celor mai buni timpi de acces si raspuns, intregul proces automat de accelerare si prioritizare trebuie realizat nu prin mecanisme de copiere/mutare a datelor pe seturi de discuri mai rapide, ci prin stocarea lor temporara la citire si la scriere in suportul hardware al acestor procese (memoria cache sau discurile SSD). Integrarea mecanismelor de accelerare si

	<p>prioritizare trebuie sa se faca transparent pentru datele stocate si aplicatiile ce acceseaza aceste date, indiferent de momentul la care se decide activarea acestor mecanisme. Deasemenea trebuie sa se integreze nativ cu restul tehnologiilor si proceselor aplicate la nivelul sistemului de stocare, respectiv asupra seturilor de date, fara a impiedica functionarea sau activarea acestora;</p>
<p>Protectia si replicarea datelor</p>	<ul style="list-style-type: none"> ▪ Platforma de stocare trebuie sa aiba incorporate baterii ce asigura protectia controller-elor si a memoriei cache la cadererile de curent prin salvarea automata a datelor din cache pe discuri dedicate flash/SSD, inainte de oprirea echipamentului; ▪ Platforma de stocare trebuie sa includa mecanisme de realizare a copiilor complete ale datelor sau bazate pe imaginea acestora la un anumit moment de timp. Spatiul rezervat copiilor de date trebuie sa poata fi configurat pe discuri separate fata de cele unde stau datele de productie. Sistemul trebuie sa permita si realizarea de copii ale oricarei copii de date. Copiile de date complete, sau bazate pe imagini, trebuie sa poata fi accesate atat in mod „citire”, cat si in mod „scriere”. Se va asigura suport pentru minim 255 de copii ale fiecarui volum de date (LUN); ▪ Suport software si hardware inclus pentru realizarea de copii de siguranță a datelor, local și la distanță, folosind o tehnologie de jurnalizare a tuturor operațiunilor de scriere, care să permită restaurarea datelor la orice moment de timp. Copiile de siguranță trebuie să poată fi grupate pe aplicație, pentru a asigura consistența recuperării aplicațiilor interdependente; ▪ Suport software si hardware inclus pentru replicarea sincrona/asincrona a datelor la distanta, intre mai multe echipamente similare. Pentru utilizarea eficientă a canalelor de comunicatie dintre centrele de date, Solutia de replicare trebuie să ofere suport pentru replicare doar a datelor modificate, precum și transmiterea numai a blocurilor de date unice (deduplicare) si compresate (compresie); ▪ Trebuie sa permita schimbarea tipului de replicare, din sincron in asincron si invers, manual sau automat pe baza anumitor reguli de performanta prestabilite (Ex.: latime de banda disponibila); ▪ Trebuie sa fie capabila sa ofere tipuri de replicare diferite (sincron, asincron), per aplicatie sau grup de aplicatii.



Proiect cofinanțat din Fondul Social European prin
Programul Operațional Capacitate Administrativă 2014-2020!

	<ul style="list-style-type: none"> ▪ Toate functionalitatile software solicitate mai sus vor fi incluse in configuratia ofertata a echipamentului de stocare, respectiv pentru intreaga capacitate de stocare ofertata, fara costuri aditionale in cazul viitoarelor extensii de capacitate de stocare;
Licentiere	<ul style="list-style-type: none"> ▪ Conectarea prin protocol iSCSI sa fie disponibila in configuratia initiala; ▪ Conectarea prin protocol NFS (v2/v3/v4) sa fie disponibila in configuratia initiala; ▪ Conectarea prin protocol CIFS (SMB2/SMB3) sa fie disponibila in configuratia initiala; ▪ Conectarea prin protocol FC sa fie disponibila in configuratia initiala; ▪ Licenta inclusa de replicare sincronă/asincronă in configuratia initiala;
Sisteme de operare suportate	<p>Platforma de stocare trebuie să suporte minim următoarele sisteme de operare:</p> <ul style="list-style-type: none"> ▪ Microsoft Windows Server 2012 R2/2016; ▪ Microsoft Hyper-V; ▪ VMware vSphere; ▪ Red Hat Enterprise Linux; <p>Platforma de stocare trebuie sa includa licentele necesare accesului sistemelor de operare suportate;</p>
Alimentare	<p>Pentru asigurarea redundantei complete a echipamentului propus fiecare element major component al platformei de stocare (controller, sasiu discuri, etc) trebuie sa ofere alimentare redundanta prin cel puțin doua surse independente de alimentare. Sursele trebuie sa ofere functionalitate hot-swap pentru inlocuirea rapida, fara oprirea alimentarii sistemului si fara intreruperea serviciilor asigurate de platforma;</p>
Ventilatie	<p>Toate elementele de asigurare a ventilatiei sistemului trebuie sa fie de tip hot-swap pentru inlocuirea lor rapida in caz de avarie, fara intreruperea functionalitatilor oferite de platforma;</p>



Handwritten signatures and initials.

Cerinte constructive	<ul style="list-style-type: none"> Platforma de stocare trebuie să fie montabilă în rack-uri standard de 19”; Ofertantul trebuie să livreze un kit cu elementele de fixare/instalare în rack (suportji, șuruburi/captive);
Garanție si suport	<ul style="list-style-type: none"> Pentru toate elementele si modulele integrate, solutia va include garantie de minim 36 de luni. Suportul si garantia trebuie asigurate in Romania de producatorul respectivelor echipamente sau prin partener autorizat; Garantia hardware va fi asigurata cu un SLA (Service Level Agreement) de 8x5xNBD (8 ore pe zi, 5 zile pe saptamana, cel mai tarziu a doua zi lucratoare – Next Business Day), care sa garanteze diagnosticarea echipamentului sau modulului defect si inlocuirea acestuia in maxim 3 zile lucratoare, fara alte costuri; Se va asigura acces 24x7 in centrul de suport al producatorului, cu posibilitatea raportarii problemelor aparute in functionare si solicitarea rezolvarii acestora in functie de severitate. De asemenea se va asigura dreptul de a face update-uri si upgrade-uri la toate componentele software (sistem de operare, firmware, etc).

4.4.1.8 Echipament de stocare de Tip 2

Platforma de stocare de Tip 2 trebuie sa indeplineasca aceleasi **specificatii tehnice minimale precum echipamentul de stocare de Tip 1.**

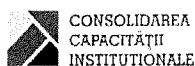
4.4.1.9 Componenta de monitorizare a dezvoltării și exploatării aplicațiilor

Componenta de monitorizare a dezvoltarii si exploatarii aplicatiilor trebuie sa indeplineasca urmatoarele **specificatii tehnice minimale:**

Caracteristica	Cerinta tehnica minimala
Instalare si configurare	<ul style="list-style-type: none"> Posibilitatea de deployment local Posibilitatea de monitorizare atat a infrastructurii locale – fizice si virtuale, cat si a infrastructurii disponibile via cloud Interfata grafica web unitara dedicata utilizatorilor, pentru management si mentenanta, cu posibilitati de monitorizare via internet browser Upgrade automatizat, fara necesitati de configurari manuale



	<ul style="list-style-type: none"> ▪ Posibilitati de vizualizare automatizata a intregii topologii de retea (fara omiterea vreunei categorii de componente) ▪ Posibilitati de identificare automatizata a: <ul style="list-style-type: none"> ○ tranzactiilor de business ○ tuturor componente in cadrul tranzactiei de business ○ sisteme tip back-end standard (baze de date, servicii web, etc.) ○ sisteme tip back-end non-standard (via configuratii tip point-and-click) ▪ Abilitatea de definire globalizata a alertelor folosind un motor de reguli integrat (versus definirea individuala per metrica) ▪ Posibilitatea de definire a unui mediu multi-tenant (chiar si in implementarea locala) ▪ Criptare SSL a traficului intre oricare sub-componente din componenta de monitorizare ▪ Profilul tranzactiilor distribuite sa poata fi realizat fara scriere/modificare de cod ▪ Componenta trebuie sa impacteze cu maxim 3% incarcarea CPU in cazul scenariilor de incarcare masiva ▪ Support pentru cel putin urmatoarele sisteme de baze de date: MS-SQL Server, MySQL, DB2, Oracle, Sybase, PostgreSQL si MongoDB ▪ Posibilitatea de monitorizare a tuturor instantelor de baze de date fara impact asupra performantelor generale la nivel de mediu/sistem ▪ Posibilitate de instalare non-invaziva - fara agenti.
Vizibilitate control si	<ul style="list-style-type: none"> ▪ Suport pentru vizualizare corelata a tranzactiilor de business distribuite intre nivele si servicii ▪ Suport pentru identificarea fiecărei componente in cadrul tranzactiilor, In scopul identificării exacte a problemelor de performanta la nivelul intregii configuratii ▪ Suport pentru diagnoza la nivel de cod (vizibilitate in cadrul claselor si metodelor) in cazul tranzactiilor cu penalitati de performanta ▪ Suport pentru monitorizarea mediului Java Virtual Machine (heap, garbage collector, generational spaces, etc.) ▪ Suport pentru monitorizare a metricelor hardware (utilizare CPU, OS memorie utilizata, disk I/O si network I/O) ▪ Suport pentru ridicarea exceptiilor si detectia erorilor de executie ▪ Sa existe facilitate de a nu se permite oprirea functionalitatii de monitorizare in situatiile de incarcare masiva a sistemului - in scopul reducerii impactului asupra aplicatiilor, tinand cont ca majoritatea problemelor apar in situatiile de incarcare masiva



	<ul style="list-style-type: none"> ▪ Componenta trebuie sa permita identificarea: <ul style="list-style-type: none"> ○ tranzactiilor de business incetinite sau stopate fara interventie manuala ○ numararea, masurarea si evaluarea fiecari tranzactii ○ tranzactiilor fara interventie manuala ○ interogarilor SQL lente fara interventie manuala ○ identificarea sistemelor back-end sau serviciilor externe fara interventie manuala ○ in regim automatizat a situatiilor tip "code deadlocks" ▪ Componenta trebuie sa ofere posibilitatea de access din interfata-utilizator catre zonele cu probleme de performanta prin intermediul alertelor cu hyper-link ▪ Componenta trebuie sa permita trimiterea de email-uri ce contin hyper-link-uri catre zonele cu probleme de performanta ▪ Componenta trebuie sa permita analiza automatizata a datelor aferente tranzactiilor integrale colectate de tip "root-cause analysis".
<p>Capabilitati de flux de lucru, reguli si alerte</p>	<ul style="list-style-type: none"> ▪ Definire fluxuri de lucru: <ul style="list-style-type: none"> ○ Creare, editare si rulare pentru intregul mediu din cadrul unui singur produs integrat ○ Definire ca o serie de activitati cu executie secventiala ○ Rularea in parallel a unei secvente de sarcini pe noduri multiple ale unui cluster ○ Utilizarea sabloanelor existente pentru sarcini comune ("startup tasks", "build/ant", "shell scripts/native tasks") ○ Crearea de sarcini tip custom si parametrizarea lor. ▪ Executie fluxuri de lucru: <ul style="list-style-type: none"> ○ Executia unui flux de lucru process din cadrul unui singur produs integrat ○ Posibilitatea de executie a unui flux de lucru printr-un singur click la nivel de utilizator ○ Executia automatizata a fluxului ca urmare a evaluarii unei regului si a unor conditii ce trebuiesc indeplinite ○ Posibilitatea de programarea a executiei unui flux la o anumita ora pentru evitarea varfurilor de incarcare ale sistemului ○ Existenta unui raport detaliat asupra statusului activitatilor/sarcinilor din cadrul fluxurilor ce se executa ▪ Motor de regului si alertare: <ul style="list-style-type: none"> ○ Existenta unei componente tip "wizard" de creare a regulilor in maniera point-and-click

	<ul style="list-style-type: none"> ○ Posibilitate de includere in analiza de multiple categorii de date ("app performance data", "machine data" si "customer provided data") ○ Posibilitate de combinare a conditiilor prin folosirea operatorilor logici booleeni AND si OR ○ Posibilitate de stopare temporara a motorului de reguli pentru operatiuni curente de mentenanta a infrastructurii sistemului ○ Generare alerte si notificari la incalcarea regulilor (email, SMS sau custom) ○ Posibilitate de combinare logica a multiple metrice in cadrul unei singure alerte.
Platforma analitica	<ul style="list-style-type: none"> ▪ Modulele aplicatiei si platforma analitica sunt disponibile in cadrul unui interfete-utilizator unitare ▪ Interfata analitica sa fie web-based (fara instalare locala de client software) ▪ Platforma analitica adreseaza intreg spectrul de date colectate la nivelul componentei/solutiei ▪ Deposit ("repository") scalabil orizontal capabil de colectare si stocare de volume mari de date aferente evenimentelor si metricelor ▪ Fara dependenta de porturi SPAN sau echipamente de mirroring a traficului (network TAPs) ▪ Mecanisme tip drill-down de navigare la nivel de context intre datele de monitorizare si cele analitice ▪ Subcomponenta de creare a interogarilor ("query buillder") disponibil in interfata grafica ▪ Adoptie Advanced Query Language ▪ Abilitatea de ajustare a scalei timpului prin mecanisme "click and drag" in cadrul unui tablou de boord ("dashboard charts") ▪ Clasarea automata (top N) a relevantei fiecarui camp indexat la sectiunea curenta ▪ Posibilitate de configurare a colectarii anumitor date/campuri aferente tranzactiilor ▪ Colectare, stocare si analiza date imediata ("in near real time") ▪ Includere de biblioteci API dedicate "Input Custom Metrics", "Analytics Events" si "Search" ▪ Posibilitatea de afisare a rezultatelor in tablouri predefinite sau tablouri definibile custom ▪ Control granular al accesului, bazat pe roluri (RBAC) ▪ Analitici la nivelul tranzactiilor:

	<ul style="list-style-type: none"> ○ Abilitatea de colectare si stocare a tranzactiilor de business de la nodurile monitorizate ○ Abilitatea de filtrare parametrizabila a tranzactiilor utilizand o interfata grafica de definire a interogariilor ("graphical query builder") ○ Identificarea tuturor tranzactiilor la nivel de utilizator intr-o perioada de timp definibila utilizand ca si criteriu de cautare un ID, o adresa email sau alti identificatori unici ▪ Analitici la nivel de fisiere tip "log file": <ul style="list-style-type: none"> ○ Abilitatea de colectare si stocare a fisierelor log de la nodurile monitorizate ○ Posibilitate de logging via TCP ○ Posibilitatea de auto-injectare a identicatorului BT pentru fiecare element al fisierului log ○ Abilitatea de filtrare a rezultatelor utilizand o componenta de interogare pe baza de text si/sau o interfata grafica de definire a interogariilor ("graphical query builder") ○ Abilitatea de extragere a oricarui camp din fisierul de log in vederea procesarii.
Integrare	<ul style="list-style-type: none"> ▪ Integrare cu componenta de monitorizare a accesului la date ▪ Integrare cu componenta de monitorizare a serviciilor.
Garanție si suport	<ul style="list-style-type: none"> ▪ Solutia va include garantie de minim 36 de luni. Suportul si garantia trebuie asigurate in Romania de producatorul respectivei solutii sau prin partener autorizat; ▪ Garantia va fi asigurata cu un SLA (Service Level Agreement) de 8x5xNBD (8 ore pe zi, 5 zile pe saptamana, cel mai tarziu a doua zi lucratoare – Next Business Day); ▪ Se va asigura acces 24x7 in centrul de suport al producatorului, cu posibilitatea raportarii problemelor aparute in functionare si solicitarea rezolvarii acestora in functie de severitate. De asemenea se va asigura dreptul de a face update-uri si upgrade-uri software.

4.4.1.10 Componenta de monitorizare a accesului la date

Componenta de monitorizare a accesului la date trebuie sa indeplineasca urmatoarele **specificatii tehnice minime**:

Caracteristica	Cerinta tehnica minimala
----------------	--------------------------

<p>Capabilitati generale</p>	<ul style="list-style-type: none"> ▪ Componenta dedicate de monitorizare a accesului la date si a nivelului de performanta a sistemelor de baze de date implementate local sau disponibile via servicii tip cloud ▪ Componenta trebuie sa o imagine de ansamblu in timp real asupra activitatii curente legata de bazele de date ▪ Componenta ofera suport pentru alertare static si dinamica privind metricile colectate de la bazele de date functionale ▪ Componenta dispune de capabilitati de evidentiere a tendintelor de utilizare si performanta a sistemelor de baze de date pe perioade de timp configurabile ▪ Componenta dispune de capabilitati de monitorizare continua a activitatilor legate de baze de date in medii de productie cu volume mari de date
<p>Instalare si configurare</p>	<ul style="list-style-type: none"> ▪ Componenta ofera suport pentru multiple platforme, precum: <ul style="list-style-type: none"> ○ Sisteme de operare: Microsoft Windows, distributii Linux, Solaris, AIX. ○ Sisteme de baze de date relationale/non-relationale: cel putin Microsoft SQL, Oracle Database, MySQL, IBM DB2, Sybase, Mongo DB, Couchbase. ○ Clienti: cel putin Internet Explorer, Mozilla Firefox, Chrome, Safari. ▪ Monitorizare a tuturor instantelor de baze de date fara impact asupra performantelor generale la nivel de mediu/sistem ▪ Implementeaza o arhitectura non-invaziva de tip zero-agenti care scuteste beneficiarii de operatiuni de instalare/configurare/mentenanta pe serverele de baze de date ▪ Suport pentru instalare si configurare facila in mediile de productie, atat locale cat si cele cu componente externalizate via cloud ▪ Suport de monitorizare a oricate instante de baze de date, nelimitand astfel un potential beneficiar cu nevoi majore de scalare a mediilor operationale
<p>Capabilitati de analiza aprofundata</p>	<ul style="list-style-type: none"> ▪ Suport pentru istoricizare, prin intermediul monitorizarii si retentiei datelor in proportie de 100% ▪ Include rapoarte de baza privind activitatea bazelor de date, cel putin "Top SQL", "Top Users" si "Top Programs"

	<ul style="list-style-type: none"> ▪ Suport pentru identificarea profilurilor/tendintelor de evolutie aferente activitatii bazelor de date in timp ▪ Colectare si stocare a: <ul style="list-style-type: none"> ○ tuturor evenimentelor tip "wait" si corelarea acestora cu procedurile SQL/stocate ○ indicatorii de performanta asociati procedurilor SQL/stocate, ce putin "CPU", "Count" si Reads/Writes ○ statistici la nivel de instanta DB, cel putin "table size", "row count" si indexes" ○ indicatorii de performanta asociati serverelor de baze de date, ce putin "CPU", "Count" si Reads/Writes ▪ Posibilitatea de evidentiere a latentei componentelor procedurilor stocate ▪ Includere de rapoarte de performanta comparate ▪ Colectarea informatiilor aferente "SQL Explain" si "Execution plan" ▪ Colectarea si stocarea datelor privind performanta obiectelor bazei de date precum scheme, tabele si indecsi ▪ Colectarea indicatorilor de performanta asociati bazelor de date si corelarea acestor informatii cu resursele de procesare si stocare ale serverelor
<p>Management si monitorizare a bazelor de date</p>	<ul style="list-style-type: none"> ▪ Evidentierea in timp real a performantei activitatii aferente bazelor de date ▪ Includerea unui tablou de bord tip multi-instanta pentru crearea unei vederi de ansamblu la nielul tuturor instanțelor de baze de date ▪ Abilitatea de trimitere de alerte pro-active aferente nivelelor de performanta a bazelor de date ▪ Includerea unui modul complex de raportare (aferente monitorizarii si performantei bazelor de date) atat pentru personal tehnic cat si pentru management ▪ Posibilitate de export date catre aplicatii externe (3rd party).
<p>Detectie anomalii si remediere</p>	<ul style="list-style-type: none"> ▪ Componenta ofera suport pentru evidentierea impactului direct al penalitatilor de performanta ale bazei de date la nivelul intregii aplicatii ▪ Componenta ofera suport pentru vizualizarea dependintelor intre nivelul instanțelor bazelor de date si celelalte niveluri (aplicatie, retea, server) ▪ Componenta ofera suport pentru remedierea rapida a sistemelor de baze de date oferind metrice si informatie relevanta de diagnoza

	<ul style="list-style-type: none"> ▪ Componenta ofera suport pentru identificarea apelurilor JDBC cu impact direct in performanta generala a aplicatiei/serviciului ▪ Componenta include algoritmi tip self-learning care calculeaza dinamic nivelul de performanta al sistemelor de baze de date si ofera suport in detectia anomaliilor ▪ Pentru diagnosticarea problemelor de performanta, componenta dispune de capabilitati tip Drill-Down disponibile intr-o interfata centralizata de analiza ▪ Componenta ofera suport pentru vizibilitate in metricile asociate bazei de date prin mecanisme de drill-down corelate cu contextul transactional de business
Integrare	Integrare cu componenta de monitorizare a serviciilor.
Garantie si suport	<ul style="list-style-type: none"> ▪ Solutia va include garantie de minim 36 de luni. Suportul si garantia trebuie asigurate in Romania de producatorul respectivei solutii sau prin partener autorizat; ▪ Garantia va fi asigurata cu un SLA (Service Level Agreement) de 8x5xNBD (8 ore pe zi, 5 zile pe saptamana, cel mai tarziu a doua zi lucratoare – Next Business Day); ▪ Se va asigura acces 24x7 in centrul de suport al producatorului, cu posibilitatea raportarii problemelor aparute in functionare si solicitarea rezolvarii acestora in functie de severitate. De asemenea se va asigura dreptul de a face update-uri si upgrade-uri software.

4.4.1.11 Componenta de monitorizare a serviciilor

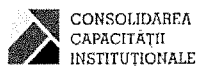
Componenta de monitorizare a serviciilor trebuie sa indeplineasca urmatoarele **specificatii tehnice** minimale:

Caracteristica	Cerinta tehnica minimala
Analiza aprofundata a traficului	<ul style="list-style-type: none"> ▪ Capabilitati de monitorizare in timp real a performantei serviciilor si securitate a rețelei bazate pe un motor de tip Machine Learning ▪ Suport pentru analiza aprofundata si corelata a intregului traficului la nivelul rețelei, dispunand de capabilitati precum "transaction analysis", "full-content analysis", "full-stream reassembly", "multi-packets", "deep-packet inspection", integrare cu NetFlow si incorporare de probe pentru captarea traficului la nivelul rețelei. ▪ Suport pentru o raportare care sa ofere o imagine dinamica de ansamblu dpdv securitate cibernetica a internetului

	<ul style="list-style-type: none"> ▪ Suport pentru identificarea si categorisirea traficului de date la nivelul rețelei in mod automatizat ▪ Suport pentru cel puțin 50 de protocoale sic el puțin 3500 metrici asociate analizei correlate aferente acestor protocoale ▪ Suport pentru creare/customizarea de metrici, tablouri de bord, decodare la nivel de protocol (UPA) si integrare de date pe baza Open Data Stream ▪ Suport pentru lucrul cu pachete de date pierdute sau fragmentate la nivelul rețelei ▪ Suport pentru lucrul cu date la nivelele L2-L7 ale rețelei (adrese IP si MAC, utilizatori, URI, fisiere) ▪ Suport pentru analiza tip top-dows si bottom-up dintr-o singura interfata, in regim de flux de lucru ▪ Suport pentru inspectia traficului in timp real, inainte de scrierea pe disk ▪ Suport pentru monitorizarea traficului la nivel de utilizator (Real User Monitoring) ▪ Suport complet pentru decriptarea SSL ▪ Suport pentru minim 1 Gbps capacitate de trafic si analiza a datelor
<p>Monitorizare echipamente server</p>	<ul style="list-style-type: none"> ▪ Suport pentru dignoza corelata a serverelor, pe baza de metrici si mecanisme tip drill-down ▪ Suport pentru monitorizarea serverelor in mod orientat per aplicatie/serviciu ▪ Suport pentru organizarea schemei asociata serverelor pe nivele ierarhice, cel puțin data center -> rack - > servers ▪ Suport pentru vizualizarea informatiilor de baza precum CPU, memorie si latime de banda consumata pentru toate serverele monitorizate, in cadrul unui tablou de bord ▪ Suport pentru vizualizarea informatiilor detaliate asociate proceselor ce ruleaza pe servere ▪ Suport pentru vizualizarea informatiilor de tip fire de executie, CPU si memorie consumata de procese ▪ Suport pentru definirea regulilor si politicilor de automatizare a solutionarii problemelor si a penalitatilor de de performanta asociate serverelor/proceselor in executie ▪ Suport pentru integrarea cu sisteme de alertare, cel puțin ServiceNow, PagerDuty si JIRA ▪ Suport pentru verificarea disponibilitatii precum si metrice minimale de performanta asociate serviciilor HTTP care nu sunt monitorizate de agentii componentei



	<ul style="list-style-type: none"> ▪ Suport pentru alertare privind timpul de raspuns HTTP pe baza unei validari personalizabile ▪ Suport pentru monitorizarea echipamentelor tip mainframe sau load balancers ▪ Suport extins pentru monitorizarea containerelor, minim Docker si VMware vSphere ▪ Capabilitati de monitorizare, ce putin "Machine availability", "CPU usage", "Disk performance", "Volume usage", "Machine load", "Memory", "SWAP", "Processes", "Network Adapter(s)", "Dynamic Baselineing", "Synthetic page checker" ▪ Suport pentru monitorizarea a cel puțin urmatoarelor platforme tehnologice Linux, UNIX, MS-Windows, VM ▪ Suport pentru istoricizarea datelor de performanta si evolutie in timp ▪ Suport pentru evidentierea imaginii de ansamblu la nivelul intregii arhitecturi corelata cu tranzactiile de business ▪ O singura interfata la nivel de utilizator pentru monitorizarea serverelor si a aplicatiilor ce ruleaza peste acestea ▪ Posibilitati de alertare bazate pe orice metrica ▪ Posibilitati de alertare la devierile de la nivelele standard de performanta.
Monitorizare retea	<ul style="list-style-type: none"> ▪ Suport pentru vizualizarea performantei intregii retele relative la contextual aplicatiei/serviciului ▪ Suport pentru auto-descoperirea/identificarea topologiei retelelor si a inter-dependintelor, incluzand echipamente tip reverse proxy si/sau load balancers ▪ Suport de centralizare/agregare a informatiilor de infrastructura aferente retelei locale si a celor externalizate via servicii de cloud ▪ Suport pentru diagnoza rapida a problemelor retelei si/sau penalitatilor de performanta ale acesteia inainte ca impactul sa afecteze aplicatiile/serviciile ▪ Suport pentru escalarea problemelor catre personalul dedicat (organizat in echipe multiple) ▪ Suport pentru identificarea latentei, congestiei sau micro-burst-urilor de retea ▪ Suport pentru monitorizarea indicatorilor de performanta asociati retelei precum throughput, packet loss, si RT rates ▪ Suport colaborativ pentru echipele de DevOps prin: <ul style="list-style-type: none"> ○ capabilitati de escalare a problemelor asociind informativ de diagnoza pe baza careia se pot demara actiuni de remediere



	<ul style="list-style-type: none"> ○ îmbunătățirea practicilor în scrierea de cod ce conduc spre optimizarea performanțelor rețelei ○ diagnoza a problemelor de rețea în medii precum highly distributed microservices sau aplicații SOA
<p>Monitorizarea la nivel de utilizator</p>	<p>Capabilități pentru platforme web:</p> <ul style="list-style-type: none"> ▪ suport pentru browsere atât pentru desktop cât și pentru mobil ▪ monitorizare a tuturor cererilor de pagini, AJAX și/sau iFrame ▪ suport pentru aplicații tip single-page ▪ detecție automatizată a erorilor JavaScript ▪ afișare timp de răspuns pe Geo Map ▪ colectare și afișare date Navigation Timing API/ Resource Timing API pentru cererile cu penalități de performanță ▪ corelarea tranzacțiilor web cu tranzacțiile din zona de server pentru analiză tip drill-down ▪ oferirea de informații la nivel de browser ("browser traces") pentru slabă performanță sau cererile utilizatorilor ▪ oferirea de analitice privind tipul și versiunea browserelor ▪ oferirea de analitice privind tipul sistemului de operare și echipamentul ▪ oferirea de analitice personalizabile pentru analiză și diagnoză ▪ oferirea de metrice privind cache-ul pentru fiecare cerere de pagină ▪ evidențierea timpului de răspuns al serverului pentru fiecare cerere de pagină ▪ corelare prin mecanisme drill-down pentru problemele de performanță ale cererilor de pagini cu zona de server în scopul unei diagnoze eficiente ▪ monitorizare la nivel de sesiune (tracking) ▪ abilitatea de generare de cereri de pagină sintetice ▪ includerea unei librării (SDK) de suport a oricărui framework pentru single-page applications ▪ validare a experienței utilizatorilor cu nivelul de performanță al aplicației ▪ includerea unui modul de raportare în interfața utilizator pentru zona de experiență a utilizatorilor ▪ date utilizator disponibile la nivel de sesiune sau cerere de pagină ▪ posibilitate de grupare de pagini la nivel root <p>Capabilități pentru platforme mobile:</p> <ul style="list-style-type: none"> ▪ suport pentru aplicații mobile și browsere pentru platforme mobile

[Handwritten signature]

[Handwritten signature]

	<ul style="list-style-type: none"> ▪ vizualizare a performantei aplicatiilor mobile, a erorilor HTTP sau de retea ▪ vizualizare a performantei API calls din aplicatia mobile in zona de server ▪ support pentru exceptii si intreruperi in monitorizare (track crashes) ▪ oferirea de analytice privind intreruperile (crashes) ▪ monitorizarea utilizatorilor pe baza de breadcrumbs ▪ monitorizarea tranzactiilor de la echipament la zona de server ▪ corelarea tranzactiilor mobile cu zona de server pentru analiza tip drill-down ▪ oferirea de informatii privind utilizarea si performanta bazata pe: <ul style="list-style-type: none"> ▪ tipul echipamentului ▪ tipul sistemului de operare ▪ versiunea sistemului de operare ▪ includerea unei interfete utilizator centralizate pentru diagnoza problemelor de mobil si celor de server.
Garantie si suport	<ul style="list-style-type: none"> ▪ Pentru toate elementele si modulele integrate, solutia va include garantie de minim 36 de luni. Suportul si garantia trebuie asigurate in Romania de producatorul respectivelor echipamente sau prin partener autorizat; ▪ Garantia hardware va fi asigurata cu un SLA (Service Level Agreement) de 8x5xNBD (8 ore pe zi, 5 zile pe saptamana, cel mai tarziu a doua zi lucratoare – Next Business Day), care sa garanteze diagnosticarea echipamentului sau modulului defect si inlocuirea acestuia in maxim 7 zile lucratoare, fara alte costuri; ▪ Se va asigura acces 24x7 in centrul de suport al producatorului, cu posibilitatea raportarii problemelor aparute in functionare si solicitarea rezolvarii acestora in functie de severitate. De asemenea se va asigura dreptul de a face update-uri si upgrade-uri software (sistem de operare, firmware, etc).

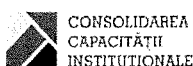
4.4.1.12 Componenta de analiză și testare de securitate a aplicațiilor

Componenta de analiză și testare de securitate a aplicațiilor trebuie să îndeplinească următoarele specificații tehnice minime:

Caracteristica	Cerinta tehnica minimala
----------------	--------------------------

Analiză Vulnerabilități

- Soluția trebuie să permită monitorizarea continuă și concurența a posturilor de securitate a aplicațiilor dezvoltate, oferind mecanisme de evaluare continuă a riscului cel puțin pentru:
 - Vulnerabilitățile nou descoperite;
 - Metricile de identificare a modificărilor și îmbunătățirilor măsurilor de securitate pentru o perioadă de tip definibilă;
 - Detectia și evaluarea automată a schimbărilor de cod efectuate asupra aplicațiilor web;
- Soluția trebuie să permită verificarea și prioritizarea rezultatelor proceselor de analiză a codului pentru eliminarea rezultatelor de tip "false positive", respectiv pentru a eficientiza procesul de remediere a vulnerabilităților, cel puțin prin următoarele mecanisme:
 - Vulnerabilitățile trebuie să poată fi prioritizate în funcție de risc, pentru a putea remedia eficient vulnerabilitățile cu grad ridicat de risc;
 - Notificări și recomandări de acțiuni ce pot fi întreprinse pentru a remedia vulnerabilitățile detectate;
 - Eliminarea automată și/sau manuală a rezultatelor de tip "false positive" pentru a economisi timpul și resursele dedicate procesului de analiză;
- Soluția trebuie să permită urmărirea în timp real și/sau bazată pe istoricul asociat unei perioade definibile de timp, a tuturor datelor ce tin de gradul de risc, cel puțin prin următoarele mecanisme:
 - Panou de afișare unificat pentru evaluarea expunerii la risc, respectiv progresul de remediere a fiecărei vulnerabilități identificate și asociate gradului respectiv de risc;
 - Comparări ale profilului de securitate asociat instituției raportat la profilele altor instituții/companii similare (în funcție de mărime, tip de industrie, etc);
 - Vizibilitate asupra întregului set de aplicații cu identificarea aplicațiilor cel mai puțin securizate, respectiv cele mai securizate;
- Soluția trebuie să permită analiza codului din punct de vedere al posturilor de securitate în orice punct al procesului de dezvoltare a aplicațiilor (chiar și pentru cod parțial dezvoltat);
- Soluția trebuie să suporte o mare varietate de limbaje de programare: .NET, Java, PHP, ASP, ColdFusion, Perl, etc;



Proiect cofinanțat din Fondul Social European prin
Programul Operațional Capacitate Administrativă 2014-2020!

	<ul style="list-style-type: none">▪ Solutia trebuie sa permita programarea rularii mecanismelor de evaluare si analiza a codului in functie de parametrii de timp si/sau la cerere;▪ Solutia trebuie sa permita scanarea codului sursa la origine (in locatiile interne institutiei/companiei), respectiv la distanta (in locatiile in care functioneaza – servere de aplicatii, servere de baze de date, etc ce ruleaza in alte locatii decat cele interne institutiei/companiei);▪ Solutia trebuie sa permita mecanisme rapide de scanare a codului sursa;▪ Solutia trebuie sa permita identificarea rapida a tuturor aplicatiilor/artefactelor de aplicatie in structura completa a serverelor de aplicatii web, atat pentru servere interne cat si pentru servere externe;▪ Solutia trebuie sa permita prioritizarea aplicatiilor si a proceselor de analiza a vulnerabilitatilor in functie de gradul de risc relevant pentru fiecare departament al institutiei/companiei;▪ Solutia trebuie sa permita procese personalizabile de testare a codului sursa de aplicatie in urma remedierii vulnerabilitatilor cel putin prin analiza introducerii de date in aplicatie, analiza cererilor de schimbare de stare a aplicatiei, analiza functionalitatilor critice;▪ Solutia trebuie sa asigure integritatea codului sursa al aplicatiilor analizate prin injectarea de cod benign in locul codului sursa de aplicatie;▪ Solutia trebuie sa permita remedierea vulnerabilitatilor folosind urmatoarele metode/mecanisme:<ul style="list-style-type: none">▪ Utilizarea unor segmente precise de cod;▪ Oferirea unui set de librarii si actualizari (patch-uri) gata dezvoltate de producatorul solutiei oferite pentru un numar cat mai mare de vulnerabilitati;▪ Testarea/re-testarea nelimitata a aplicatiilor si codului sursa;▪ Integrarea nativa cu solutiile de protectie a serviciilor de aplicatie (in speta cu solutia de protectie a serviciilor de aplicatie oferita);
Performanțele analizei	<ul style="list-style-type: none">▪ Solutia nu trebuie sa introduca nici un fel de latenta si/sau penalizare de performanta in functionarea aplicatiilor ce sunt analizate din perspectiva vulnerabilitatilor, prin posibilitatea personalizarii extensive a procesului de analiza;

Integrare	<ul style="list-style-type: none">▪ Soluția trebuie să permită integrarea nativă cu uneltele uzuale folosite de dezvoltatori, indiferent de limbajul de programare folosit în dezvoltarea codului sursă:<ul style="list-style-type: none">▪ Integrări native cu medii de dezvoltare uzuale: Eclipse, Xcode, Visual Studio, IntelliJ, etc – Detaliile despre vulnerabilitățile identificate trebuie să fie disponibile direct din mediul de dezvoltare;▪ Integrări native cu sistemele uzuale de management al erorilor de cod: Atlassian Jira – Trebuie să permită deschiderea automată a tichetelor de urmărire a erorilor de cod în urma procesului de detecție a vulnerabilităților, respectiv închiderea tichetelor de urmărire a erorilor de cod în urma procesului de remediere a vulnerabilităților;▪ Integrări native cu sistemele uzuale de tip repository de cod: Git, SVN, Perforce, CVS, TFS, etc – Trebuie să permită procesele de evaluare și analiză a vulnerabilităților direct din aceste repository, fără descărcarea prealabilă a codului sursă;▪ Integrări native cu sistemele uzuale de management al dependințelor: Jenkins, Nuget, Maven, Gradle, etc – Trebuie să permită rezolvarea automată a dependințelor de cod, pentru a putea fi incluse în procesele de analiză și evaluare a vulnerabilităților codului sursă, respectiv trebuie să permită analiză individuală a fiecărei librării terțe de cod inclus, cel puțin din perspectiva licențierii, valabilității și versiunii (cu indicarea posibilităților și versiunilor de actualizare în vederea reducerii vulnerabilităților și gradului de risc asociat);▪ Integrări native cu sistemele uzuale de management al ciclului de viață al aplicațiilor: Atlassian Jira, Borland StarTeam, HP ALM, HP Quality Center, IBM Rational Team Concert, IBM Rational Requirements Composer, Microsoft Team Foundation Server, ThoughtWorks Mingle, Rally, VersionOne, Bugzilla, Serena Business Manager, ServiceNow, etc – Trebuie să permită integrarea bi-direcțională a artefactelor de securitate (vulnerabilități detectate, status remediere, grad de risc, etc) oferite de soluția propusă;▪ Integrările native cu sistemele enumerate trebuie să se realizeze pe baza standardelor deschise (Open API), astfel încât soluția oferită
-----------	---

	<p>sa permita extinderea ulterioara cu sisteme ce suporta respectivele standarde, fara a impune limitari de licentiere si functionalitate;</p> <ul style="list-style-type: none"> ▪ Solutia trebuie sa fie compatibila si sa permita integrarea nativa in procesele de certificare PCI DSS la nivelul proceselor de analiza si evaluare a vulnerabilitatilor, respectiv la nivelul proceselor de remediere si raportare;
Identificarea vulnerabilităților din surse multiple	<ul style="list-style-type: none"> ▪ Solutia trebuie sa asigure actualizarea semnăturilor și informațiilor despre vulnerabilități în mod automat; ▪ Solutia trebuie sa permita introducerea manuală a definițiilor inclusiv a celor definite de administratori;
Administrare sistem	<ul style="list-style-type: none"> ▪ Solutia trebuie sa asigure crearea rolurilor de administrare și a drepturilor aferente acestora pentru setarea politicilor de scanare și controlul priorităților; ▪ Solutia trebuie sa includă politici de analiză și scanare asociabile unor grupuri de active, pentru a realiza analiză de context; ▪ Solutia trebuie sa permită rularea scanărilor în mod manual sau automat inclusiv configurarea și definirea unor intervale de scanare a activelor sau a grupurilor de active; ▪ Solutia trebuie sa asigure administrarea prin intermediul unei interfețe web care permite modificarea informațiilor afișate în funcție de necesități. Accesul la interfața grafică se va realiza în mod securizat, prin protocol SSL;
Clasificarea activelor	<ul style="list-style-type: none"> ▪ Solutia trebuie sa asigure definirea unei structuri ierarhice de grupuri de active; ▪ Solutia trebuie sa permita realizarea de clasificări pe diverse criterii (de exemplu criteriul organizațional, topologic, geografic sau la nivel de sistem);
Raportare	<ul style="list-style-type: none"> ▪ Solutia trebuie sa furnizeze rapoarte per activ sau grup de active pentru următoarele nivele ierarhice: ▪ Rapoarte pentru managementul de top; ▪ Rapoarte pentru managementul secundar; ▪ Rapoarte pentru tehnicieni; ▪ Solutia trebuie sa asigure capabilități de notificare prin e-mail; ▪ Solutia trebuie sa asigure emiterea rapoartelor în mod programat sau rularea ad-hoc a acestora; ▪ Solutia trebuie sa asigure furnizarea de rapoarte de remediere;

	<ul style="list-style-type: none">▪ Soluția trebuie să asigure emiterea de rapoarte privitoare la tendințele de schimbare privind managementul vulnerabilităților;▪ Soluția trebuie să asigure stabilirea unei linii de bază și urmărirea evoluției în timp a vulnerabilităților existente (emiterea de rapoarte ce evidențiază diferențele identificate între sesiuni de scanare separate în timp);▪ Soluția trebuie să furnizeze informații suplimentare despre vulnerabilitățile identificate: descriere, criticitate, risc, identificator specific producătorului, metode pentru remediere (inclusiv patch-uri software, configurări de administrare sau căi alternative destinate acoperirii vulnerabilităților detectate);▪ Soluția trebuie să dispună de șabloane de raportare predefinite și de posibilitatea de creare a altor șabloane personalizate;▪ Rapoartele să poată fi exportate cel puțin în format PDF și CSV;▪ Gruparea și repartizarea automată/definibilă a rapoartelor în funcție de tipul raportului, domeniului de interes, departamentului, gradului de risc, tipului de aplicație, etc;▪ Capabilități avansate de raportare cu posibilitatea urmăririi continue a tendințelor și parametrilor cheie (rate de remediere, timpul de rezolvare a vulnerabilităților, timpul de viață al vulnerabilităților, etc);▪ Generarea unor indecsi de securitate pentru fiecare tip de aplicație analizată;▪ Generarea unor liste de atacuri posibile relativ la fiecare vulnerabilitate descoperită;
Garanție și suport	<ul style="list-style-type: none">▪ Soluția va include garanție de minim 36 de luni. Suportul și garanția trebuie asigurate în România de producătorul respectivei soluții;▪ Garanția va fi asigurată cu un SLA (Service Level Agreement) de 8x5xNBD (8 ore pe zi, 5 zile pe săptămână, cel mai târziu a doua zi lucrătoare – Next Business Day);▪ Se va asigura acces 24x7 în centrul de suport al producătorului, cu posibilitatea raportării problemelor aparute în funcționare și solicitarea rezolvării acestora în funcție de severitate. De asemenea se va asigura dreptul de a face update-uri și upgrade-uri la toate componentele software.

4.4.1.13 Componenta de analiză și remediere a vulnerabilităților de securitate

Se va livra o componenta de analiză și remediere a vulnerabilităților de securitate, cu modul de identificare automată și catalogare a tuturor activelor autorității contractante, plus toate licențele aferente, ce va îndeplini următoarele **specificatii tehnice minimale**:

Caracteristica	Cerinta tehnica minimala
Analiză Vulnerabilități	<ul style="list-style-type: none"> ▪ Soluția trebuie să permită instalarea motorului de scanare cel puțin pe următoarele sisteme de operare: <ul style="list-style-type: none"> ▪ Microsoft Windows Server 2012 R2/2016; ▪ RedHat Enterprise Linux 6/7; ▪ Trebuie să ruleze fără a necesita instalarea unui agent pe activele existente în rețea (agentless); ▪ Trebuie să permită rularea de fișiere de comenzi (script-uri și API-uri) personalizate fără actualizarea codului aplicației; ▪ Trebuie să asigure emularea atacurilor informatice: capacitatea de a efectua teste de penetrare într-o manieră neinvazivă sau invazivă, în scopul analizei efectelor unor atacuri reale. Se va asigura integrarea cu o soluție de exploatare a vulnerabilităților care va fi inclusă în soluția pentru managementul vulnerabilităților oferată; ▪ Trebuie să asigure automatizarea procesului de identificare, prioritizare, analiză și indicații pentru remedierea vulnerabilităților, prin validarea acestora cu soluția de exploatare a vulnerabilităților oferată; ▪ Trebuie să asigure rularea de scanări pentru identificarea vulnerabilităților rețelei și ale sistemelor existente (Active discovery scan); ▪ Trebuie să asigure prioritizarea scanărilor și a analizei în funcție de criticitatea activelor identificate în rețea; ▪ Trebuie să asigure scanarea sistemelor ce dețin adrese IPv4 și IPv6; ▪ Trebuie să fie validată și aprobată PCI Council Approved Scanning Vendor (ASV);
Performanțele analizei	<ul style="list-style-type: none"> ▪ Soluția trebuie să asigure scanarea unui număr nelimitat de segmente de rețea diferite; ▪ Soluția trebuie să asigure scanarea unui număr nelimitat de IP-uri diferite;

Handwritten signature

Handwritten signature

	<ul style="list-style-type: none"> Soluția trebuie să suporte un număr nelimitat de motoare de scanare;
Identificarea vulnerabilităților din surse multiple	<ul style="list-style-type: none"> Soluția trebuie să asigure actualizarea semnăturilor și informațiilor despre vulnerabilități în mod automat; Soluția trebuie să asigure importul de definiții Microsoft Group Policy; Soluția trebuie să asigure capacitatea de a integra vulnerabilități indicate de sistemele IPS; Soluția trebuie să permită introducerea manuală a definițiilor inclusiv a celor definite de administratori;
Administrare sistem	<ul style="list-style-type: none"> Soluția trebuie să asigure crearea rolurilor de administrare și a drepturilor aferente acestora pentru setarea politicilor de scanare și controlul priorităților; Soluția trebuie să includă politici de analiză și scanare asociabile unor grupuri de active, pentru a realiza analiză de context; Soluția trebuie să permită rularea scanărilor în mod manual sau automat inclusiv configurarea și definirea unor intervale de scanare a activelor sau a grupurilor de active; Soluția trebuie să asigure administrarea prin intermediul unei interfețe web care permite modificarea informațiilor afișate în funcție de necesități. Accesul la interfața grafică se va realiza în mod securizat, prin protocol SSL;
Identificarea și urmărirea activelor	<ul style="list-style-type: none"> Soluția trebuie să scaneze și să identifice cel puțin: <ul style="list-style-type: none"> Software de bază pentru echipamente de rețea (routere, switch-uri); Sisteme de operare pentru desktop-uri și servere (cel puțin Microsoft Windows XP, 7, 8.x, 10, Server 2003, 2008, 2008 R2, 2012, 2012 R2, 2016, Red Hat Enterprise Linux, Oracle Linux și Solaris); Echipamente de tip IDS/IPS; Echipamente de tip firewall; Aplicații de tip baze de date (cel puțin Microsoft SQL Server 2005, 2008, 2012, MySQL, Oracle, IBM DB2 și PostgreSQL); Servere și servicii web, cel puțin Microsoft IIS și Apache; Funcționalitatea trebuie să fie disponibilă pentru utilizare fără o configurare specială (out of the box);

Handwritten signature

Handwritten signature

<p>Tehnici de identificare a activelor</p>	<p>Soluția trebuie să suporte cel puțin următoarele tehnici de identificare a activelor:</p> <ul style="list-style-type: none"> ▪ Ping sweep; ▪ UDP probe; ▪ Asset fingerprinting; ▪ Rapid discovery; ▪ NetBIOS-based discovery; ▪ TCP discovery; ▪ UDP port discovery; ▪ OS fingerprinting; ▪ Application fingerprinting; ▪ Integrated NMAP database;
<p>Clasificarea activelor</p>	<ul style="list-style-type: none"> ▪ Soluția trebuie să asigure definirea unei structuri ierarhice de grupuri de active; ▪ Soluția trebuie să asigure importul din Active Directory; ▪ Soluția trebuie să permită realizarea de clasificări pe diverse criterii (de exemplu criteriul organizațional, topologic, geografic sau la nivel de sistem);
<p>Raportare</p>	<ul style="list-style-type: none"> ▪ Soluția trebuie să furnizeze rapoarte per activ sau grup de active pentru următoarele nivele ierarhice: <ul style="list-style-type: none"> ▪ Rapoarte pentru managementul de top; ▪ Rapoarte pentru managementul secundar; ▪ Rapoarte pentru tehnicieni; ▪ Soluția trebuie să asigure capabilități de notificare prin e-mail; ▪ Soluția trebuie să asigure emiterea rapoartelor în mod programat sau rularea ad-hoc a acestora; ▪ Soluția trebuie să asigure furnizarea de rapoarte de remediere; ▪ Soluția trebuie să asigure emiterea de rapoarte privitoare la tendințele de schimbare privind managementul vulnerabilităților; ▪ Soluția trebuie să asigure stabilirea unei linii de bază și urmărirea evoluției în timp a vulnerabilităților existente (emiterea de rapoarte ce evidențiază diferențele identificate între sesiuni de scanare separate în timp); ▪ Soluția trebuie să furnizeze informații suplimentare despre vulnerabilitățile identificate: descriere, criticitate, risc, identificator specific producătorului, metode pentru remediere (inclusiv patch-uri

	<p>software, configurări de administrare sau căi alternative destinate acoperirii vulnerabilităților detectate);</p> <ul style="list-style-type: none"> ▪ Solutia trebuie sa dispună de șabloane de raportare predefinite și de posibilitatea de creare a altor șabloane personalizate; ▪ Rapoartele să poată fi exportate cel puțin în format PDF și CSV;
Garanție și suport	<ul style="list-style-type: none"> ▪ Solutia va include garanție de minim 36 de luni. Suportul și garanția trebuie asigurate în România de producătorul respectivei soluții; ▪ Garanția va fi asigurată cu un SLA (Service Level Agreement) de 8x5xNBD (8 ore pe zi, 5 zile pe săptămână, cel mai târziu a doua zi lucrătoare – Next Business Day); ▪ Se va asigura acces 24x7 în centrul de suport al producătorului, cu posibilitatea raportării problemelor aparute în funcționare și solicitarea rezolvării acestora în funcție de severitate. De asemenea se va asigura dreptul de a face update-uri și upgrade-uri la toate componentele software.

4.4.1.14 Componenta de analiză a accesării și utilizării resurselor

Componenta de analiză a accesării și utilizării resurselor trebuie să îndeplinească următoarele specificații tehnice minime:

Caracteristica	Cerința tehnică minimă
Capabilități tehnice	<p>Soluția permite valorificare inteligentă a datelor maritor de audit generate la nivel de sesiune utilizator:</p> <ul style="list-style-type: none"> ▪ Indexarea textului care apare pe ecran, inclusiv la nivelul imaginilor, în sesiuni de tip remote desktop sau în aplicații Java; ▪ Capabilități de căutare, inclusiv identificarea utilizatorilor care au văzut pe ecran un anume text, respectiv redarea înregistrării sesiunilor de lucru la nivel de desktop în care acesta a apărut; ▪ Posibilitatea de a căuta prin identificarea exactă a textului, ca atare, sau prin utilizarea de simboluri și formule specializate, inclusiv de tip wildcard, și expresii regulate ▪ Posibilitatea de a formula reguli care determină o anumită acțiune, în funcție de textul care apare pe ecran, inclusiv în ceea ce privește mascarea parțială a textului în înregistrări, sau, după caz, oprirea unei aplicații și blocarea accesului utilizatorului la aceasta, respectiv cu, sau fără, notificarea utilizatorului.

Soluția permite monitorizarea activității în timp real, cu posibilitatea înregistrării și a redării filmului acesteia:

- Streaming în timp real al filmului activității utilizatorului vizat, la nivel de post de lucru;
- Accesul, exclusiv pentru administratori specific autorizați la redarea înregistrării, pe diverse platforme, inclusiv de tipul terminalelor mobile inteligente;
- Posibilitatea de exportare / descărcare a înregistrărilor, într-un format standardizat;
- Posibilitatea de căutare, pe baza informației martor de audit (loguri), și de regăsire rapidă a înregistrărilor de interes.

Soluția asigură posibilitatea de a identifica și, respectiv, de a permite sau de a bloca activități la nivel de utilizator.

Protecția caracterului privat al situației și, respectiv, al informației va fi asigurată prin:

- Utilizarea de profile de monitorizare pentru configurarea parametrilor aplicabili;
- Activarea și/sau dezactivarea monitorizării în funcție de o multitudine de criterii, inclusiv în funcție de aplicație sau website, precum și pe bază de program orar.

Posibilitatea de a identifica și de urmări, la nivel de post de lucru și de utilizator va include:

- Mesajele email primite sau trimise;
- Conectarea locală de medii de stocare amovibile;
- Transferul de local fișiere;
- Aplicațiile care rulează;
- Utilizarea tastaturii;
- Paginile de Internet vizitate;
- Căutările pe Internet;

- Documentele imprimate.

Soluția va asigura posibilitatea de acces interactiv și de preluare efectivă a controlului, în situații asimilate incidentelor de securitate, exclusiv pentru administratori specific autorizați;

Soluția va asigura posibilitatea de definire a unor acțiuni (și secvențe de acțiuni) specifice pentru situații specificate, inclusiv:

- Blocarea încercării de trimitere a unui mesaj de email către o destinație neautorizată;
- Blocarea imediată a accesului la stația de lucru în cazul copierii neautorizate a unui fișier pe un suport de stocare amovibil;
- Limitarea duratei zilnice de utilizare a unei aplicații specificate, cu posibilitatea de blocare ulterioară a accesului la aceasta;
- Blocarea accesului de la distanță al utilizatorilor externi în afara programului de lucru specificat;
- Blocarea lansării neautorizate de către utilizatori a unor programe fără legătură cu rolul acestora.

Soluția va asigura analiza de risc și orchestrarea reacției specifice asociate setului activ de reguli și politici de utilizare a resurselor la nivel de post de lucru, inclusiv:

- Identificarea posturii generale de securitate, la nivel de organizație;
- Definirea de reguli care să poată fie bloca proactiv o mare varietate de acțiuni nedorite, cu sau fără notificarea administratorilor, fie notifica proactiv și îndruma utilizatorul;
- Blocarea acțiunilor nedorite va putea fi însoțită de blocarea accesului utilizatorului la stație;
- Operarea cu niveluri de risc pre-definite în raport de care pot fi definite și regrupate politicile de securitate;
- Operarea cu scoruri de risc, rezultate din analiza, care pot fi asociate la nivel de utilizator sau de departament.

Mecanismele de monitorizare, inclusiv înregistrare, și cele de aplicare a politicilor de securitate vor fi continua să fie active și în cazul pierderii temporare a conectivității de rețea:

- În acest caz, regulile vor ține seama de profilul aplicat la cea mai recentă conectare la server;
- După reconectare, datele colectate vor fi sincronizate automat, în mod transparent și controlat, cu serverul.

Soluția va include instrumente de analiza a productivității, relativ la accesul utilizatorilor la resurse și la utilizarea efectivă a acestora;

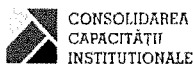
Soluția va dispune de mecanisme interne de alertare automată, în timp real, și de raportare.

Arhitectura soluției constă în agenți instalați la nivelul instanțelor de sisteme de operare de post de lucru suportate, coordonați și controlați de cel puțin o instanță virtualizată de tip server.

Platformele suportate pentru componenta de tip agent vor include cel puțin Windows 7/8/10 (32-bit / 64-bit), Windows Server 2008 /2008 R2 /2012 /2012 R2.

Instalarea agenților se va purtea face atât în mod manual, pe bază de pachete de tip .msi, cât și în mod programatic, inclusiv la nivel de Group Policy, local sau de la distanță și cu opțiuni de instalare automată, transparentă, fără notificarea și fără intervenția utilizatorului.

Comunicarea între agenți și instanțele de tip server vor presupune lățime de bandă redusă la nivel LAN (de ordinul a 10kbs).



Proiect cofinanțat din Fondul Social European prin
Programul Operațional Capacitate Administrativă 2014-2020!

<p>Garanție și suport</p>	<ul style="list-style-type: none"> ▪ Soluția va include garanție de minim 36 de luni. Suportul și garanția trebuie asigurate în România de producătorul respectivei soluții sau prin partener autorizat; ▪ Garanția va fi asigurată cu un SLA (Service Level Agreement) de 8x5xNBD (8 ore pe zi, 5 zile pe săptămână, cel mai târziu a doua zi lucrătoare – Next Business Day); ▪ Se va asigura acces 24x7 în centrul de suport al producătorului, cu posibilitatea raportării problemelor apărute în funcționare și solicitarea rezolvării acestora în funcție de severitate. De asemenea se va asigura dreptul de a face update-uri și upgrade-uri software.
---------------------------	---

4.4.1.15 Componenta de redistribuție a accesului la serviciile de aplicație

Platforma de redistribuție a accesului la serviciile de aplicație trebuie să îndeplinească următoarele specificații tehnice minime:

Caracteristica	Cerința tehnică minimă
Arhitectura	<ul style="list-style-type: none"> ▪ Platforma va suporta implementarea în oricare din următoarele scenarii: Active-Standby, Active-Active și configurații N+1; ▪ Soluția va permite sincronizarea configurațiilor, starea conexiunilor și persistența pentru asigurarea disponibilității aplicațiilor în caz de failover;
Redistribuție a accesului la serviciile de aplicație	<ul style="list-style-type: none"> ▪ Platforma va oferi suport IPv4, IPv6, topologii NAT64, IP anycast; ▪ Platforma va furniza răspunsuri de autoritate DNS (server autoritar DNS/server secundar DNS) îndreptând traficul către adresele IP corecte; ▪ Platforma va obține informațiile despre starea obiectelor și metrice în mod automat din ADC; ▪ Platforma va oferi posibilitatea deservirii răspunsurilor pentru obiectele configurate din memoria cache de mare viteză; ▪ Platforma va include funcționalitatea de authoritative slave DNS server și va răspunde și la cereri pentru hostname-uri nebalansate; ▪ Platforma va oferi posibilitatea validării cererilor de la clienți pe baza de RFC; ▪ Platforma va suporta DNS SEC și pentru răspunsuri la hostname-uri balansate; ▪ Platforma va oferi suport de SSL offloading și DNSSEC în hardware;

	<ul style="list-style-type: none"> ▪ Platforma va include o baza de date de geolocalizare in scopul directarii utilizatorilor catre cel mai apropiat data center; ▪ Platforma va permite colectarea/construcția unei baze de date de geolocalizare pentru adrese IP private; ▪ Platforma va permite balansarea pe baza urmatoarelor metrici: <ul style="list-style-type: none"> ▪ Round Trip Time; ▪ Hops; ▪ Topology; ▪ Completion Rate; ▪ Packet Rate; ▪ Virtual Server Capacity; ▪ Bits/second; ▪ Link Capacity
Disponibilitate	<ul style="list-style-type: none"> ▪ Soluția va suporta mirroring pentru conexiunile non-SSL in configuratie Active-Standby; ▪ Soluția va permite backup și restore pentru fisierul de configurare din interfata grafica; ▪ Soluția va permite failover între modulele sau echipamentele corespondente configurate, in functie de: defectiuni hardware, defectiuni de sistem, nefunctionarea acceleratoarelor SSL, nefunctionarea rețelei, nefunctionarea gateway-ului; ▪ Soluția va suporta implementarea intr-un mediu / topologie cu o singura sub-rețea (subnet);
Management	<ul style="list-style-type: none"> ▪ Platforma va permite primirea de mesaje SOAP/XML de la instrumente externe pentru modificarea configuratiei controller-elor de aplicatii; ▪ Soluția permite management-ul prin interfata seriala, CLI (cu SSH) și https GUI; ▪ Platforma va permite colectarea de informatii statistice și istorice despre utilizarea memoriei, procesorului, conexiuni și trafic și afisarea acestora in grafice disponibile in interfata grafica. Unitatile de timp minim disponibile vor fi: per ora, zi, saptamana sau luna; ▪ Soluția va permite generarea și afisarea unei harti a rețelei pentru adresele IP și pool-urile serverelor virtuale; ▪ Soluția va suporta generarea unei tabele de rutare ierarhizata compusa din diferite segmente (tip "parent" "child") pentru spatiile de IP-uri izolate sau suprapuse;

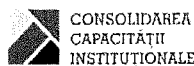


Handwritten signature

Handwritten signature



	<ul style="list-style-type: none"> ▪ Platforma / Soluția va permite alocarea dinamică și controlabilă a resurselor tip CPU și memorie RAM (ex. dedicat, funcționare nominală, funcționare minimă); ▪ Soluția va putea trimite alerte despre diverse erori prin SNMP, syslog, e-mail; ▪ Soluția va permite definirea de multiple domenii de administrare; ▪ Soluția va permite resetarea la configurațiile inițiale ("din fabrică");
Alimentare	Pentru asigurarea redundanței complete a echipamentului propus fiecare element major component al platformei de protecție a serviciilor de aplicație trebuie să ofere alimentare redundantă prin cel puțin două surse independente de alimentare. Sursele trebuie să ofere funcționalitate hot-swap pentru înlocuirea rapidă, fără oprirea alimentării sistemului și fără întreruperea serviciilor asigurate de platformă;
Ventilație	Toate elementele de asigurare a ventilației sistemului trebuie să fie de tip hot-swap pentru înlocuirea lor rapidă în caz de avarie, fără întreruperea funcționalităților oferite de platformă;
Cerințe constructive	<ul style="list-style-type: none"> ▪ Platforma de protecție a serviciilor de aplicație trebuie să fie montabilă în rack-uri standard de 19"; ▪ Ofertantul trebuie să livreze un kit cu elementele de fixare/instalare în rack (suporturi, șuruburi/captive);
Garanție și suport	<ul style="list-style-type: none"> ▪ Pentru toate elementele și modulele integrate, soluția va include garanție de minim 36 de luni. Suportul și garanția trebuie asigurate în România de producătorul respectivelor echipamente; ▪ Garanția hardware va fi asigurată cu un SLA (Service Level Agreement) de 8x5xNBD (8 ore pe zi, 5 zile pe săptămână, cel mai târziu a doua zi lucrătoare – Next Business Day), care să garanteze diagnosticarea echipamentului sau modulului defect și înlocuirea acestuia în maxim 3 zile lucrătoare, fără alte costuri; ▪ Se va asigura acces 24x7 în centrul de suport al producătorului, cu posibilitatea raportării problemelor aparute în funcționare și solicitarea rezolvării acestora în funcție de severitate. De asemenea se va asigura dreptul de a face update-uri și upgrade-uri software (sistem de operare, firmware, etc).

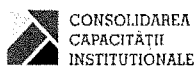


4.4.1.16 Componenta de protecție a serviciilor de aplicație

Platforma de protecție a serviciilor de aplicație trebuie să îndeplinească următoarele **specificatii tehnice minime**:

Caracteristica	Cerinta tehnica minimala
Arhitectura	<ul style="list-style-type: none"> ▪ Platforma va suporta implementarea in oricare din urmatoarele scenarii: Active-Standby, Active-Active si configuratii N+1; ▪ Soluția va permite sincronizarea configuratiilor, starea conexiunilor si persistenta pentru asigurarea disponibilitatii aplicatiilor in caz de failover;
Optimizare si balansare/rebalansare	<ul style="list-style-type: none"> ▪ Platforma de protecție a serviciilor de aplicație trebuie să poată funcționa în mod full proxy, respectiv în mod reverse proxy; ▪ Capacitate de a procesa trafic TCP și UDP generat de diferite aplicații; ▪ Multipli algoritmi sau metode de balansare a traficului: round-robin, ratio și priority (cu un număr minim de membri activi); ▪ Multipli algoritmi sau metode dinamice de balansare a traficului: fastest-response, least-connections, combinația fastest-response least-connections, precum și bazate pe resursele serverelor de aplicații (ex: utilizare CPU, încărcarea memorie, gradul de încărcare al rețelei etc); ▪ Capacitatea de trimite cereri gradual către serverele de aplicații nou adăugate; ▪ Capacitatea de redirectare a traficului pentru diferite tipuri de (ex: http to https); ▪ Monitorizarea aplicațiilor "content based", cum ar fi: HTTP/HTTPS, FTP (pasiv/activ), POP3, IMAP, SIP, SMTP, telnet, RADIUS, LDAP (cu TLS sau peste canal SSL), SASP, Oracle, MSSQL, SNMP DCA, WMI, RPC și SOAP; ▪ Capabil să proceseze cereri bazat pe IP sursa/destinație, SSL, hash persistence; ▪ Capabil să utilizeze diferite metode pentru "cookie persistence": pasiv, insert, rewrite; ▪ Capabil să utilizeze metode de persistență a sesiunilor în funcție de orice variabilă din header-ul pachetelor TCP/UDP sau din payload;

- NAT (network address translation) și NAPT (network address port translation) bazat pe IP sursa și/sau IP destinație;
- Capabilitate de a returna pachete bazate pe adresa MAC a ultimului hop (asigurarea rutării asimetrice);
- Capacitatea de a decide direcționarea traficului în funcție de URI, method, HTTP host, version, cookie, tipul browser-ului folosit de client, etc;
- Capacitate de a genera reguli noi pentru managementul traficului în funcție de anumite evenimente, folosind un limbaj de scripting;
- Capacitate de a controla fluxul de trafic bazat pe conținutul acestuia, în mod bi-direcțional;
- Capabil de a folosi o combinație mixtă de adrese virtuale și noduri IPv4 și IPv6;
- Capabil să translateze trafic IPv6-IPv4 și IPv4-IPv6;
- Capabil de inserție XFF în header-e HTTP, cu IP-ul de origine al clientului;
- Redirecționare URL către mai multe servere virtuale în funcție de HTTP response code sau URL pattern;
- Capacitatea de a returna o pagină de eroare în cazul în care resursele/serverele de aplicație nu sunt disponibile. Pagina de eroare și mesajul trebuie să poată fi personalizate și să poată conține grafică;
- Capabilitatea de a folosi "chunked transfer encoding" pentru menținerea persistenței sesiunilor;
- Capabilitatea de a agrega și refolosi multiple sesiuni client într-o singură sesiune server-side;
- Capabilitatea de a transforma sesiuni HTTP 1.0 în sesiuni HTTP 1.1 pentru consolidare sesiunilor server-side;
- Capabilitate built-in de compresie HTTP pentru reducerea traficului;
- Capabilitate built-in pentru accelerare și caching HTTP;
- Capabilitate built-in pentru optimizare simetrică de date, compresie, criptare și tunneling;
- Capabilitate de criptare AES SSL;
- Capabilitate pentru caching multi-store pentru conținut dinamic și static (RFC2616);



Proiect cofinanțat din Fondul Social European prin
Programul Operațional Capacitate Administrativă 2014-2020!

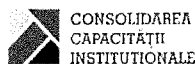
	<ul style="list-style-type: none"> ▪ Capabilitati pentru optimizarea traficului LAN/WAN conform: RFC2582 (optimizare Reno asimetrica), RFC1323 (extensii TCP pentru retele de mare viteza), RFC3042, RFC2018, RFC3168;
Procesare SSL/TLS	<ul style="list-style-type: none"> ▪ Platforma va suporta terminarea de trafic SSL/TLS; ▪ Platforma va dispune de acceleratori SSL pentru SSL offloading; ▪ Platforma va putea comunica prin SSL/TLS cu un server de aplicatii backend; ▪ Platforma va suporta ajustarea parametrilor SSL precum metoda de criptare utilizata, versiunea; ▪ Platforma va suporta SSLv3 si TLSv1; ▪ Platforma va suporta certificate wildcard;
Protectie a serviciilor de aplicatie Web	<ul style="list-style-type: none"> ▪ Capabilitate de inspectie a cererilor/raspunsurilor HTTP; ▪ Capabilitatea de blocare a codurilor de eroare generate de anumite servere de aplicatii; ▪ Capabilitatea de a bloca atacuri tip DoS prin connection proxy; ▪ Abilitatea de a folosi ambele modele de securitate: pozitiva si negativa ▪ Capabilitate de filtrare a pachetelor OSI L3-L7; ▪ Capabilitatea de a ascunde informatiile despre serverele de aplicatii si mesajele generate de acestea ("Resource cloaking"); ▪ Capabilitatea de a detecta si bloca anomalii de protocol TCP/UDP, pentru protectie DoS; ▪ Solutia trebuie sa aiba capacitatea de a construi in mod automat politici de securitate; ▪ Solutia trebuie sa aiba capacitatea de a accepta prin interventie manuala fals-positives; ▪ Solutia trebuie sa poata defini politici diferite de securitate pentru diverse aplicatii; ▪ Capabilitate de definire a politicilor de blocare pentru atacuri tip DoS; ▪ Capabilitate de combinare a mecanismelor detectie si prevenire; ▪ Mecanism de roll-back a politicilor de securitate; ▪ Mecanism de versionare a politicilor de securitate;



- Mecanism de construire a politicilor de securitate real-time, cu functie de auto-invatare;
- Politici predefinite pentru diferite aplicatii (ex: MS SharePoint, Oracle Application 10g etc);
- Capabilitate de monitorizare a aplicatiilor protejate pentru prevenirea, detectarea si raportarea anomaliilor de trafic precum si pentru protectia impotriva atacurilor L7 DoS;
- Solutia va suporta urmatoarele metode / tehnici de detectie:
 - Decodare URL;
 - Null byte string termination;
 - Self-referencing paths (ex. utilizarea `./` si echivalente codate);
 - path back-references (ex. utilizarea `./` si echivalente codate);
 - Combinatii de litere mari si mici;
 - Utilizarea excesiva de spatii libere;
 - Eliminarea comentariilor (ex. transformarea `DELETE/**/FROM` in `DELETE FROM`);
 - Conversia caracterelor backslash in forward slash (suportat in windows);
 - Conversia codarii unicode specifica IIS (`%uXXYY`);
 - Decodarea entitatilor HTML (ex. `c`, `"`, `પ`);
 - Caractere speciale (ex. `\t`, `\001`, `\xAA`, `\UAABB`);
 - Suport pentru modelul de securitate pozitiva - "permite tot traficul cunoscut" si blocheaza tot traficul necunoscut;
 - Traseu/conexiune specifica per aplicatie;
 - Motor integrat de detectie pentru tentativele de evitare a inspectiei;
 - Operarea intr-o arhitectura full Proxy si control inline complet asupra traficului prin echipament;
 - Detectie bazata pe semnaturi;
 - Platforma de protectie a serviciilor de aplicatie ajuta la implementarea unui model de securitate pozitiva. Acest model trebuie sa poata fi configurat atat manual cat si automat fara utilizarea de instrumente aditionale / externe (bazat pe traficul de productie si fara impact asupra acestuia);
- Solutia trebuie sa suporte gruparea semnaturilor;



- Solutia trebuie sa suporte cel putin urmatoarele categorii de semnaturi:
 - Baze de date: Microsoft SQL, ORACLE, MySQL, PostgreSQL, Sybase, MariaDB;
 - Sisteme de operare: Windows, Linux, UNIX;
 - Limbaje si contexte de aplicatie: .NET, PHP, Java;
 - Servere web: Apache, Microsoft IIS;
- Generarea manuala sau automata a politicilor de securitate pozitiva trebuie sa includa minim urmatoarele:
 - Metode HTTP;
 - URNs;
 - Header-e;
 - Parametri permisi pentru un URN specific;
 - Seturi de caractere speciale pentru fiecare valoare de parametru;
 - Semnaturi pentru valori specifice de parametru;
- Solutia trebuie sa permita dezvoltarea politicii de securitate fara script-uri aditionale;
- Solutia trebuie sa permita generarea automata a politicii de securitate;
- Solutia trebuie sa recunoasca host-urile/entitatile (IP-urile) de incredere (trusted). Cererile acestora trebuiesc tratate corespunzator;
- Solutia trebuie sa permita asimilarea structurii unei aplicatii (URN, parametri, tipuri de parametri, semnaturi si caractere speciale per parametru) fara interventia operatorului uman;
- Solutia trebuie sa suporte detectia parametrilor ascunsi/dinamici;
- Utilizatorii vor putea inspecta politica de securitate (audit si raportare);
- Solutia va putea proteja obiectele / paginile cu continut nou fara a fi nevoie de a crea politica de securitate de la zero;
- Solutia va permite relaxarea sau inasprirea (adaptarea) ulterioara a politicii de securitate generata automat;
- Interactiunea cu instrumente third party de evaluare a vulnerabilitatilor;



	<ul style="list-style-type: none"> ▪ Va fi posibila constructia politicii de securitate pe baza de instrumente third party de evaluare a vulnerabilitatilor - spre exemplu prin import); ▪ Platforma de protectie a serviciilor de aplicatie va fi pre-integrata cu producatorii de top: Qualys, IBM etc; ▪ Managementul configuratiei; ▪ Platforma de protectie a serviciilor de aplicatie va permite definirea de roluri pentru utilizatori si va solicita autentificare; ▪ Platforma de protectie a serviciilor de aplicatie va permite inlocuirea / customizarea paginilor cu mesaje de eroare sau de blocare; ▪ Platforma de protectie a serviciilor de aplicatie va permite definirea de pagini HTML, AJAX si JSON cu mesaje de blocare; ▪ Platforma de protectie a serviciilor de aplicatie va permite actualizarea manuala sau automata a semnaturilor (mentinute si publicate de furnizori);
Disponibilitate	<ul style="list-style-type: none"> ▪ Solutia va suporta mirroring pentru conexiunile non-SSL in configuratie Active-Standby; ▪ Solutia va permite backup si restore pentru fisierul de configurare din interfata grafica; ▪ Solutia va permite failover intre echipamentele corespondente configurate, in functie de: defectiuni hardware, defectiuni de sistem, nefunctionarea acceleratorilor SSL, nefunctionarea retelei, nefunctionarea gateway-ului; ▪ Solutia va suporta implementarea intr-un mediu / topologie cu o singura sub-retea (subnet);
Management	<ul style="list-style-type: none"> ▪ Platforma va permite primirea de mesaje SOAP/XML de la instrumente externe pentru modificarea configuratiei controller-elor de aplicatii; ▪ Solutia permite management-ul prin interfata seriala, CLI (cu SSH) si https GUI; ▪ Platforma va permite colectarea de informatii statistice si istorice despre utilizarea memoriei, procesorului, conexiuni si trafic si afisarea acestora in grafice disponibile in interfata grafica. Unitatile de timp minim disponibile vor fi: per ora, zi, saptamana sau luna;

	<ul style="list-style-type: none"> ▪ Solutia va permite generarea si afisarea unei harti a retelei pentru adresele IP si pool-urile serverelor virtuale; ▪ Solutia va suporta generarea unei tabele de rutare ierarhizata compusa din diferite segmente (tip "parent" "child") pentru spatiile de IP-uri izolate sau suprapuse; ▪ Platforma / Solutia va permite alocarea dinamica si controlabila a resurselor tip CPU si memorie RAM (ex. dedicat, functionare nominala, functionare minima); ▪ Solutia va dispune de template-uri de configurare generice customizabile in functie de nevoile specifice; ▪ Solutia va putea trimite alerte despre diverse erori prin SNMP, syslog, e-mail; ▪ Solutia va permite definirea de multiple domenii de administrare; ▪ Solutia va permite resetarea la configuratiile initiale ("din fabrica");
Alimentare	Pentru asigurarea redundantei complete a echipamentului propus fiecare element major component al platforma de protectie a serviciilor de aplicatie trebuie sa ofere alimentare redundanta prin cel puțin doua surse independente de alimentare. Sursele trebuie sa ofere functionalitate hot-swap pentru inlocuirea rapida, fara oprirea alimentarii sistemului si fara intreruperea serviciilor asigurate de platforma;
Ventilatie	Toate elementele de asigurare a ventilatiei sistemului trebuie sa fie de tip hot-swap pentru inlocuirea lor rapida in caz de avarie, fara intreruperea functionalitatilor oferite de platforma;
Cerinte constructive	<ul style="list-style-type: none"> ▪ Platforma de protectie a serviciilor de aplicatie trebuie să fie montabilă în rack-uri standard de 19"; ▪ Ofertantul trebuie să livreze un kit cu elementele de fixare/instalare în rack (suportți, șuruburi/captive);
Garanție si suport	<ul style="list-style-type: none"> ▪ Pentru toate elementele si modulele integrate, solutia va include garantie de minim 36 de luni. Suportul si garantia trebuie asigurate in Romania de producatorul respectivelor echipamente;

	<ul style="list-style-type: none"> ▪ Garanția hardware va fi asigurată cu un SLA (Service Level Agreement) de 8x5xNBD (8 ore pe zi, 5 zile pe săptămână, cel mai târziu a doua zi lucrătoare – Next Business Day), care să garanteze diagnosticarea echipamentului sau modulului defect și înlocuirea acestuia în maximum 3 zile lucrătoare, fără alte costuri; ▪ Se va asigura acces 24x7 în centrul de suport al producătorului, cu posibilitatea raportării problemelor apărute în funcționare și solicitarea rezolvării acestora în funcție de severitate. De asemenea se va asigura dreptul de a face update-uri și upgrade-uri software (sistem de operare, firmware, etc).
--	---

4.4.1.17 Componenta centrală de protecție avansată antimalware

Componenta centrală de protecție avansată antimalware trebuie să îndeplinească următoarele specificații tehnice minime:

Caracteristica	Cerința tehnică minimală
Arhitectura	<ul style="list-style-type: none"> ▪ Platforma hardware dedicată de detecție, analiză și protecție împotriva amenințărilor avansate, ce monitorizează traficul pe toate porturile pentru mai mult de 100 de protocoale de rețea și aplicații; ▪ Platforma va asigura acoperire și vizibilitate completă în toate punctele din rețea, astfel încât permite detecția atacurilor direcționate, de tip ransomware și a amenințărilor avansate persistente; ▪ Platforma va primi traficul de rețea prin porturi mirror, SPAN, TAP sau mecanisme similare de copiere a traficului și va permite monitorizarea pentru cel puțin trafic de tip HTTP, SMTP, FTP, DNS, CIFS, etc; ▪ Va include funcționalitate de tip sandbox nativă prin intermediul aceluși platforme hardware, fără a necesita platforma hardware dedicată acestei funcționalități;
Detecție amenințări avansate	<ul style="list-style-type: none"> ▪ Soluția va asigura detecție și analiză în toate fazele unui atac, raportând descoperirile pentru fiecare fază în parte: <ul style="list-style-type: none"> ▪ Colectarea de informații;

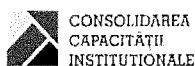


The Hub

Dez...

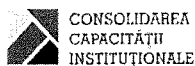


- Punctul de intrare;
- Comunicatia de tip Command & Control;
- Miscarea laterala;
- Descoperirea de resurse si date;
- Extragerea datelor;
- Solutia va asigura suport de detectie si analiza in retele de date IPv4 si IPv6, respectiv va oferi suport pentru comunicarea parametrilor de stare prin protocol SNMPv2/v3 si netSNMP;
- Solutia trebuie sa permita crearea de reguli si definitii de scanare a resurselor de infrastructura atat in mod individual cat si prin grupari de reguli, reguli si grupari de reguli ce vor putea fi activate/dezactivate individual;
- Solutia va asigura detectia continutului malitios cel putin prin urmatoarele mecanisme:
 - Scanare de malware cu motoare bazate pe semnături, respectiv prin metode euristice, pentru detectarea de malware cunoscut si necunoscut;
 - Detectie a kit-urilor de exploatare a browser-elor web;
 - Decodare si decompresie fisiere embedded;
 - Simulare in sandbox pentru fisiere suspicioase;
- Solutia va asigura detectarea si analiza comunicatiei suspecte cel putin prin urmatoarele mecanisme:
 - Analiza de destinatii (URL, IP, domenii, e-mail, IRC, etc) prin blacklisting si whitelisting dinamic local;
 - Detectie e-mailuri de tip Spear Phishing si/sau Phishing;
 - Detectie comunicatie de tip Command & Control;
 - Analiza reputationala pentru toate URL-urile solicitate si integrate in alte resurse (ex: fisiere Office);
- Reguli de amprentare a traficului de comunicatie;
- Solutia va asigura urmatoarele mecanisme de analiza comportamentala:
 - Reguli de analiza euristica;
 - Identificare si analiza pentru utilizarea a peste 100 de protocoale si aplicatii, inclusiv aplicatii web (SMTP, POP3, IMAP4, HTTP, HTTPS, Kerberos, RADIUS, LDAP, DCE-RPC, SMB, SMB2, DNS request, DNS response, DHCP, DHCPv6, FTP, TFTP, File Transfer, RDP, SSH, TELNET, VNC, Cisco-TELNET, RADMIn, MODBUS-UDP, MODBUS-TCP, SQL,



MySQL, MSSQL, Oracle, PostGres, RTSP/RTP-UDP, RTSP/RTP-TCP, RTSP/RDT-UDP, RTSP/RDT-TCP, WMSP, SHOUTCast, RTMP, Gmail, Hotmail, Yahoo mail, ARP, IGMP, MMS, ICMP, IRC, SIP2, Bittorent, Direct Connect, Kazaa, Google Talk, MSN, YMSG, Skype, Yahoo Web Messenger, Ares, Blubster, Cabos, Deepnet Explorer, eDonkey_eMule, eDonkey, Foxy, FreeWire, Gnucleus LAN, Gimme, GnuDNA GWebCache, Gnutella/Limewire/Bearshare/Shareaza, iMesh, Jubster, Kceasy, KuroMiranda, MLDonkey, MoodAmp, MyNapster, Nova GWebCache, OpenNap, Ppstream, SoulSeek, Swapper GWebCache, Winny, WinMX, Xnap, Xolox, Zultrax, AIM Express, Chikka SMS Messenger, eBuddy, ICQ2Go, ILoveIM Web Messenger, IMUnitive, mabber, meebo, etc);

- Fingerprinting de comportamente;
- Soluția trebuie să identifice și să marcheze sursele de încredere pentru transmiterea datelor (sisteme și aplicații marcate ca nefiind infectate cu elemente malițioase), cel puțin pentru următoarele tipuri de resurse:
 - Gama de adrese IP;
 - Domenii;
 - Tipuri de servere: Kerberos, Active Directory, FTP, SMTP, HTTP proxy, Domain Controller, Contain Management Server, File Server (SMB), RADIUS, DNS, Database server, Web Server, Software Update Server, etc;
- Soluția trebuie să ofere protecție împotriva amenințărilor malware comune, cel puțin pentru:
 - Vulnerabilități (CVE): Apache Struts, Foxit Reader, MS SilverLight, Mozilla, Joomla, Sun Java, IE, Shellshock, SSL CCS Injection, etc;
 - Unelte și kit-uri de penetrare: Cobaltstrike, Metasploit reverse (shell, bash, telnet, perl, netcat, etc), Poisonivy, Meterpreter reverse (PHP/Python/Perl), PsExec, Keylogger http request, IRCbot connection, DDOS tools (HOIC, LOWC, LOIC), TOR, Bitcoin request, etc;
 - Amenințări de tip ransomware: Cerber, Locky, Cryptesla, etc;



Proiect cofinanțat din Fondul Social European prin
Programul Operațional Capacitate Administrativă 2014-2020!



[Handwritten signature]

[Handwritten signature]

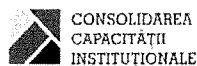
	<ul style="list-style-type: none"> ▪ Unelte si kit-uri de exploatare a vulnerabilitatilor: Neutrino, Magnitude, Rig, Angler, Nuclear, Range HTTP, Ghost SMTP, etc; ▪ Solutia trebuie sa permita definirea intervalului orar de lucru, respectiv a proceselor de detectie si analiza ce ruleza in functie de respectivul orar; ▪ Solutia trebuie sa permita definirea de exceptii de la regulile de analiza si detectie cel putin pentru urmatoarele tipuri de resurse: Host, Protocol, Adresa IP, Gama de adrese IP, etc; ▪ Solutia trebuie sa permita crearea rapida de filtre de analiza, detectie si raportare, bazate cel putin pe urmatoarele tipuri de resurse: sisteme afectate, sisteme cu un numar mare de detectii/evenimente de securitate, obiecte suspicioase (adrese IP, domenii, fisiere, etc); ▪ Solutia trebuie sa permita transmiterea manuala a fișierelor de analiza, precum si un API de interfatare cu alte produse terte pentru transmiterea de solicitari de analiza si extragere de rezultate, inclusiv partajare de obiecte suspicioase si indicatori de compromis; ▪ Solutia trebuie sa permita integrarea nativa cu Componenta de protecție a resurselor la nivel de post de lucru, asigurand monitorizarea la nivel de context a posturii de securitate a intregului ecosistem, respectiv raportarea activitatilor detaliate de sistem, precum si natura si dimensiunea oricarui atac survenit; ▪ Solutia trebuie sa permita trimiterea obiectelor malitioase identificate (amprenta criptografica a fișierelor, adrese IP, domenii, adrese URL, etc) catre toate sistemele cu care se integreaza nativ astfel incat amenintarile si obiectele malitioase sa poata fi blocate in intreaga infrastructura deservita;
<p>Functionalitati de tip Sandbox</p>	<p>Platforma ofertata va include functionalitate integrata hardware pentru procesele specifice activitatilor de tip "sandbox":</p> <ul style="list-style-type: none"> ▪ Va permite analiza elementelor suspecte, dupa filtrarea lor prealabila efectuata de modulele de detectie a amenintarilor avansate; ▪ Va permite functionalitati avansate de evitare a evadarii din sandbox, precum si un mod de "safe live" pentru analiza unor descarcari multi-nivel, URL, Command & Control, etc;

- Va oferi următoarele metode de analiza si detectie:
- Soluția trebuie să fie capabilă să detecteze și să prevină software-ul malițios avansat, atacuri de tipul „zero-day” și de tip APT (Advanced Persistent Threat) direcționate;
- Soluția trebuie să detecteze software-ul malițios de tip “zero-day multi-stage” și atacuri direcționate fără o cunoaștere prealabilă a software-ului malițios;
- Analiza statica, euristica si comportamentala;
- Analiza bazata pe reputatia adreselor si fisierelor pentru URL-uri;
- Analiza conexiunilor de retea outbound sau de mesagerie suspicioase;
- Analiza fisierelor suspicioase ce efectueaza conexiuni la servere de tip Command & Control;
- Analiza atacurilor de tip ransomware, deception, social-engineering, hijack, redirectionare si/sau furt de date, rootkit cloaking;
- Analiza operatiunilor cu fisiere: file drop, download, partajare si/sau replicare de fisiere;
- Analiza operatiunilor ce vizeaza modificarile de procese, servicii sau obiecte de memorie;
- Evaluarea continua a amenintarilor, actiunilor intreprinse de elementele malware si impactul asupra sistemului analizat;
- Mecanisme incluse de analiza de tip forensics, cel putin prin captura pachetelor de date relevante (PCAP);
- Soluția trebuie să asigure procese de analiză cu suport atât pentru arhitecturi de tip x86 cât și pentru arhitecturi de tip x64;
- Soluția trebuie să asigure restaurarea mașinilor virtuale de analiză la o configurație de bază după finalizarea analizei unui software malițios, automat sau manual;
- Mașinile virtuale preinstalate vor avea configurate aplicații de tip browser (cel puțin Internet Explorer, Mozilla Firefox, Google Chrome, Safari), plugin-uri (cel puțin Adobe Flash, Adobe Shockwave, Adobe Air) precum și aplicații uzuale (cel puțin Adobe Acrobat Reader, Microsoft Office Word, Excel, Powerpoint, Outlook, Oracle Java JRE, Windows Media Player, Quicktime Player);
- Soluția trebuie să asigure cel puțin analiza celor mai comune tipuri de fișiere cunoscute ca fiind folosite pentru distribuirea sau

	<p>găzduirea de aplicații malware (fișiere executabile – EXE, DLL, documente Microsoft Office – DOC, DOCX, XLS, XLSX, PPT, PPTX, documente PDF, fișiere JAR, BAT, fișiere de tip imagine, fișiere de tip video, Flash, arhive – ZIP, RAR, SFX);</p> <ul style="list-style-type: none"> ▪ Soluția trebuie să asigure extinderea tipurilor de fișiere ce pot fi analizate; ▪ Soluția trebuie să asigure cel puțin analiza obiectelor Web prin furnizarea unui URL; ▪ Soluția trebuie să fie capabilă să simuleze acțiuni ale utilizatorilor finali (interacțiunea dintre mașina virtuală de analiză și utilizator) în scopul de a forța executarea de software malițios care se bazează pe astfel de acțiuni (de exemplu un click de mouse, răspuns la ferestre dialog sau parcurgerea unor pași de instalare) sau pe observarea prezenței utilizatorului (prin apelarea unor funcții Windows native sau din interfața Windows API); ▪ Soluția trebuie să asigure jurnalizarea apelurilor de funcții Windows native și din interfața Windows API relevante pentru depistarea comportamentului malițios; ▪ Soluția trebuie să asigure identificarea și rularea software-ului malițios care are capacitatea de a identifica mediile virtualizate sau emulate; ▪ Soluția trebuie să genereze un set de indicatori de compromitere după execuția virtuală a software-ului malițios; ▪ În cazul unui atac soluția trebuie să raporteze cel puțin IP-ul sursă, IP-ul destinație, serverul de tip Command & Control, URL-ul, botname-ul, clasa de malware, protocoalele utilizate și severitatea infecției;
<p>Raportare</p>	<ul style="list-style-type: none"> ▪ Soluția trebuie să prezinte rezultatele analizei software-ului malițios sub forma unui tablou de bord grafic (dashboard) și/sau a unui raport care detaliază comportamentul amenințării; ▪ Soluția trebuie să permită reconfigurarea tabloului de bord grafic prin folosirea unor elemente de tip widget (cel puțin elemente pentru gradul de încărcare CPU/RAM/Disc, top amenințări/URL-uri, top sisteme cu evenimente de securitate, top comportamente suspicioase, top sisteme infectate, top sisteme exploatare, top aplicații/fișiere cu comportament suspicios, traficul în timp real generat de procesele de analiză și detecție, etc); ▪ Raportul furnizat va conține cel puțin următoarele informații:

	<ul style="list-style-type: none"> ▪ Tipul fișierului analizat; ▪ Sumele de control (MD5, SHA) ale fișierelor analizate sau create pe mașina virtuală de analiză; ▪ Dacă fișierul este executabil se va preciza dacă au fost folosite aplicații de tip packer și tipul acestora; ▪ Informații extrase din header-ul fișierelor executabile; ▪ Modificările produse la nivelul sistemului de operare; ▪ Modificările produse la nivelul aplicațiilor instalate; ▪ Modificările produse asupra sistemului de fișiere; ▪ Modificările produse asupra regiștrilor; ▪ Librării DLL încărcate la rulare; ▪ Funcțiile API apelate, în ordine cronologică; ▪ Informații despre procesele create/modificate/oprite; ▪ Informații despre serviciile create/modificate/oprite; ▪ Obiecte de tip Mutex create; ▪ Eventuale hook-uri SSDT, IDT sau IRP create; ▪ Eventuale conexiuni de rețea create și protocoalele de transport folosite; ▪ Interogările DNS; ▪ URL-urile accesate; ▪ Adrese IP contactate și porturile logice folosite; ▪ Informații de localizare geografică a adreselor IP contactate; ▪ Captura zonelor de memorie aferente proceselor suspecte de comportament malițios; ▪ Tipul de exploit folosit; ▪ Soluția trebuie să permită ordonarea/re-ordonarea câmpurilor din raport după culoana/coloanele selectate (indicator de risc al sistemelor, faza de atac, numele sistemelor, adresa IP, data la care a survenit atacul, etc); ▪ Soluția trebuie să permită exportul rapoartelor și al alertelor despre software-ul malițios cel puțin în format PDF, HTML și XLS; ▪ Soluția trebuie să suporte automatizarea raportării cel puțin pentru următoarele intervale de timp: zilnic, săptămânal, lunar și definit de utilizator;
Integrare	<ul style="list-style-type: none"> ▪ Soluția oferită trebuie să se integreze nativ cel puțin cu următoarele tipuri de servicii oferite de producătorul soluției (servicii ce vor permite actualizarea automată, neasistată a definițiilor de elemente malware):

	<ul style="list-style-type: none">▪ La nivelul filtrării URL: Serviciu de analiza bazat pe reputatia adreselor si fisierelor pentru URL-uri, respectiv motor intern responsabil de scanarea, detectarea si atasarea unui scor de risc fiecărei resurse URL solicitate si accesate. Acest motor trebuie sa permita si scanarea retroactiva pentru elementele malitioase de tip Command & Control;▪ La nivelul filtrării de fisiere: Serviciu de analiza bazat pe reputatia fisierelor cunoscute de la producatori cunoscuti, pentru a putea efectua procesele de comparare cu fisierele detectate in analiza locala, respectiv serviciu global de identificare a fisierelor malitioase prin colectarea datelor de la toti senzorii pe care producatorul solutiei oferite ii are instalati la nivel global;▪ La nivelul aplicatiilor mobile: Serviciu de analiza bazat pe reputatia aplicatiilor mobile, in vederea detectarii unor activitati malitioase, utilizarii de resurse si incalcarii ale nivelurilor de confidentialitate;▪ Solutia trebuie sa ofere un API de interfatare cu alte produse terte (specific cu producatorul Componentei de protectie la nivel de retea oferite, respectiv cel putin cu urmasorii producatori de solutii de securitate: Check Point, IBM Security, Palo Alto Networks, F5 Networks, BlueCoat, A10 Networks, etc) pentru transmiterea de solicitari de analiza si extragere de rezultate, inclusiv partajare de obiecte suspicioase si indicatori de compromis;▪ Solutia trebuie sa permita integrarea nativa cu Componenta de protectie a resurselor la nivel de post de lucru oferita, asigurand monitorizarea la nivel de context a posturii de securitate a intregului ecosistem, respectiv raportarea activitatilor detaliate de sistem, precum si natura si dimensiunea oricarui atac survenit;▪ Solutia trebuie sa permita integrarea nativa cu produse de tip SIEM pentru transferul evenimentelor cel putin prin mecanisme UDP/TCP/SSL;▪ Solutia trebuie sa permita integrarea descriptorilor malware cu solutii terte (ex: YARA);
Management	<ul style="list-style-type: none">▪ Soluția trebuie să asigure administrarea sa prin intermediul unei console web, fără instalarea de software suplimentar;▪ Solutia permite management-ul prin interfata seriala, CLI (cu SSH) si https GUI;



Proiect cofinanțat din Fondul Social European prin
Programul Operațional Capacitate Administrativă 2014-2020!



	<ul style="list-style-type: none"> ▪ Soluția trebuie să utilizeze un canal de comunicare criptat între administratori și consola de administrare; ▪ Platforma va permite colectarea de informații statistice și istorice despre utilizarea memoriei, procesorului, conexiuni și trafic și afișarea acestora în grafice disponibile în interfața grafică; ▪ Soluția trebuie să asigure crearea de conturi cu roluri diferite în administrarea sau monitorizarea alertelor; ▪ Soluția trebuie să poată identifica numele stației de lucru implicate în alertă; ▪ Soluția trebuie să asigure păstrarea logurilor arhivate. Aceste loguri trebuie să poată fi descărcate pe stația de lucru a unui utilizator cu rol de administrare a soluției; ▪ Soluția va putea trimite alerte despre diverse erori prin SNMP, syslog, e-mail; ▪ Soluția va permite definirea de multiple domenii de administrare; ▪ Soluția trebuie să poată fi actualizată online și offline; ▪ Soluția trebuie să poată utiliza un proxy cu autentificare pentru contactarea serverului de update; ▪ Soluția va permite resetarea la configurațiile inițiale ("din fabrică");
Alimentare	<p>Pentru asigurarea redundanței complete a echipamentului propus fiecare element major component al componentei centrale de protecție avansată antimalware trebuie să ofere alimentare redundantă prin cel puțin două surse independente de alimentare. Sursele trebuie să ofere funcționalitate hot-swap pentru înlocuirea rapidă, fără oprirea alimentării sistemului și fără întreruperea serviciilor asigurate de platformă;</p>
Ventilație	<p>Toate elementele de asigurare a ventilației sistemului trebuie să fie de tip hot-swap pentru înlocuirea lor rapidă în caz de avarie, fără întreruperea funcționalităților oferite de platformă;</p>
Cerințe constructive	<ul style="list-style-type: none"> ▪ Componenta centrală de protecție avansată antimalware trebuie să fie montabilă în rack-uri standard de 19"; ▪ Ofertantul trebuie să livreze un kit cu elementele de fixare/instalare în rack (suporturi, șuruburi/captive);



[Handwritten signature]


[Handwritten signature]

<p>Garanție si suport</p>	<ul style="list-style-type: none"> ▪ Pentru toate elementele si modulele integrate, solutia va include garantie de minim 36 de luni. Suportul si garantia trebuie asigurate in Romania de producatorul respectivelor echipamente; ▪ Garantia hardware va fi asigurata cu un SLA (Service Level Agreement) de 8x5xNBD (8 ore pe zi, 5 zile pe saptamana, cel mai tarziu a doua zi lucratoare – Next Business Day), care sa garanteze diagnosticarea echipamentului sau modulului defect si inlocuirea acestuia in maxim 3 zile lucratoare, fara alte costuri; ▪ Se va asigura acces 24x7 in centrul de suport al producatorului, cu posibilitatea raportarii problemelor aparute in functionare si solicitarea rezolvarii acestora in functie de severitate. De asemenea se va asigura dreptul de a face update-uri si upgrade-uri software (sistem de operare, firmware, etc).
---------------------------	---

4.4.1.18 Componenta de protecție a resurselor la nivel de post de lucru

Componenta de protectie a resurselor la nivel de post de lucru trebuie sa indeplineasca urmatoarele specificatii tehnice minime:

Caracteristica	Cerinta tehnica minimala
<p>Arhitectura</p>	<ul style="list-style-type: none"> ▪ Solutia va asigura protectia mediilor fizice (cu suport pentru o plaja larga de sisteme de operare), a mediilor virtuale (in principal pentru platforma de virtualizare ofertata, respectiv pentru VMware vSphere, Microsoft Hyper-V, Citrix Xen Server, Open Stack, containere Docker, etc) si sistemelor de tip cloud public (VMware, Amazon AWS, Microsoft Azure, etc); ▪ Solutia va oferi flexibilitate in licentiere, configurare, distributie si operare, astfel incat se va putea configura local, Software-as-a-Service sau prin intermediul Marketplace in Amazon AWS si Microsoft Azure; ▪ In mediile virtuale trebuie sa functioneze in mod agentless, asigurand protectie avansata pentru toate sistemele instalate in platforma de virtualizare, respectiv automatizarea fluxurilor de securitate prin izolarea sistemelor in zonele de carantina ale retelelor virtuale segmentate; ▪ Platforma va asigura acoperire si vizibilitate completa in toate punctele din retea, astfel incat permite detectarea atacurilor



	<p>directionate, de tip ransomware si a amenintarilor avansate persistente;</p> <ul style="list-style-type: none">▪ Va include functionalitate de tip sandbox nativa prin intermediul componentei centrale de protecție avansată antimalware, fara a necesita platforma hardware dedicata acestei functionalitati;
Detectie si protectie amenintari avansate	<ul style="list-style-type: none">▪ Solutia trebuie sa includa un motor de detectie si preventie a elementelor de tip malware, bazat pe serviciu de reputatie al aplicatiilor/serviciilor/proceselor, motor ce va oferi cel puțin urmatoarele functionalitati:<ul style="list-style-type: none">▪ Analiza si detectia elementelor de tip virus, spyware, grayware, ransomware, exploit, etc;▪ Analiza proceselor si a zonelor de memorie in care respectivele procese ruleaza;▪ Analiza comportamentala pentru aplicatii si procese;▪ Corelarea amenintarilor detectate in toate sistemele de tip endpoint analizate (sisteme de lucru, servere, etc);▪ Detectarea amenintarilor inainte de a se executa efectiv, folosind algoritmi matematici de predictie, dar si analiza comportamentala, proces ce va ajuta la detectarea amenintarilor in timpul executiei acestora, folosind sabloane comportamentale;▪ Solutia trebuie sa includa un motor de detectie si preventie a elementelor de tip malware, bazat pe un serviciu de reputatie a adreselor web, motor ce va oferi cel puțin urmatoarele functionalitati:<ul style="list-style-type: none">▪ Va colaboreaza cu motorul anti-malware descris mai sus, pentru a furniza un rating al resurselor URL accesate de sistemul analizat;▪ Va permite functionarea in mod detectie/protectie cu comportament asemanator cu cel al unui proxy de retea, inasa pentru sistemul pe care ruleaza;▪ Solutia trebuie sa includa un motor de detectie si preventie a elementelor de tip malware, bazat pe un serviciu de tip host firewall/IDS/IPS, motor ce va oferi cel puțin urmatoarele functionalitati:<ul style="list-style-type: none">▪ Motor de tip firewall flexibil ce poate functiona in mod restrictiv sau permisiv, prin utilizarea modurilor tap si/sau inline;

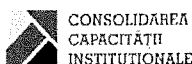


Handwritten signature

Handwritten signature



- Va putea aplica politici de detectie/monitorizare sau de protectie/blocare, plus strategii permissive ("allow all/deny explicit") sau restrictive ("deny all/allow explicit");
- Blocarea/filtrarea se va putea face dupa: sursa/destinatie, adresa IP/MAC, porturi de comunicatie, tip de trafic (TCP/UDP);
- Ve permite scanarea porturilor deschise pe sistemele de tip endpoint si va oferi optiuni de blocare sau doar de jurnalizare a evenimentelor;
- Motor de tip IDS/IPS ce va permite actualizarea software (Virtual Patching) pentru sisteme de operare, aplicatii si servere de aplicatii;
- Motor de scanare de vulnerabilitati, ce se va putea initia printr-un proces de scanare recomandata si va permite identificarea in mod particularizat a informatiilor (profiling) legate de sistemul pe care ruleaza agentul: sistem de operare, aplicatii, servere de aplicatii, etc, respectiv va descarca semnaturile actualizarilor software pentru elementele detectate;
- Semnaturile detectate prin procesul de scanare se vor putea aplica in mod automat pe sistem, la fiecare activitate de scanare, astfel incat sa nu necesite interventie din partea administratorului. Aplicarea automata a patchurilor virtuale nu va impacta disponibilitatea si/sau functionalitatea serviciilor;
- Motorul de scanare de vulnerabilitati va asigura detectia continua si aplicarea automata a actualizarilor software din momentul zero al aparitiei vulnerabilitatilor respective;
- Va permite inspectia traficului de tip SSL;
- Solutia trebuie sa includa un motor de control automatizat al aplicatiilor, motor ce va oferi cel putin urmatoarele functionalitati:
 - Va asigura urmarirea devierilor de la setul initial de aplicatii instalate, prin compararea unui baseline de inventar de aplicatii cu situatia curenta rezultata dintr-o operatiune de analiza;
 - Se vor putea folosi seturi de reguli (inventar de configurare) partajate intre mai multe sisteme cu inventare asemanatoare de aplicatii;
 - Se vor putea urmari modificari ale aplicatiilor la mai multe niveluri: denumire fisier, cale sau locatie, marca de timp,



	<p>permisiuni, continut fisiere, folosind metode de comparatie la nivel de hash, dimensiune fisier, cale sau denumire fisier;</p> <ul style="list-style-type: none">▪ In urma detectarii unor modificari in lista de aplicatii instalate, se vor putea configura actiuni de blocare sau aprobare a executiei;▪ Solutia trebuie sa includa un motor de asigurare a integritatii fisierelor, serviciilor si aplicatiilor, motor ce va oferi cel putin urmatoarele functionalitati:<ul style="list-style-type: none">▪ Detectarea modificarilor realizate la nivel de fisiere sau zone critice de sistem (fisiere de tip DLL/EXE, directoare, registrul Windows, procese, porturi de retea deschise, in directoare temporare, in Recycle Bin, fisierul hosts, aplicatiile ce ruleaza la pornirea sistemului de operare, fisierele de configurare a setarilor de retea, in Task Scheduler, a conturilor de utilizator, a aplicatiilor de tip browser, in directorul Windows, System32, etc) ce pot indica o activitate suspicioasa;▪ Motorul va dispune de reguli predefinite pentru sistemele de operare cunoscute, astfel incat, in urma unui proces de analiza, se va construi un baseline ce va ajuta la identificarea tuturor tipurilor de fisiere prezente pe sistem;▪ Va permite configurarea analizelor intr-un interval orar, respectiv in timp real, cu prioritate de resurse ridicata sau scazuta;▪ Solutia trebuie sa includa un motor de inspectie a jurnalelor de sistem, motor ce va oferi cel putin urmatoarele functionalitati:<ul style="list-style-type: none">▪ Va permite identificarea evenimentelor importante din multitudinea de evenimente de securitate/operationale ce sunt generate in mod curent de sistemele de operare/servicii/aplicatii (Squid, jurnale de sistem Windows, jurnale de sistem generate de aplicatii si servicii native Microsoft Windows Server: IIS, Routing and Remote Access Server, Terminal Server, AD Server, Exchange Server, DHCP, DNS, etc);▪ Va permite detectarea comportamentelor suspicioase, colectarea evenimentelor din sisteme de operare si servere de aplicatii diverse, identificarea evenimentelor operationale problematice, crearea si mentinerea unei liste de evenimente
--	---

	<p>administrative, precum și satisfacerea unor cerințe de conformitate (ex: PCI DSS);</p> <ul style="list-style-type: none">▪ Evenimentele vor fi detectate în baza unei analize ce va detecta categoria de evenimente ce se doresc urmărite (ex: Database Server - MSSQL, FTP Server - ProFTPD, Mail Server - Microsoft Exchange, etc);▪ Soluția va oferi următoarele mecanisme integrate de detecție și prevenție a amenințărilor informatice avansate:<ul style="list-style-type: none">▪ Descoperirea sistemelor prin maparea structurii extrase din sisteme de tip directory (Active Directory sau similar), prin analiza unui set de adrese IP, prin integrarea directă cu platformele de management al mediilor de virtualizare (în special cu platforma de management al soluției de virtualizare oferite, VMware vSphere, Microsoft Hyper-V, etc);▪ Va permite aplicarea de politici în mod automat în funcție de apartenența la un astfel de grup de resurse descoperite, astfel ca orice sistem virtual din platforma de virtualizare, respectiv orice sistem fizic (stație de lucru și/sau server) va putea fi automat protejat în funcție de criteriile de apartenență;▪ Soluția va oferi suport pentru următoarele sisteme de operare: Microsoft Windows Server 2003/2003 R2/2008/2008 R2/2012/2012 R2/2016, Microsoft Windows 7/8/8.1/10, Red Hat Linux 5/6/7, CentOS 5/6/7, Suse Linux, Oracle Linux, Debian, Ubuntu;▪ Soluția va include o platformă de management dedicată, integrată nativ cu componenta centrală de protecție avansată antimalware, respectiv cu funcționalitatea de tip sandbox disponibilă în aceasta;▪ Platforma de management va oferi suport de instalare pentru următoarele baze de date: Microsoft SQL, Postgres, etc;▪ Platforma de management va putea fi instalată în topologie redundanță de tip cluster activ-activ;▪ Platforma de management va permite integrarea cu sisteme de tip directory (Active Directory, LDAP, etc) și platforme de management al mediilor de virtualizare (în special cu platforma de management al soluției de virtualizare oferite, VMware vSphere, Microsoft Hyper-V, etc);
--	--



M. Blis

[Handwritten signatures]

	<ul style="list-style-type: none"> ▪ Platforma de management va permite nativ definirea de utilizatori locali si roluri de utilizare, cu seturi diferite de permisiuni granulare aplicabile actiunilor administrative si/sau seturilor de date. Deasemenea trebuie sa permita integrarea cu un sistem director de tip LDAP, pentru sincronizarea utilizatorilor si a drepturilor de acces. Pentru sporirea securitatii in mecanismele de autentificare, platforma trebuie sa permita integrarea cu un sistem NTP/SNTP pentru sincronizarea informatiilor de timp; ▪ Platforma de management va permite activarea agentilor pe sistemele endpoint in mod automat/manual, cu/fara parola de activare, respectiv reactivarea agentilor pe masinile virtuale ce au fost clonate/copiate; ▪ Platforma de management va oferi acces securizat prin HTTPS (TLS), respectiv va oferi optiuni de autentificare multi-factor; ▪ Platforma de management va oferi posibilitatea de trimiterea a jurnalelor si evenimentelor catre sisteme de tip Syslog/SIEM, respectiv va oferi mesaje SNMP catre sistemele de monitorizare a infrastructurii;
<p>Functionalitati de tip Sandbox</p>	<p>Prin integrarea nativa cu componenta centrală de protecție avansată antimalware solutia ofertata va include functionalitate integrata pentru procesele specifice activitatilor de tip "sandbox":</p> <ul style="list-style-type: none"> ▪ Va permite analiza elementelor suspecte, dupa filtrarea lor prealabila efectuata de modulele de detectie a amenintarilor avansate; ▪ Va permite functionalitati avansate de evitare a evadarii din sandbox, precum si un mod de "safe live" pentru analiza unor descarcari multi-nivel, URL, Comamnd & Control, etc; ▪ Va oferi urmatoarele metode de analiza si detectie: ▪ Soluția trebuie să fie capabilă să detecteze și să prevină software-ul malițios avansat, atacuri de tipul „zero-day” și de tip APT (Advanced Persistent Threat) direcționate; ▪ Soluția trebuie să detecteze software-ul malițios de tip "zero-day multi-stage" și atacuri direcționate fără o cunoaștere prealabilă a software-ului malițios; ▪ Analiza statica, euristica si comportamentala; ▪ Analiza bazata pe reputatia adreselor si fisierelor pentru URL-uri;



[Handwritten signature]

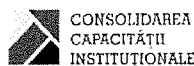
[Handwritten signature]

- Analiza conexiunilor de rețea outbound sau de mesagerie suspicioase;
- Analiza fișierelor suspicioase ce efectuează conexiuni la servere de tip Command & Control;
- Analiza atacurilor de tip ransomware, deception, social-engineering, hijack, redirectionare și/sau furt de date, rootkit cloaking;
- Analiza operațiunilor cu fișiere: file drop, download, partajare și/sau replicare de fișiere;
- Analiza operațiunilor ce vizează modificările de procese, servicii sau obiecte de memorie;
- Evaluarea continuă a amenințărilor, acțiunilor întreprinse de elementele malware și impactul asupra sistemului analizat;
- Mecanisme incluse de analiză de tip forensics, cel puțin prin captura pachetelor de date relevante (PCAP);
- Soluția trebuie să asigure procese de analiză cu suport atât pentru arhitecturi de tip x86 cât și pentru arhitecturi de tip x64;
- Soluția trebuie să asigure restaurarea mașinilor virtuale de analiză la o configurație de bază după finalizarea analizei unui software malițios, automat sau manual;
- Mașinile virtuale preinstalate vor avea configurate aplicații de tip browser (cel puțin Internet Explorer, Mozilla Firefox, Google Chrome, Safari), plugin-uri (cel puțin Adobe Flash, Adobe Shockwave, Adobe Air) precum și aplicații uzuale (cel puțin Adobe Acrobat Reader, Microsoft Office Word, Excel, Powerpoint, Outlook, Oracle Java JRE, Windows Media Player, Quicktime Player);
- Soluția trebuie să asigure cel puțin analiza celor mai comune tipuri de fișiere cunoscute ca fiind folosite pentru distribuirea sau găzduirea de aplicații malware (fișiere executabile – EXE, DLL, documente Microsoft Office – DOC, DOCX, XLS, XLSX, PPT, PPTX, documente PDF, fișiere JAR, BAT, fișiere de tip imagine, fișiere de tip video, Flash, arhive – ZIP, RAR, SFX);
- Soluția trebuie să asigure extinderea tipurilor de fișiere ce pot fi analizate;
- Soluția trebuie să asigure cel puțin analiza obiectelor Web prin furnizarea unui URL;

	<ul style="list-style-type: none">▪ Soluția trebuie să fie capabilă să simuleze acțiuni ale utilizatorilor finali (interacțiunea dintre mașina virtuală de analiză și utilizator) în scopul de a forța executarea de software malițios care se bazează pe astfel de acțiuni (de exemplu un click de mouse, răspuns la ferestre dialog sau parcurgerea unor pași de instalare) sau pe observarea prezenței utilizatorului (prin apelarea unor funcții Windows native sau din interfața Windows API);▪ Soluția trebuie să asigure jurnalizarea apelurilor de funcții Windows native și din interfața Windows API relevante pentru depistarea comportamentului malițios;▪ Soluția trebuie să asigure identificarea și rularea software-ului malițios care are capacitatea de a identifica mediile virtualizate sau emulate;▪ Soluția trebuie să genereze un set de indicatori de compromitere după execuția virtuală a software-ului malițios;▪ În cazul unui atac soluția trebuie să raporteze cel puțin IP-ul sursă, IP-ul destinație, serverul de tip Command & Control, URL-ul, botname-ul, clasa de malware, protocoalele utilizate și severitatea infecției;
Funcționalități de detecție și prevenție a scurgerilor de date	<p>Soluția oferită trebuie să includă un motor de detecție și prevenție a scurgerilor de informații, motor ce va oferi cel puțin următoarele funcționalități:</p> <ul style="list-style-type: none">▪ Recunoașterea în timp real a conținutului și contextului unui anumit fișier sau a unei informații;▪ Învățarea folosind informații confidențiale/senzitive deja existente (exemplu: conținutul documentelor definite ca fiind confidențiale să poată fi identificat în alte documente dacă procentul de asemănare depășește o valoare prestabilită și care poate fi configurată);▪ Recunoașterea și analizarea conținutului a cel puțin 300 de tipuri de fișiere diferite (funcționalitatea trebuie să fie disponibilă pentru utilizare fără o configurare specială - out of the box);▪ Asigurarea lucrului cu documente scrise în limba română (cel puțin activitățile de detectare, amprentare și indexare a acestora);▪ Setarea unui procent minim de detecție pentru fișierele amprentate;



- Inspectarea conținutului în baza unor liste de cuvinte/fraze cheie mari, fără degradarea performanței;
- Asigurarea detectării pe baza conținutului și nu pe baza extensiei fișierelor;
- Protejarea conținutului prin metode de detecție bazate pe un set redus de documente care să asigure o detecție corectă a unor documente similare;
- Specificarea coloanelor de date amprentate care să declanșeze un incident (de exemplu, prenume, nume de familie, adresă și CNP) și a celor care să nu declanșeze un incident (de exemplu, prenume și nume de familie);
- Detectarea comunicațiilor sau a fișierele criptate;
- Posibilitatea de a utiliza o singură politică de scanare a conținutului indiferent dacă informația este stocată sau utilizată în rețea sau pe stația de lucru;
- Stocarea incidentelor și a detaliilor aferente acestora în mod criptat în baza de date a platformei de management;
- Posibilitatea de a normaliza diverse variante ale prezentării datelor (exemplu: dacă documentul conține un string "123456789", să se declanșeze alerte cel puțin la variante de forma "123-456-789", "123.456.789", "[123][456][789]");
- Definirea unor tipuri de noi de fișiere care să fie recunoscute și analizate chiar dacă nu sunt în lista de fișiere recunoscute implicit;
- Configurarea de reguli multiple de răspuns la un incident cel puțin în funcție de severitate și politica ce a declanșat incidentul;
- Evidențierea în pagina de afișare a incidentului a motivelor principale care au dus la violarea unei politici;
- Corelarea după expeditor, destinatar, nume fișier, proprietarul fișierului, numele utilizatorului sau politica declanșată;
- Emiterea de rapoarte de sumarizare pe nivele multiple (grupate cel puțin pe utilizatori, politici, severitate sau alte criterii disponibile);
- Extragerea de atribute despre utilizatori din structura de tip Active Directory existentă și includerea acestora în informațiile despre incidentele generate;



[Handwritten signature]

[Handwritten signature]

	<ul style="list-style-type: none"> ▪ Permiteea adăugării oricărui atribut structură de tip Active Directory în platforma de management a soluției și în detaliile incidentelor; ▪ Se vor putea rula cel puțin următoarele tipuri de rapoarte aferente incidentelor: lista incidentelor, lista personalizată a incidentelor după caracteristici specifice, lista incidentelor declanșate de funcțiile de căutare la nivelul stațiilor de lucru; ▪ Filtrarea avansată pe nivele a incidentelor după diverse reguli definibile: configurația agentului, starea configurației agentului, numele aplicației care a generat incidentul, numele fișierului, locația fișierului, mărimea fișierului, adresa de email a proprietarului fișierului, numele proprietarului fișierului, adresa de IP a destinației, data detecției, identificatorul stației care a generat incidentul, numele domeniului asociat incidentului, locația stației care a generat incidentul, ultima dată la care a fost modificat fișierul, data la care au fost generate incidentele, adresa de IP a stației care a generat incidentul, protocol, lista de control a accesului la fișierul care a generat incidentul, lista de control a partajării fișierului care a generat incidentul, existența anterioară a incidentului, etc; ▪ Monitorizarea și identificarea datelor confidențiale din fișierele arhivate (comprimate); ▪ Inspectarea recursivă a arhivelor (zip, rar, tar) și detecția în interiorul arhivelor incluse pe mai multe niveluri; ▪ Efectuarea de acțiuni manuale sau automate ca răspuns la încălcarea unei politici (pe care le poate lua o persoană competentă sau soluția în urma configurării politicilor); ▪ Furnizarea unui set extins de politici predefinite bazate pe legislație și/sau standarde de conformitate sau pe bunele practici în domeniu, set care să poată fi modificat/particularizat în funcție de necesități; ▪ Definirea de politici bazate pe informații din structura de tip Active Directory (cel puțin departament, OU, group, user);
<p>Raportare</p>	<p>Platforma de management inclusa in componenta de protecție a resurselor la nivel de post de lucru trebuie sa ofere urmatoarele capabilitati de raportare centralizata, indiferent de tipul si numarul agentilor din solutie:</p>

- Solutia trebuie să prezinte rezultatele analizei software-ului malițios sub forma unui tablou de bord grafic (dashboard) și/sau a unui raport care detaliază comportamentul amenințării;
- Solutia trebuie să permită reconfigurarea tabloului de bord grafic prin folosirea unor elemente de tip widget (cel puțin pentru top amenințări/URL-uri, top sisteme cu evenimente de securitate, top comportamente suspicioase, top sisteme infectate, top sisteme exploatare, top aplicații/fisiere cu comportament suspicios, traficul în timp real generat de procesele de analiză și detecție, etc);
- Raportul furnizat va conține cel puțin următoarele informații:
 - Tipul fișierului analizat;
 - Sumele de control (MD5, SHA) ale fișierelor analizate sau create pe mașina virtuală de analiză;
 - Dacă fișierul este executabil se va preciza dacă au fost folosite aplicații de tip packer și tipul acestora;
 - Informații extrase din header-ul fișierelor executabile;
 - Modificările produse la nivelul sistemului de operare;
 - Modificările produse la nivelul aplicațiilor instalate;
 - Modificările produse asupra sistemului de fișiere;
 - Modificările produse asupra regiștrilor;
 - Librării DLL încărcate la rulare;
 - Funcțiile API apelate, în ordine cronologică;
 - Informații despre procesele create/modificate/oprite;
 - Informații despre serviciile create/modificate/oprite;
 - Obiecte de tip Mutex create;
 - Eventuale hook-uri SSDT, IDT sau IRP create;
 - Eventuale conexiuni de rețea create și protocoalele de transport folosite;
 - Interogările DNS;
 - URL-urile accesate;
 - Adrese IP contactate și porturile logice folosite;
 - Informații de localizare geografică a adreselor IP contactate;
 - Captura zonelor de memorie aferente proceselor suspecte de comportament malițios;
 - Tipul de exploit folosit;

	<ul style="list-style-type: none">▪ Solutia trebuie sa permita emiterea de rapoarte de sumarizare pe nivele multiple (grupate cel puțin pe utilizatori, politici, severitate sau alte criterii disponibile);▪ Se vor putea rula cel puțin următoarele tipuri de rapoarte aferente incidentelor de scurgere de informatii: lista incidentelor, lista personalizată a incidentelor după caracteristici specifice, lista incidentelor declanșate de funcțiile de căutare la nivelul stațiilor de lucru/serverelor;▪ Solutia trebuie sa permita ordonarea/re-ordonarea campurilor din raport dupa coloana/coloanele selectate (indicator de risc al sistemelor, faza de atac, numele sistemelor, adresa IP, data la care a survenit atacul, etc);▪ Soluția trebuie să permită exportul rapoartelor și al alertelor despre software-ul malițios cel puțin în format PDF, HTML și XLS;▪ Soluția trebuie să suporte automatizarea raportării cel puțin pentru următoarele intervale de timp: zilnic, săptămânal, lunar și definit de utilizator;
Integrare	<ul style="list-style-type: none">▪ Solutia ofertata trebuie sa se integreze nativ cel puțin cu următoarele tipuri de servicii oferite de producatorul solutiei (servicii ce vor permite actualizarea automata, neasistata a definițiilor de elemente malware):▪ La nivelul filtrării URL: Serviciu de analiza bazat pe reputatia adreselor și fisierelor pentru URL-uri, respectiv motor intern responsabil de scanarea, detectarea și atasarea unui scor de risc fiecărei resurse URL solicitate și accesate. Acest motor trebuie sa permita și scanarea retroactiva pentru elementele malițioase de tip Command & Control;▪ La nivelul filtrării de fisiere: Serviciu de analiza bazat pe reputatia fisierelor cunoscute de la producatori cunoscuti, pentru a putea efectua procesele de comparare cu fisierele detectate in analiza locala, respectiv serviciu global de identificare a fisierelor malițioase prin colectarea datelor de la toti senzorii pe care producatorul solutiei ofertate ii are instalati la nivel global;▪ La nivelul aplicatiilor mobile: Serviciu de analiza bazat pe reputatia aplicatiilor mobile, in vederea detectarii unor activitati malițioase, utilizarii de resurse și incalcării ale nivelurilor de confidentialitate;



Handwritten signature

Handwritten signature

	<ul style="list-style-type: none"> ▪ Soluția trebuie să ofere un API de interfațare cu alte produse terțe (specific cu producătorul Componentei de protecție la nivel de rețea oferite, respectiv cel puțin cu următorii producători de soluții de securitate: Check Point, IBM Security, Palo Alto Networks, F5 Networks, BlueCoat, A10 Networks, etc) pentru transmiterea de solicitări de analiză și extragere de rezultate, inclusiv partajare de obiecte suspicioase și indicatori de compromis; ▪ Soluția trebuie să permită integrarea nativă cu Componenta centrală de protecție avansată antimalware oferită, asigurând monitorizarea la nivel de context a posturii de securitate a întregului ecosistem, respectiv raportarea activităților detaliate de sistem, precum și natura și dimensiunea oricărui atac survenit; ▪ Soluția trebuie să permită integrarea nativă cu produse de tip SIEM pentru transferul evenimentelor cel puțin prin mecanisme UDP/TCP/SSL; ▪ Soluția trebuie să permită integrarea descriptorilor malware cu soluții terțe (ex: YARA);
<p>Garanție și suport</p>	<ul style="list-style-type: none"> ▪ Pentru toate elementele și modulele integrate, soluția va include garanție de minim 36 de luni. Suportul și garanția trebuie asigurate în România de producătorul respectivei soluții sau prin partener autorizat; ▪ Se va asigura acces 24x7 în centrul de suport al producătorului, cu posibilitatea raportării problemelor aparute în funcționare și solicitarea rezolvării acestora în funcție de severitate. De asemenea se va asigura dreptul de a face update-uri și upgrade-uri software.

4.4.1.19 Componenta de management a datelor de audit

Componenta de management a datelor de audit trebuie să îndeplinească următoarele **specificatii tehnice minime**:

Caracteristica	Cerința tehnică minimă
Arhitectura	<ul style="list-style-type: none"> ▪ Soluția va asigura managementul datelor de audit din mediile fizice (cu suport pentru o plajă largă de sisteme de operare) și

	<p>mediile virtuale (in principal pentru platforma de virtualizare ofertata);</p> <ul style="list-style-type: none"> ▪ Solutia va oferi flexibilitate in licentiere, configurare, distributie si operare, astfel incat se va putea configura local, Software-as-a-Service sau prin intermediul Marketplace in Amazon AWS si Microsoft Azure; ▪ Platforma va asigura acoperire si vizibilitate completa in toate punctele din retea, astfel incat va permite managementul datelor de audit pentru intreaga infrastructura; ▪ Solutia va permite instalarea in topologie multiplu-redundanta de tip cluster activ, cu posibilitatea de scalare orizontala (multiple noduri de procesare) si verticala (adaugarea de resurse de procesare), respectiv va permite instalarea in topologie multi-site;
<p>Functionalitati de management a datelor de audit</p>	<p>Solutia ofertata trebuie sa asigure urmatoarele capabilitati si functionalitati:</p> <ul style="list-style-type: none"> ▪ Va permite importul datelor din sisteme relationale de baza de date, cu suport cel putin pentru: Microsoft SQL Server, Oracle Database, MySQL, PostgreSQL, etc; ▪ Va permite agregarea datelor din fisiere sistem, jurnale de audit specifice si comunicatie directa de tip syslog (peste retea prin porturi definibile TCP/UDP) pentru sisteme de operare, echipamente hardware, aplicatii, servicii, servicii API, etc; ▪ Analiza datelor de audit se va face in baza unor metrici (puncte numerice de date in relatie directa cu datele de audit colectate intr-un anumit interval de timp) ce pot fi comprimati, stocati si procesati mult mai eficient decat datele de jurnalizare clasice; ▪ Cautarea datelor relevante pentru analiza informatiilor de audit se va face pe baza unei scheme de cautare (parametrii de cautare agregati) ce va fi construita in timp real la momentul executarii cautarii si va putea fi rulata inclusiv asupra datelor ce sunt colectate in timp real; ▪ Datele de audit colectate vor fi stocate in format brut pentru a nu fi nevoie de transformari mari consumatoare de timp si resurse de procesare, respectiv pentru a facilita procesul de cautare in timp real asupra datelor colectate;

- Determinarea automată a marilor temporale, atât pentru datele ce sunt colectate și analizate în timp real (chiar și pentru formate atipice de marci temporale), cât și pentru datele ce nu conțin o marcă temporală (soluția trebuie să ataseze o marcă temporală bazată pe context);
- Procesele de căutare și investigație asupra datelor de audit colectate trebuie să se realizeze în timp real indiferent de tipul și mărimea seturilor de date colectate, respectiv să ofere suport pentru cel puțin următoarele tipuri de corelare a datelor: timp, tranzacții, căutări/cautări subsecvente în rezultatele regasite, alipiri ale termenilor de căutare, etc;
- Soluția trebuie să permită atât căutarea în timp real asupra datelor de audit colectate, cât și afișarea rezultatelor în context istoric asupra aceluiași set de date analizate. Trebuie să permită căutarea cu operatori de tip Boolean, bazată pe câmpuri multiple de căutare, căutarea statistică, respectiv căutarea subsecventă în rezultatele regasite. Rezultatele și modele de date trebuie să poată fi afișate pe măsură ce procesele de căutare se execută, permițând corelarea facilă a evenimentelor de audit. Căutările trebuie să poată fi salvate și rulate la o dată ulterioară, respectiv să poată fi integrate ca obiecte de tip widget în panoul de afișare central;
- Soluția trebuie să permită agregarea, corelarea și căutarea unor colecții de evenimente din sisteme și aplicații diferite ce fac în parte dintr-o singură tranzacție/set de tranzacții (evenimente ce sunt generate de o acțiune/un set de acțiuni de un anumit tip însa la îndeplinirea lor se generează evenimente de audit într-un set larg de echipamente, sisteme și aplicații – Ex.: Trimiterea unui e-mail, plasarea unei comenzi într-un site web, plasarea unui apel de video-conferință, etc);
- Soluția trebuie să permită afișarea interactivă a rezultatelor căutării datelor de audit, cu posibilitatea de a mari/micsora în timp real perioada de timp, pentru a identifica tendințe, varfuri și anomalii ale datelor analizate. Trebuie să includă posibilitatea de a face "drill-down" asupra reprezentărilor grafice a evenimentelor de audit pentru a afișa direct datele în format brut ce au generat respectivele grafice, respectiv posibilitatea de a defini afișări personalizate pentru oricare set de date;

- Solutia trebuie sa ofere posibilitatea de esantionare a seturilor de date de audit, astfel incat sa permita regasirea si analiza rapida a datelor relevante la termenii de cautare folositi;
- Solutia trebuie sa permita corelarea evenimentelor complexe din seturi de date foarte mari, respectiv dintr-un numar foarte mare de surse (sisteme, aplicatii, servicii, etc) pentru evenimente de audit ce aparent nu au nici o legatura evidenta. Corelarea trebuie sa se faca cel putin in functie de: timp, locatia geografica, tranzactii, cautarea subsecventa in rezultatele regasite, cautarea bazata pe campuri, alipiri ale termenilor de cautare, etc);
- Solutia trebuie sa permita adnotarea evenimentelor de audit pentru a adauga context suplimentar de corelare;
- Solutia trebuie sa permita detectia modelelor relevante indiferent de sursa si tipul datelor de audit;
- Solutia trebuie sa permita folosirea a diferite seturi de date (modele de date pentru a descrie relatiile dintre evenimentele de audit, tabele pentru afisarea structurata a datelor complexe de audit, "lookups" pentru extinderea si imbogatirea datelor de audit prin integrari cu surse externe de date) pentru a defini si mentine colectii structurate a datelor ce pot fi folosite/refolosite in constructia modelelor de analiza si raportare;
- Posibilitatea de a crea afisari pe baza de tabele, afisari ce permit imbunatatirea, rafinarea, filtrarea si agregarea datelor de audit. Afisarile vor putea fi exportate si partajate cu alti utilizatori ai solutiei, respectiv vor permite crearea de rapoarte si elemente in panoul centralizat de afisare;
- Solutia va permite generarea de afisari personalizate a tabloului de bord (dashboard) pentru tulizatori diferiti ai solutiei, respectiv va permite generarea, exportul si distributia de rapoarte personalizate cel putin in format PDF;
- Solutia va permite folosirea de reprezentari grafice de tip chart predefinite, pentru a reprezenta datele de audit corelate, respectiv va permite definirea de noi vizualizari grafice ce vor putea fi partajate cu alti utilizatori ai solutiei;
- Solutia va permite definirea de alerte pentru evenimentele de audit critice, alerte ce vor putea declansa actiuni sau seturi de actiuni de alertare a utilizatorilor solutiei (alertare prin e-mail, SNMP, executarea scripturilor de remediere, etc). Alertele vor fi

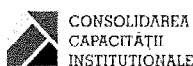
	<p>personalizabile si vor putea fi definite cel putin in functie de: limite variabile realtiv la datele de audit, tendintele evenimentelor de audit, modele complexe de corelare a evenimentelor de audit (ex: atacuri de forta bruta, scenarii de frauda, etc);</p> <ul style="list-style-type: none"> ▪ Solutia va permite integrarea nativa cu aplicatii terte prin intermediul unui API ce exporta intregul set de functionalitati, respectiv prin conexiune directa de tip ODBC; ▪ Solutia va permite integrarea nativa cu sisteme de tip Hadoop, oferind mecanisme integrate de import bi-directional si cautare in seturile de date de audit; ▪ Solutia va permite extinderea functionalitatilor prin aplicatii terte, nativ compatibile, aplicatii ce se vor instala ca module in solutia ofertata;
<p>Management</p>	<ul style="list-style-type: none"> ▪ Solutia va permite nativ definirea de utilizatori locali si roluri de utilizare, cu seturi diferite de permisiuni granulare aplicabile actiunilor administrative si/sau seturilor de date. Deasemenea trebuie sa permita integrarea cu un sistem director de tip LDAP (Active Directory, Sun e-Directory, etc) pentru sincronizarea utilizatorilor si a drepturilor de acces, respectiv cu sisteme Single Sign-On in tehnologie SAML (Okta, Ping Federate, Azure AD, CA SiteMinder, OneLogin, etc). Pentru sporirea securitatii in mecanismele de autentificare, platforma trebuie sa permita integrarea cu un sistem NTP/SNTP pentru sincronizarea informatiilor de timp; ▪ Solutia va oferi acces securizat prin HTTPS (TLS), respectiv prin protocol SSH; ▪ Solutia va oferi un panou central de monitorizare a modulelor si componentelor (afisari ale topologiei, starea generala a sistemului, starea individuala a componentelor cu posibilitati de alertare, performanta si capacitatea sistemului, interconectarea componentelor sistemului, etc);
<p>Garanție si suport</p>	<ul style="list-style-type: none"> ▪ Solutia va include garantie de minim 36 de luni. Suportul si garantia trebuie asigurate in Romania de producatorul respectivei solutii sau prin partener autorizat; ▪ Se va asigura acces 24x7 in centrul de suport al producatorului, cu posibilitatea raportarii problemelor aparute in functionare si solicitarea rezolvarii acestora in functie de severitate. De

asemenea se va asigura dreptul de a face update-uri si upgrade-uri software.

4.4.1.20 Componenta portal

Componenta Portal ce va asigura interacțiunea utilizatorilor externi cu Buletinul Electronic al Registrului Comertului trebuie să respecte următoarele cerințe tehnologice:

- Va oferi suport pentru tehnologii și standarde deschise;
- Va oferi suport multi-lingvistic pentru prezentare;
- Va oferi suport multi-home pentru instalarea de servere multiple pe aceeași mașină fizică;
- Va fi compatibilă cu standardele platformei Java 2 Enterprise Edition (J2EE) sau echivalentă;
- Va oferi Portleți predefiniți care să permită gestiunea publicării de pagini web, gestiunea de documente, gestiunea de formulare web, etc ;
- Va oferi suport multi-site, multi-portal pentru aplicații distincte instalate pe aceeași mașină fizică;
- Va furniza un unic punct de acces către aplicațiile și serviciile electronice din sistem;
- Accesul la conținut se va face printr-un navigator Web de tip Internet Explorer, Mozilla Firefox, Safari, Chrome sau echivalent;
- Va oferi o vedere unică, consistentă asupra unei game variate de surse de informații și în concordanță cu acțiunile pe care utilizatorul le are de realizat;
- Interfața prezentată utilizatorului după autentificare va conține modalitățile de acces strict legate de aplicațiile la care utilizatorul are drepturi de acces în funcție de drepturile acordate;
- Conținutul accesat va fi automat ajustat, pe baza rolurilor predefinite ale utilizatorilor în funcție de drepturile acordate;
- Sa includa suport pentru integrarea cu sistemul de gestiune a identității utilizat în cadrul ONRC (Oracle Access Manager);
- Sa includa suport pentru autentificare prin LDAP, producator SAML si consumator OAuth;
- Interfață web standardizată, simplă și intuitivă;
- Interfață cu utilizatorii bogată în funcționalități, care să ofere un nivel ridicat de accesibilitate, conform cu cerințele de accesibilitate WCAG versiunea 1.0 sau echivalente;
- Interfață web cu template disponibil gratuit pentru look & feel comun organizației;
- Grad ridicat de securitate a sistemului, care va garanta confidențialitatea și securitatea datelor utilizatorilor pentru accesul neautorizat atât din afară cât și din interiorul sistemului;
- Serviciile și extensiile vor fi modulare și vor permite dezvoltarea ulterioară de noi funcționalități;
- Soluția de federalizare de conținut va oferi suport pentru WSRP 1.0 și 2.0 sau echivalent;
- Administrarea și configurarea componentei se va putea realiza facil, utilizând doar un browser web;
- Va conține un motor de căutare performant, care va permite efectuarea de interogări în toate sursele de informații prezente în mediul portal;



Proiect cofinanțat din Fondul Social European prin
Programul Operațional Capacitate Administrativă 2014-2020!



- Soluția de portal va oferi un motor de căutare avansat, care să permită utilizarea unor criterii de relevanță pentru obținerea rapidă a informațiilor căutate;
- Motorul de căutare va include mecanisme de învățare pe baza căutarilor deja efectuate pentru strângerea informațiilor referitoare la relevanță;
- Motorul de căutare va include capacități de căutare în cadrul documentelor XML;
- Motorul de căutare va permite utilizarea expresiilor booleene în cadrul căutărilor;
- Motorul de căutare va permite căutarea de documente similare cu un anumit document dat;
- Motorul de căutare va oferi mecanisme de tip proximitate pentru regăsirea mai ușoară a informațiilor căutate;
- Va îmbunătăți experiența utilizatorilor prin utilizarea unor tehnologii bazate pe Web 2.0 și AJAX sau echivalente;
- Va oferi acces către toate resursele prezente în cadrul interfeței consolidate printr-o singură autentificare, la deschiderea sesiunii;
- Componenta de portal va oferi suport pentru standardele deschise JSR 168, JSR 286 sau echivalente, standarde ce permit publicarea de portleți moderni și ușor de construit;
- Va include suport pentru standardul JSR 170 sau echivalent, în vederea administrării și gestionării elementelor de conținut;
- Soluția oferită va asigura suport pentru standardul deschis JSF sau echivalent;
- Posibilitatea de a avea portleți obligatorii în secțiuni predefinite și portleți selectabili de către utilizatori;
- Suport pentru monitorizarea activității (capturi de metrice, statistici, audit, etc.);
- Va oferi utilizatorilor versiuni diferite ale interfeței consolidate în funcție de tipul utilizatorului;
- Soluția va oferi suport pentru RSS sau echivalent;
- Soluția de portal va permite interfațarea cu sisteme de content management precum: Oracle Webcenter Content, Microsoft Sharepoint, EMC Documentum și Alfresco sau echivalente;
- Soluția de portal va oferi capacități avansate pentru reunirea mai multor portaluri / aplicații web într-o singură interfață, agregată;
- Servicii de Single Sign-On la nivelul tuturor informațiilor prezentate în portal.
- Să permită rularea platformei de integrare pe distribuțiile majore de sisteme de operare prezente pe piață (cel puțin Windows și Linux).
- Componenta Portal va rula pe infrastructura de servere de aplicație pusă la dispoziție de componenta server de aplicație.
- Să se integreze și utilizeze mecanismele scalabilitate și failover puse de dispoziție de componenta server de aplicație.
- Să existe posibilitatea de a utiliza de mecanisme de clustering, balansare.
- Să includa pe durata garanției servicii de suport și mentenanța software de la producător

Având în vedere nevoia de disponibilitate ridicată a sistemului ce va fi implementat, soluția oferită trebuie să includă accesul la update-uri și serviciile de suport ale producătorului (inclusiv pentru fix-uri, securitate și îmbunătățiri) pe durata garanției echipamentelor hardware. Nu se accepta oferte care

nu includ subscripție de la producator asigurată pe toată perioada de garanție a echipamentelor hardware.

4.4.1.21 Componenta server de aplicație

În arhitectura n-tier, serverul de aplicații este cel care expune nivelul logic și procesele de business, pentru a fi accesate/utilizate de către celelalte aplicații/componente.

Caracteristicile tehnice ale serverului de aplicații sunt următoarele:

- Compatibil cu specificațiile platformei Java Enterprise Edition 7 sau echivalent;
- Platformă tehnologică completă pentru instalarea și execuția site-urilor web dinamice, serviciilor web și aplicațiilor JEE sau echivalent;
- Suport complet pentru specificațiile Java Servlets 3.1 sau echivalent;
- Suport complet pentru specificațiile JavaServer Pages 2.3 sau echivalent;
- Suport complet pentru specificațiile Enterprise JavaBeans 2.0, 2.1, 3.0, 3.1, 3.2 sau echivalent;
- Suport pentru servicii web conform specificațiilor WS-I Basic Profile 1.1, 1.2 și 2.0 sau echivalent;
- Suport complet pentru servicii web utilizând specificațiile JAX-WS 2.2 și JAX-RPC 1.1 sau echivalent;
- Suport pentru Simple Object Access Protocol (SOAP) versiunile 1.1 și 1.2 și SOAP with Attachments API for Java (SAAJ) sau echivalent;
- Transformarea datelor în format XML utilizând standardul W3C Extensible Stylesheet Language (XSL) sau echivalent;
- Securizarea serviciilor web utilizând standardele WS-Security și WS-SecurityPolicy sau echivalente;
- Suport complet pentru standardul Java Database Connectivity (JDBC) sau echivalent;
- Suport pentru conectarea la multiple sisteme de gestiune a bazelor de date relaționale;
- Suport complet pentru standardul Java Messaging Service (JMS) versiunile 2.0 sau echivalent;
- Suport complet pentru managementul tranzacțiilor utilizând specificația Java Transaction API (JTA) versiunile 1.2 sau echivalente;
- Implementare proprie pentru specificația Java Persistence API (JPA) sau echivalentă, cu suport pentru Enterprise Java Beans (EJB) sau echivalent;
- Cache-ul de date distribuit va oferi mecanisme de acces concurrent la date și participare în tranzacții distribuite;
- Va implementa mecanisme avansate de caching;
- Va oferi un mediu de execuție a aplicațiilor Java critice cu cerințe de procesare în timp real;
- Va asigura mecanisme de grupare a serverelor în clustere de servere de aplicații atât în topologii de tip activ-activ cât și activ-pasiv;

- Va permite stoparea temporară a unui nod din cluster pentru mentenanță și suport, sistemul în acest timp fiind disponibil pentru activități normale;
- Va asigura mecanisme de balansare dinamică a încărcării sistemului între resursele administrate în cadrul aceluiași cluster;
- Server web integrat care sa permita inclusiv acoperirea stratului arhitectural din zona DMZ;
- Va oferi mecanisme de cache pentru optimizarea accesului la conținutul stocat.
- Va permite rularea serverului de aplicații pe distribuțiile majore de sisteme de operare prezente pe piață (cel puțin Windows și Linux).

Având în vedere nevoia de disponibilitate ridicată a sistemului ce va fi implementat, soluția oferită trebuie să includă accesul la update-uri și serviciile de suport ale producătorului (inclusiv pentru fix-uri, securitate și îmbunătățiri) pe durata garanției echipamentelor hardware. Nu se accepta oferte care nu includ subscripție de la producător asigurată pe toată perioada de garanție a echipamentelor hardware.

4.4.1.22 Componenta de integrare a aplicațiilor

În secțiunea „Interconectarea cu sistemele existente interne și externe” a prezentului document sunt descrise modalitățile de interconectare a platformei pentru Buletinul Electronic al Registrului Comerțului cu alte sisteme. Din punct de vedere tehnic, pentru realizarea acestei interconectări, se va utiliza o componentă de integrare ce va oferi suport pentru:

- modelarea și execuția proceselor de afaceri rezultate ca urmare a orchestrării de servicii standard reutilizabile;
- integrarea sistemelor informatice utilizând o soluție de tip magistrală de mesaje (Service Bus) cu capabilități extinse de conectare la soluții tehnologice eterogene;
- monitorizarea proactivă a fluxurilor în execuție prin accesul direct, sub forma de tablouri de control, la indicatorii cheie de execuție;
- capturarea și tratarea de evenimente provenite din surse diferite;
- securizarea accesului la serviciile și fluxurile modelate pe baza unor politici de acces definite și administrate centralizat.

Din punct de vedere tehnic/tehnologic această platformă de integrare prezintă următoarele caracteristici:

- Va oferi suport complet pentru dezvoltarea, testarea, execuția, monitorizarea, optimizarea și administrarea proceselor de integrare;

- Va oferi suport pentru soluții moderne și deschise de integrare conform principiilor și conceptelor arhitecturilor Service Oriented Architecture (SOA) și Event Driven Architecture (EDA);
- Va fi bazată pe standardele deschise de interoperabilitate a aplicațiilor WS-I Basic Profile, WSDL (Web Services Description Language), WS-*, XML, SOAP sau echivalente;
- Va permite modelarea declarativă a proceselor de integrare utilizând standardul OASIS (Organization for the Advancement of Structured Information Standards) BPEL (Business Process Execution Language);
- Va permite comunicații sincrone și asincrone inter-aplicații;
- Va oferi mecanisme transparente de persistență a stării proceselor și informațiilor de audit într-o bază de date relațională;
- Va permite folosirea canalelor de notificare moderne (email, SMS) pentru informarea utilizatorilor despre evenimentele semnificative apărute în aplicații;
- Va suporta transformări și manipulări de date complexe pentru implementarea logicii proceselor de business;
- Sistemul va include capabilități extinse de transformare a mesajelor XML utilizând standarde deschise W3C Extensible Stylesheet Language (XSL), XPath și XQuery sau echivalente;
- Va oferi soluții de conectare predefinite la principalele tipuri de tehnologii: baze de date relaționale, cozi de mesaje (JBossMQ, Oracle AQ, IBM Websphere MQ, MSMQ sau echivalente), sisteme de fișiere, etc;
- Va oferi un cadru de dezvoltare pentru noi soluții de conectare la sisteme externe bazat pe standarde deschise;
- Va oferi servicii de transport cu suport pentru persistența datelor;
- Va oferi servicii de transport cu suport pentru garantarea livrării datelor;
- Va include o soluție de tipul monitorizare a activității de afaceri - Business Activity Monitoring (BAM) sau echivalentă;
- Va permite monitorizarea în timp real a indicatorilor de tipul Key Performance Indicators (KPI) sau echivalentă;

- Va permite monitorizarea în timp real a SLA-urilor (Service Level Agreement) de business sau operaționale;
- Va oferi un modul centralizat de gestiune și aplicare a politicilor de securitate peste portofoliul de fluxuri electronice instalat;
- Va oferi servicii de securitate la nivel de aplicație;
- Pentru asigurarea securității la nivel transport, soluția va permite utilizarea protocolul Secure Socket Layer (SSL) și a certificatelor compatibile X.509;
- Va permite implementarea de servicii de securitate specifice lucrului cu serviciile web standard:
 - o autentificarea accesului la servicii;
 - o autorizarea accesului la servicii;
- Soluția va fi bazată pe standardele deschise de securitate a serviciilor web, precum WS-Security, WS-Policy and WS-Security Policy, Security Assertion Markup Language (SAML) sau echivalente;
- Soluția va putea securiza totalitatea apelurilor către serviciile existente printr-un mod de funcționare de tip poartă de acces (gateway) fără să fie necesară modificarea proceselor instalate;
- Să ofere mecanisme de grupare a serverelor în clustere pentru toate componentele platformei de integrare atât în topologii de tip activ-activ cât și activ-pasiv;
- Posibilitatea stopării temporare a unui nod din cluster pentru mentenanță și suport, sistemul în acest timp fiind disponibil pentru activități normale;
- Mecanisme de balansare a încărcării sistemului între resursele administrate în cadrul aceleiași cluster;
- Mecanisme de scalare a sistemului pe orizontală (Scale Out).
- Va permite rularea serverului de aplicații pe distribuțiile majore de sisteme de operare prezente pe piață (cel puțin Windows și Linux);

Având în vedere nevoia de disponibilitate ridicată a sistemului ce va fi implementat, soluția oferită trebuie să includă accesul la update-uri și serviciile de suport ale producătorului (inclusiv pentru fix-uri, securitate și îmbunătățiri) pe durata garanției echipamentelor hardware. Nu se accepta oferte care

nu includ subscripție de la producător asigurată pe toată perioada de garanție a echipamentelor hardware.

4.4.1.23 Componenta de integrare a datelor

Se dorește includerea în sistemul informatic a unei componente de integrare și consolidare oferind următoarele module de bază:

- replicare de date între surse eterogene de informații
- transformare date (ETL) din surse eterogene, prin:
 - o modelare declarativă a fluxurilor de integrare de date;
 - o sincronizare de date între surse eterogene de informații.

Replicarea datelor între Baza de date operațională existentă (baza de date de producție a sistemelor RC, RL și BPI) și baza de date a Buletinului Electronic al Registrului Comerțului. Rolul acestei componente este de a capta modificările apărute în baza de date sursă și de a le transfera către modulul de Transformare date, în vederea modificării structurilor de date și/sau a câmpurilor și aplicării acestora în baza de date destinată.

Modulul **Replicare Date** va oferi suport tranzacțional astfel încât să nu se propage în bazele de date destinate tranzacțiilor incomplete, în cazul apariției unei erori în baza de date sursă. Captarea datelor modificate în baza de date sursă se va face prin mecanisme care nu au impact asupra performanței acestora. Se acceptă mecanisme de captare a modificărilor bazate pe log-ul tranzacțional al bazei de date. Nu se acceptă mecanisme ce presupun definirea de trigger-i pe tabelele bazei de date.

Funcționalitățile majore pe care trebuie să le asigure modulul **Replicare date** sunt:

- posibilitatea de replicare între sistemul de gestiune a bazelor de date existent (Oracle) și Componenta de gestiune baze de date din cadrul noului sistem informatic;
- replicarea se va baza pe mecanisme care nu impactează performanța bazelor de date, cum ar fi log-ul tranzacțional al bazei de date;
- posibilitatea de replicare bi-direcțională între baze de date Oracle;
- soluția trebuie să permită replicare de tabele, secvențe oracle, precum și comenzi DDL.
- soluția trebuie să permită replicarea întregii baze de date, sau a unui set de tabele, sau chiar a unei singure table. De asemenea să permită doar replicarea unui subset din coloanele, sau rândurile tablei. Această funcționalitate este esențială având în vedere specificul replicărilor necesare în cadrul proiectului, unde se vor replica doar acele înregistrări necesare subsistemului Buletinul electronic al Registrului Comerțului.
- soluția trebuie să funcționeze cu variantele de bază de date Oracle din sistemul informatic integrat existent;

- soluția trebuie să aplice în timp real modificările în baza de date destinație, întârzierea între sursă și destinație să fie minimă.
- soluția trebuie să fie capabilă să replice baze de date configurate atât în mod arhivare cât și baze de date aflate în NONARCHIVE mode.
- soluția trebuie să păstreze bazele de date destinație deschise astfel încât poată fi utilizate pentru operațiunile curente specifice aplicațiilor care rulează pe aceste baze de date.

Modulul de **Transformare date** are ca scop asigurarea instrumentelor/funcționalităților de transformare a datelor cadrul sistemului nou creat. Acesta va oferi funcționalități de extragere date (din sursa de date), transformări ale acestora și încărcare în destinație, și va fi folosit pentru transferuri programate ale datelor, spre deosebire de instrumentul de replicare care va fi folosit pentru replicarea continuă a datelor.

Modulul de **Transformare date** va răspunde următorului set de cerințe tehnice:

- Va putea accesa și integra date din baze de date pe tehnologii diferite: Oracle, Fox Pro, Microsoft SQL Server, MySQL, IBM DB2, etc, și să ofere suport pentru accesarea datelor din date aflate în fișiere (.txt, .csv, etc);
- Va permite configurarea surselor de date de tip bază de date cu suport cel puțin pentru baza de date Oracle Database și pentru baza de date ofertată.
- Va avea suport pentru protocoale de transport cel puțin HTTP și dar altele precum JMS sau echivalent.
- Va avea suport pentru JSON/XML.
- Va avea suport pentru transformarea datelor folosind operatori aritmetici, condiționali, modificări șir de caractere, etc.
- Va avea suport pentru planificarea execuției unor acțiuni la momente de timp definite.
- Va avea suport pentru monitorizarea rulării instrumentului.
- Va funcționa în arhitectura cluster pentru asigurarea unei disponibilități ridicate.

Având în vedere nevoia de disponibilitate ridicată a sistemului ce va fi implementat, soluția ofertată trebuie să includă accesul la update-uri și serviciile de suport ale producătorului (inclusiv pentru fix-uri, securitate și îmbunătățiri) pe durata garanției echipamentelor hardware. Nu se accepta oferte care nu includ subscripție de la producător asigurată pe toată perioada de garanție a echipamentelor hardware.

4.4.1.24 Componenta de gestiune documente

Componenta va respecta următoarele cerințe:

- Oferă capabilități de management al conținutului nestructurat;
- Funcționalitățile trebuie să fie disponibile nativ (out-of-the-box) la nivelul componentei oferite, fără a fi necesare dezvoltări suplimentare pentru acoperirea cerințelor.
- Permite definirea securității (drepturilor de acces) pentru roluri, foldere și documente.
- Gestionează documentele, precum și metadescriptorii asociați acestora;
- Va permite crearea automată de structuri de foldere în funcție de valori ale metadatelor documentelor;
- Permite încărcarea de documente în depozitul de documente cel puțin prin următoarele modalități:
 - drag & drop, bulk upload, copy & paste în windows explorer,
 - monitorizare casuta de email și încărcare directă în depozitul de documente a tuturor fișierelor atasate care se trimit la acea casuta de email, fără nici o intervenție umană
- Permite utilizatorilor adăugarea de metadate speciale în afara de cele standard ale tipului de document, metadate valabile doar pe acea instanță de document;
- Conține un set de metadescriptori predefiniți asociați unui document;
- Oferă posibilitatea de a adăuga noi metadescriptori și taguri pentru căutare pe document;
- Permite organizarea colecțiilor de documente într-o structură ierarhică în conformitate cu schemele de indexare care se vor stabili în etapa de analiză;
- Nu va impune și nu va limita prin arhitectură sau prin implementare, numărul de documente care se pot adăuga în depozitul de documente;
- Permite gestiunea oricărui tip de documente;
- Permite accesul utilizatorilor printr-o interfață web a componentei
- Permite deschiderea, salvarea și popularea metadatelor pe fișiere direct din aplicațiile office (de ex. word, excel, powerpoint)
- Interfețele web ale componentei trebuie să fie disponibile utilizatorilor și administratorilor în limba Română
- Permite conversia automată a documentelor de tip MS Office sau OpenOffice în formate web (HTML, PDF), pentru o publicare facilă a acestora;
- Permite adăugarea de note, adnotări pe document;
- Permite accesarea funcționalităților platformei prin intermediul unor API și servicii web;
- Permite versionarea documentelor (fără vreo limitare privind numărul acestora);
- Permite blocarea/deblocarea documentelor (check-in/check-out);
- Include un instrument avansat de căutare care va permite efectuarea de interogări atât asupra metadatelor ce însoțesc un document cât și asupra conținutului documentului respectiv și să afișeze rezultatele într-o interfață de tip web-browser;
- Permite căutări de tip Fuzzy Search sau echivalent, bazate pe textul introdus de utilizator;
- Asigură regăsirea documentelor de către mai mulți utilizatori simultan;
- Va utiliza componenta de gestiune a bazelor de date oferită pentru stocarea metadatelor asociate documentelor;

- Permite ca opțiuni de stocare a conținutului nestructurat în componenta de gestiune a bazelor de date oferită și în sistemul de fișiere;
- Permite integrarea și utilizarea de mecanisme de clustering, balansare, scalabilitate și failover puse de dispoziție de componenta server de aplicații oferită;
- Permite integrarea cu LDAP și Active Directory pentru autentificarea utilizatorilor
- Permite expunerea de conținut către componenta Portal, pentru toți utilizatorii acesteia, fără a necesita costuri suplimentare pentru beneficiar;
- Permite rularea pe distribuțiile majore de sisteme de operare prezente pe piață (cel puțin Windows și Linux).

Având în vedere nevoia de disponibilitate ridicată a sistemului ce va fi implementat, soluția oferită trebuie să includă accesul la update-uri și serviciile de suport ale producătorului (inclusiv pentru fix-uri, securitate și îmbunătățiri) pe durata garanției echipamentelor hardware. Nu se acceptă oferte care nu includ subscripție de la producător asigurată pe toată perioada de garanție a echipamentelor hardware.

4.4.1.25 Componenta de procesare OCR

Componenta de procesare OCR va asigura conversia documentelor intrate în ONRC cu scopul de a fi publicate în Buletinul Electronic al Registrului Comerțului, printr-un proces de recunoaștere optică a caracterelor. Serverul OCR va permite conversia automată, în bloc, a documentelor salvate în depozitele de date cu diferite formate.

Componenta de procesare OCR va respecta următoarele cerințe:

- Funcționalitățile trebuie să fie disponibile nativ (out-of-the-box) la nivelul componentei oferite, fără a fi necesare dezvoltări suplimentare pentru acoperirea cerințelor.
- Permite procesare OCR pentru toate limbile europene (inclusiv limba română)
- Permite recunoașterea codurilor de bare, cel puțin: Check Code 39, Code 128, PDF 417, Data Matrix, QR Code, Check Interleaved 2 of 5
- Suporta un număr mare de formate de fișiere de intrare, printre care: JPEG, JPEG2000, JBIG2, PDF, HTML, PNG, DOC, DOCX, XLSX, PNG, BMP, GIF, PCX, DCX, TIFF multipagina (compresie cel puțin CCITT4, JPEG, LZW și ZIP)
- Suporta cel puțin următoarele formate de ieșire: PDF, PDF/A, RTF, DOC, DOCX, TXT, HTML
- Pune la dispoziție în mod nativ funcționalitățile de procesare OCR prin următoarele modalități: foldere de filesystem monitorizate, foldere FTP monitorizate, casute email monitorizate, servicii web sau conectori specializați pentru integrarea cu sisteme de gestiune continuă.

- Are o arhitectura scalabila cu distribuirea automata a incarcarii si procesare paralela astfel incat sa foloseasca la maxim capacitatea de procesare existenta
- Dispune nativ de mecanisme de balansare a incarcarii si procesarii documentelor intre mai multe servere

Avand in vedere nevoia de disponibilitate ridicata a sistemului ce va fi implementat, solutia oferata trebuie să includă accesul la update-uri si serviciile de suport ale producatorului (inclusiv pentru fix-uri, securitate si imbunatatiri) pe durata garanției echipamentelor hardware. Nu se accepta oferte care nu includ subscripție de la producator asigurată pe toată perioada de garanție a echipamentelor hardware.

4.4.1.26 Componenta de dezvoltare aplicatii mobile

Platforma de dezvoltare aplicatii mobile va respecta urmatoarele cerinte:

- Sa permita scrierea de aplicatii o data si sa poata rula pe oricare din dispozitivele mobile importante (iOS, Android, Windows).
- Sa foloseasca tehnologii web (HTML, CSS, Javascript) in procesul de dezvoltare aplicatii mobile
- Sa detina un nivel ridicat de flexibilitate in ceea ce priveste proiectarea interfetei utilizator (paleta , liste, navigare pagini, tab-uri, larga de culori, butoane, meniuri derulante, formulare de introducere date, etc)
- Sa permita testarea aplicatiilor pe baza de simulatoare incluse in platforma si cu browsere mobile (de ex. Safari pentru iOS)
- Se asigure acces la functionalitati importante din sistemul de operare in care aplicatia va rula precum: baterie, camera, localizare, acces la log-uri, etc. Sa permita dezvoltarea de plugin-uri pentru acoperirea accesului la functionalitati native.
- Sa detina o comunitate larga de dezvoltatori
- Sa detina un kit de dezvoltare software orientat catre dezvoltarea de aplicatii cu un nivel ridicat de interactivitate

Avand in vedere nevoia de disponibilitate ridicata a sistemului ce va fi implementat, solutia oferata trebuie să includă accesul la update-uri si serviciile de suport ale producatorului (inclusiv pentru fix-uri, securitate si imbunatatiri) pe durata garanției echipamentelor hardware. Nu se accepta oferte care nu includ subscripție de la producator asigurată pe toată perioada de garanție a echipamentelor hardware.

4.4.1.27 Componenta de gestiune baze de date

Sistemul de gestiune a bazelor de date va respecta următoarele cerințe:

- Sa fie un sistem de gestiune a bazelor de date de tip relațional;
- Sa utilizeze limbaj standard SQL pentru manipularea datelor (cel puțin SELECT, UPDATE, DELETE)
- Sa utilizeze limbaj standard pentru definire (cel puțin CREATE, ALTER, DROP, RENAME)
- Sa permita View-uri / View-uri materializate pentru tabele sau mecanisme similare
- Sa permita diverse tipuri de date printre care cel puțin: întregi, boolean, șir de caractere de mărime fixă și de mărime variabilă, numere în virgulă flotantă, date binare de mărime fixă și de mărime variabilă, JSON sau similar, dată și timp;
- Sa permita minim 250 coloane într-un tabel;
- Sa permita funcții tip fereastră (cel puțin RANK, DENSE_RANK, LEAD, ROW_NUMBER)
- Sa permita indecși de tip primar, coloană unică și multi-coloană;
- Sa permita partiționare pentru date și indecși
- Sa permita importul și exportul de date în formate de date general acceptate;
- Sa permita minimizarea conflictelor de acces la date;
- Sa ofere suport pentru proceduri stocate și triggeri;
- Sa ofere suport pentru tranzacții autonome;
- Sa permita partiționare logică a tabelelor mari în scopul reducerii timpului de acces la date după diverse criterii de partiționare (list, range, hash);
- Sa ofere suport pentru Unicode UTF-8;
- Sa ofere suport de replicare bidirecțională a datelor între două instanțe ale bazei de date;
- Sistemul va asigura o disponibilitate 100% pentru utilizatori, în cazul apariției unei defecțiuni hardware la unul din serverele cluster-ului;
- Sistemul de gestiune a bazelor de date relațional (SGBDR) va asigura balansarea încărcării între noduri la nivelul cererilor și execuțiilor pe baza de date aflată în cluster;
- Sa ofere mecanisme de control și blocare la nivel de înregistrare și mecanisme de asigurare a consistenței la citire, pentru a permite accesul în mod concurent al utilizatorilor la date;
- Sa permita restricționarea accesului la nivelul obiectelor bazei de date;
- Sa permita instalarea unei singure baze de date pe mai multe noduri (arhitectură de tip cluster activ-activ) pentru a asigura toleranță la defecte hardware sau nefuncționare planificată, scalabilitate și disponibilitate crescută a sistemului;
- Va oferi posibilitatea de a limita numărul de conexiuni la baza de date prin folosirea unui mecanism de tip database connection pooling;
- Va oferi un utilitar grafic pentru administrarea și monitorizarea SGBDR;
- Baza de date relațională va avea componente pentru optimizarea interogărilor;
- Va exista posibilitatea de a cripta tot traficul de rețea dinspre și către baza de date;
- Va permite stoparea temporară a unui nod pentru mentenanță, suport, upgrade sistemul în acest timp să rămână disponibil;

- Stocare criptată a datelor în baza de date în mod transparent față de aplicație, fără a fi necesară scrierea de cod în aplicație pentru a se cripta și decripta datele stocate în baza de date;
- Va permite rularea pe distribuțiile majore de sisteme de operare prezente pe piață (cel puțin Windows și Linux).

Având în vedere nevoia de disponibilitate ridicată a sistemului ce va fi implementat, soluția oferită trebuie să includă accesul la update-uri și serviciile de suport ale producătorului (inclusiv pentru fix-uri, securitate și îmbunătățiri) pe durata garanției echipamentelor hardware. Nu se acceptă oferte care nu includ subscripție de la producător asigurată pe toată perioada de garanție a echipamentelor hardware.

4.4.1.28 Componenta de gestiune a proiectelor

Componenta propusă va respecta următoarele cerințe:

- Funcționalitățile trebuie să fie disponibile nativ (out-of-the-box) la nivelul componentei oferite, fără a fi necesare dezvoltări suplimentare pentru acoperirea cerințelor.
- permite planificarea și urmărirea proiectelor (inclusiv a celor de dezvoltare software)
- permite planificarea și urmărirea muncii membrilor echipei la nivel granular inclusiv distribuirea sarcinilor pentru aceștia
- permite rularea de rapoarte predefinite și crearea de noi rapoarte.
- permite urmărirea sarcinilor
- permite atasarea de informații conexe sarcinilor, cum ar fi comentarii, statusuri, atasamente
- permite monitorizarea performanței în cadrul unui tablou de bord
- permite gruparea sarcinilor în proiecte și crearea de sub-sarcini
- include șabloane de proiecte
- include funcționalități de căutare rapidă și filtrare personalizată
- oferă suport pentru REST sau Java APIs
- permite integrarea cu un serviciu director de tip LDAP
- permite afișarea informațiilor despre sarcini într-un tablou de bord
- permite ca unui utilizator să i se poată asigna un rol într-un proiect sau rezolvarea unei sarcini
- permite managementul portofoliului de proiecte și al fluxurilor de lucru
- permite folosirea de formulare pentru colectarea informațiilor
- permite crearea unui colector de cerințe pentru captarea informațiilor din formularele de feedback încorporate în web site-uri
- permite integrarea cu componenta de gestiune a ciclului de viață a aplicațiilor
- include un designer de fluxuri de lucru
- permite trimiterea automată de notificări în cazul schimbării statusului unei sarcini

Având în vedere nevoia de disponibilitate ridicată a sistemului ce va fi implementat, soluția oferită trebuie să includă accesul la update-uri și serviciile de suport ale producătorului (inclusiv pentru fix-uri, securitate și îmbunătățiri) pe durata garanției echipamentelor hardware. Nu se accepta oferte care nu includ subscripție de la producător asigurată pe toată perioada de garanție a echipamentelor hardware.

4.4.1.29 Componenta de colaborare a echipelor

Componenta propusă va respecta următoarele cerințe:

- funcționalitățile trebuie să fie disponibile nativ (out-of-the-box) la nivelul componentei oferite, fără a fi necesare dezvoltări suplimentare pentru acoperirea cerințelor.
- să permită crearea de pagini diverse, pentru planuri de proiect, minutele întâlnirilor, cerințe de produs etc.
- să permită alocarea de sarcini utilizatorilor
- să permită adăugarea de comentarii la nivel granular pentru pagini și fișiere atașate
- să permită versionarea automată a documentelor
- să permită accesarea folosind clienți de tip desktop sau pentru dispozitive mobile și interfața să fie adaptată în funcție de tipul clientului
- să permită organizarea în spații de lucru
- să ofere posibilitatea de creare bloguri și discuții ce pot include comentarii, mențiuni de tip @ și aprecieri
- să includă șabloane de tip cele mai bune practici pentru a genera rapid pagini
- să ofere posibilitatea de abonare la conținut prin notificări pe email sau de tip RSS
- să permită acordarea de permisiuni la nivel granular, pentru pagini individuale, la nivel de spațiu de lucru și la nivel global
- să permită integrarea cu Microsoft Office pentru editarea de pagini
- să includă un editor de tip "rich text" cu posibilitate de "drag and drop" pentru atașamente și short-cut-uri pentru tastatură
- să includă funcționalități de căutare rapidă și căutare completă
- să ofere suport pentru limba română
- să permită crearea unei baze de date de cunoștințe
- să conțină un spațiu de lucru pentru colectarea și organizarea cererilor și răspunsurilor pe diverse topicuri, creând astfel o bază de date de cunoștințe
- să ofere suport pentru indexare și căutare, pentru găsirea cererilor și răspunsurilor cu ușurință
- să permită afișarea rezultatelor căutării din mai multe surse (pagini, postări on bloguri, atașamente)
- să permită vizualizarea persoanelor care contribuie cel mai mult cu răspunsuri
- să aibă o funcție de găsire și afișare informații similare din baza de date de cunoștințe
- să propună un mecanism pentru identificarea informațiilor corecte

- va permite includerea in cereri/raspunsuri de continut media (imagini, video), text formatat, link-uri, cod sursa, etc.
- va oferi posibilitatea de informare pe e-mail in cazul aparitiei unor informatii de interes
- va permite restrictionarea accesului la nivel de grupuri
- va oferi statistici privind folosirea spatiului de lucru ce contine cereri si raspunsuri

Avand in vedere nevoia de disponibilitate ridicata a sistemului ce va fi implementat, solutia ofertata trebuie să includă accesul la update-uri si serviciile de suport ale producatorului (inclusiv pentru fix-uri, securitate si imbunatatiri) pe durata garanției echipamentelor hardware. Nu se accepta oferte care nu includ subscripție de la producator asigurată pe toată perioada de garanție a echipamentelor hardware.

4.4.1.30 Componenta de gestiune a ciclului de viata al aplicatiilor

Componenta propusa va respecta următoarele cerințe:

- functionalitatile trebuie sa fie disponibile nativ (out-of-the-box) la nivelul componentei ofertate, fara a fi necesare dezvoltari suplimentare pentru acoperirea cerintelor.
- sa permita crearea de proiecte de dezvoltare software, planficarea si urmarirea acestora;
- sa permita inserarea de comentarii;
- sa ofere suport pentru roluri de utilizatori;
- sa permita gestionarea testarii;
- sa permita versionarea cerintelor;
- sa asigure suport pentru procesul de gestiune a calitatii software;
- sa permita integrarea cu medii de dezvoltare populare, cum ar fi: Eclipse, Visual Studio, Intelij, NetBeans;
- sa ofere suport pentru accelerarea ciclurilor de testare prin posibilitatea de planificare si rulare automata a testelor, prin integrare cu componenta de instalare si integrare continua a aplicatiilor;
- sa permita proiectarea cu usurinta a rapoartelor si a tablourilor de bord pe baza datelor proiectului;
- sa gestioneze multiple tipuri de cerinte si va permite trasabilitatea intre cerinte, teste, defecte, modificari de cod sursa si sistemele de construire a release-ului.

Avand in vedere nevoia de disponibilitate ridicata a sistemului ce va fi implementat, solutia ofertata trebuie să includă accesul la update-uri si serviciile de suport ale producatorului (inclusiv pentru fix-uri, securitate si imbunatatiri) pe durata garanției echipamentelor hardware. Nu se accepta oferte care nu includ subscripție de la producator asigurată pe toată perioada de garanție a echipamentelor hardware.

4.4.1.31 Componenta de instalare si integrare continua a aplicatiilor

Componenta propusa va respecta următoarele cerințe:

- functionalitatile trebuie sa fie disponibile nativ (out-of-the-box) la nivelul componentei oferite, fara a fi necesare dezvoltari suplimentare pentru acoperirea cerintelor.
- va oferi suport pentru o gama larga de limbaje de programare si pentru alte tehnologii populare precum AWS CodeDeploy, Docker și Amazon S3
- va dispune de agenti dedicati pentru rezolvarea erorilor critice
- va oferi suport pentru peste 50 de agenti pentru a rula loturi de teste in paralel
- va oferi posibilitatea de alocare permisiuni per mediu de lucru
- va oferi posibilitatea de blocare in carantina a testelor care nu functioneaza corect
- va oferi un proces automat de dezvoltare si testare software care nu depinde de un mediu local specific
- va oferi suport pentru REST APIs
- va permite ca testele de integrare sa fie declanșate automat dupa ce dezvoltatorii comit codul (integrare continua)
- va suporta optimizarea performantei dezvoltarii de software prin folosirea paralelizarii
- va permite gestionarea lansarii de versiuni software
- va permite rularea de teste automate in paralel
- va permite criptarea datelor in tranzit
- va permite criptarea credentialelor in baza de date si in backup-uri
- va permite rularea pe toate distribuțiile majore de sisteme de operare prezente pe piață: Windows si Linux.

Avand in vedere nevoia de disponibilitate ridicata a sistemului ce va fi implementat, solutia oferita trebuie să includă accesul la update-uri si serviciile de suport ale producatorului (inclusiv pentru fix-uri, securitate si imbunatatiri) pe durata garanției echipamentelor hardware. Nu se accepta oferte care nu includ subscripție de la producator asigurată pe toată perioada de garanție a echipamentelor hardware.

4.4.1.32 Componenta de testare automata a aplicatiilor

Componenta propusa va respecta următoarele cerințe:

- functionalitatile trebuie sa fie disponibile nativ (out-of-the-box) la nivelul componentei oferite, fara a fi necesare dezvoltari suplimentare pentru acoperirea cerintelor.
- permite folosirea unui limbaj de programare standard (Javascript, Vbscript, Jscript, Python) pentru crearea de teste pe interfata utilizator sau imbunatatirea inregistrarilor testelor existente;

- permite convertirea facilă în script-uri a testelor înregistrate în interfața grafică utilizator;
- dispune de un mediu de testare built-in;
- permite rularea de teste de tip cross-browser;
- permite rularea unui test automatizat pe mai multe ediții și versiuni de browsere, suportând browserele majore existente pe piață;
- permite automatizarea testării funcționale pentru multiple tehnologii desktop (de exemplu Windows / Java / .NET / Oracle Forms);
- permite separarea datelor de comenzile de test și modificarea datelor de intrare pentru lărgirea ariei de testare;
- conține o platformă de testare completă și integrată, atât pentru testarea desktop cât și pentru cea a aplicațiilor mobile și web.

Având în vedere nevoia de disponibilitate ridicată a sistemului ce va fi implementat, soluția oferită trebuie să includă accesul la update-uri și serviciile de suport ale producătorului (inclusiv pentru fix-uri, securitate și îmbunătățiri) pe durata garanției echipamentelor hardware. Nu se acceptă oferte care nu includ subscripție de la producător asigurată pe toată perioada de garanție a echipamentelor hardware.

4.4.1.33 Componenta de testare de performanță a aplicațiilor

Componenta propusă va respecta următoarele cerințe:

- funcționalitățile trebuie să fie disponibile nativ (out-of-the-box) la nivelul componentei oferite, fără a fi necesare dezvoltări suplimentare pentru acoperirea cerințelor.
- oferă suport pentru cele mai recente tehnologii web, cel puțin pentru: HTML5, WebSocket și Oracle Forms;
- permite, pentru crearea testelor, designul acestora fără a fi necesare scripturi;
- oferă suport pentru programarea vizuală a testelor;
- permite crearea de reguli pentru extragerea datelor variabile din pagini;
- suportă cel puțin SSL, Kerberos, NTLM și autentificări de tip Basic, Digest sau folosind certificate client;
- permite înregistrarea aplicațiilor mobile (cu browser de tip nativ, hibrid sau mobil) direct, de pe orice dispozitiv mobil;
- permite adăugarea/eliminarea de utilizatori virtuali în timpul execuției testelor;
- oferă suport pentru o gamă largă de produse software, incluzând însă nelimitându-se la sisteme de operare, servere de aplicații, servere web, baze de date;
- permite monitorizarea fără agenți;
- oferă suport pentru GIT;
- oferă suport pentru testarea cel puțin a aplicațiilor .NET și Java;

- permite rularea de teste de incarcare la nivelul API (SOAP, REST), la nivelul componentelor sau la nivelul microservicilor;
- permite analizarea performantei sistemului dupa rularea unui test pe baza datelor colectate din straturile arhitecturale relevante;
- permite rularea de rapoarte de analiza a performantei pe diferite nivele de detaliu (de tip sumar sau la nivel de tranzactie) si rapoarte pentru determinarea incadrarii performantei intr-un SLA predefinit
- Portabilitate: va permite rularea cel puțin pe urmatoarele distribuțiile de sisteme de operare prezente pe piață: Windows si Linux.

Avand in vedere nevoia de disponibilitate ridicata a sistemului ce va fi implementat, solutia oferata trebuie să includă accesul la update-uri si serviciile de suport ale producatorului (inclusiv pentru fix-uri, securitate si imbunatatiri) pe durata garanției echipamentelor hardware. Nu se accepta oferte care nu includ subscripție de la producator asigurată pe toată perioada de garanție a echipamentelor hardware.

4.4.2 Dimensionarea subsistemelor tehnice

Subsistemele tehnice vor fi dimensionate astfel incat sa raspunda atat cerintelor cantitative mentionate pentru fiecare in parte cat si celor calitative.

La acești indicatori se vor adăuga în faza de analiză o serie de indicatori de performanță suplimentari pentru evaluarea performanțelor soluției și se vor defini valorile pentru aceștia.

La dimensionarea componentelor hardware și software ale soluției se va avea în vedere asigurarea premizelor pentru obținerea unor criterii de performanță care să asigure eficiența activităților derulate de utilizatori. Astfel, timpii de răspuns ai sistemului informatic la solicitări standard de acces la informație sau de scriere de informații nu vor depăși câteva secunde (maxim 3 secunde), la o încărcare maximă a sistemului, unde, prin timp de răspuns se înțelege timpul scurs între lansarea unei cereri (de scriere sau de citire din baza de date) și momentul în care sistemul răspunde cererii respective și devine din nou disponibil pentru o nouă cerere.

4.4.2.1 Echipamente de tip șasiu modular

În configurația preconizată, soluția hardware va include 2 seturi (câte un set pentru fiecare site), iar fiecare set va include cel puțin 2 echipamente de tip șasiu modular pentru servere de tip blade.

Fiecare șasiu va fi echipat și configurat pentru a asigura cel puțin:

- 2 module interne de I/O tip port-extender sau fabric extender;

- 8 porturi 40Gbps uplink convergent către top-of-rack în fiecare modul de I/O;
- 4 module de racire / ventilare, în configurație redundată;
- 4 surse de alimentare, în configurație redundată.

Pentru fiecare din cele două site-uri, soluția preconizată va include cel puțin 1 echipament de tip rack (19in, min. 42RU înălțime, min. 80 cm lățime și min. 100 cm adâncime), ventilat pasiv și echipat pentru montarea și interconectarea echipamentelor de tip șasiu modular, precum și a tuturor celorlalte echipamente.

Vor fi incluse toate repererele și subansamblurile necesare pentru montarea în rack a echipamentelor de tip șasiu modular, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN și/sau SAN (acolo unde este cazul).

4.4.2.2 Echipamente de interconectare privata LAN/SAN

În configurația preconizată, soluția hardware va include 2 seturi (câte un set pentru fiecare site), iar fiecare set va include cel puțin 2 echipamente de interconectare privată (de tip port sau fabric extender) convergentă LAN/SAN.

Fiecare echipament de interconectare privată (de tip port sau fabric extender) convergentă LAN/SAN va fi echipat și configurat pentru a asigura cel puțin:

- 16 porturi 10/40Gbps Ethernet cu interfețe modulare QSFP, din care 10 echipate cu transceiver optic SR;
- 4 porturi 8/16Gbps FC cu interfețe modulare SFP+, din care 4 echipate cu transceiver optic 16Gbps SR;
- 4 1/10Gbps Ethernet cu interfețe modulare SFP+, echipate cu transceiver optic 10Gbps SR.
- 2 module de racire / ventilare, în configurație redundată;
- 2 surse de alimentare, în configurație redundată.

Vor fi incluse toate repererele și subansamblurile necesare pentru montarea în rack, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN și/sau SAN (acolo unde este cazul).

4.4.2.3 Echipamente de procesare generală

În configurația preconizată, soluția hardware va include 12 seturi (8 seturi pentru site-ul principal, respectiv 4 seturi pentru site-ul secundar), iar fiecare set va include cel puțin un echipament de procesare generală de tip server "blade".

Fiecare echipament de procesare generală de tip server "blade" va fi echipat și configurat pentru a asigura cel puțin:

- 2 procesoare fizice x86_64 (sau echivalent) 2GHz / 16-core / 20MB cache fiecare;
- 128GB RAM DDR3 sau DDR4;
- 200GB Flash, capacitate dedicată instalării hipervizorului;
- 2 porturi CNA 40Gbps pentru conectarea la rețeaua locală LAN.

Vor fi incluse toate repererele și subansamblurile necesare pentru montarea în șasiu, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN și/sau SAN (acolo unde este cazul).

4.4.2.4 Componenta de virtualizare generală

În configurația preconizată, soluția software va include 1 set de licențe, iar licențierea va acoperi utilizarea acestora pe ansamblul resurselor de procesare, la nivelul de echipare efectivă a echipamentelor de procesare generală.

Licențierea funcționalităților solicitate va acoperi exploatarea concurrentă a tuturor unităților de tip procesor multi-core instalate în toate echipamentele de tip server "blade", fără a introduce alte limitări (nici în legătură cu volumul de memorie activă instalată și nici cu volumul de stocare alocată local sau în sistemele specializate), având incluse cel puțin 2 instanțe de platforme de management centralizat.

Configurația va include garantarea dreptului de utilizare software, precum și de acces al beneficiarului la actualizările și pachetele corective publicate de producător, fără costuri suplimentare, pe durata de viață a produsului, dar nu mai puțin de 3 ani de la darea în funcțiune a sistemului.

4.4.2.5 Componenta de platformă de operare

În configurația preconizată, componenta va include 1 set de licențe, dimensionate conform cerințelor din prezenta documentație tehnică coroborate cu specificul/necesitățile fiecărui producător, pentru susținerea unui număr nelimitat de mașini virtuale la nivel de host, respectiv echipamentele de procesare generală – cu suport pentru tehnologiile VMware și Microsoft Hyper-V.

Configurația va include garantarea dreptului de utilizare software, precum și de acces al beneficiarului la actualizările și pachetele corective publicate de producător, fără costuri suplimentare, pe durata de viață a produsului, dar nu mai puțin de 3 ani de la darea în funcțiune a sistemului.

4.4.2.6 Echipamente de integrare LAN

În configurația preconizată, soluția hardware va include 2 seturi (câte un set pentru fiecare site), iar fiecare set va include cel puțin 2 echipamente de integrare LAN.

Fiecare echipament de integrare LAN va fi echipat și configurat pentru a asigura cel puțin:

- 48 porturi 1/10/25Gbps Ethernet cu interfețe modulare SFP+, din care 16 echipate cu transceiver optic 10Gbps SR și 4 echipate pentru conexiune 1Gbps, conectorizare electrică sau optică.
- 4 porturi 40Gbps Ethernet cu interfețe modulare QSFP, echipate cu transceiver optic SR;
- 2 module de racire / ventilare, în configurație redundată;
- 2 surse de alimentare, în configurație redundată.

Vor fi incluse toate reperetele și subansamblurile necesare pentru montarea în rack, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN și/sau SAN (acolo unde este cazul).

4.4.2.7 Echipament de stocare de Tip 1

În configurația preconizată, soluția hardware va include 1 set (care va fi instalat în site-ul principal), iar fiecare set va include cel puțin 1 echipament de stocare consolidată unificată (SAN/NAS).

Fiecare echipament de stocare consolidată unificată (SAN/NAS) va fi echipat și configurat pentru a asigura cel puțin:

- 2 unități de tip controller, în configurație redundată;
- 4 porturi de 16Gbps FC per controller;
- 4 porturi de 10Gbps Ethernet per controller;
- 40TB capacitate utilă totală (fără a lua în calcul compresia sau deduplicare), din care 16TB pe suport Flash/SSD (prin utilizarea a cel puțin 8 unitati Flash/SSD) și 24TB pe suport SAS (prin utilizarea a cel puțin 16 unitati de disc SAS cu mecanica de 10K rpm);
- 2 module de racire / ventilare, în configurație redundată;
- 2 surse de alimentare, în configurație redundată.

Vor fi incluse toate reperetele și subansamblurile necesare pentru montarea în rack, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN și/sau SAN (acolo unde este cazul).

4.4.2.8 Echipament de stocare de Tip 2

În configurația preconizată, soluția hardware va include 1 set (care va fi instalat în site-ul secundar), iar fiecare set va include cel puțin 1 echipament de stocare consolidată unificată (SAN/NAS).

Fiecare echipament de stocare consolidată unificată (SAN/NAS) va fi echipat și configurat pentru a asigura cel puțin:

- 2 unități de tip controller, în configurație redundantă;
- 4 porturi de 16Gbps FC per controller;
- 4 porturi de 10Gbps Ethernet per controller;
- 20TB capacitate utilă totală (fără a lua în calcul compresia sau deduplicare), din care 8TB pe suport Flash/SSD (prin utilizarea a cel puțin 4 unitati Flash/SSD) și 12TB pe suport SAS (prin utilizarea a cel puțin 8 unitati de disc SAS cu mecanica de 10K rpm);
- 2 module de racire / ventilare, în configurație redundantă;
- 2 surse de alimentare, în configurație redundantă.

Vor fi incluse toate reperetele și subansamblurile necesare pentru montarea în rack, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN și/sau SAN (acolo unde este cazul).

4.4.2.9 Componenta de monitorizare a dezvoltării și exploatării aplicațiilor

În configurația preconizată, soluția software va include 1 set de licențe, iar licențierea va acoperi utilizarea acestora în mod concurent pentru cel puțin 24 de (instanțe de) aplicații respectiv instalate și licențiate pe cel puțin 160 CPU-cores. Fiecare instanță de aplicație va fi considerată la nivel de mașină virtuală (JVM) sau la nivel de instanță O/S care găzduiește mediul virtual de runtime (.Net).

Configurația va include garantarea dreptului de utilizare software, precum și de acces al beneficiarului la actualizările și pachetele corective publicate de producător, fără costuri suplimentare, pe durata de viață a produsului, dar nu mai puțin de 3 ani de la darea în funcțiune a sistemului.

4.4.2.10 Componenta de monitorizare a accesului la date

În configurația preconizată, soluția software va include 1 set de licențe, iar licențierea va acoperi utilizarea acestora în mod concurent pentru cel puțin 22 instanțe de baze de date respectiv instalate și licențiate pe cel puțin 176 CPU-cores.

Configurația va include garantarea dreptului de utilizare software, precum și de acces al beneficiarului la actualizările și pachetele corective publicate de producător, fără costuri suplimentare, pe durata de viață a produsului, dar nu mai puțin de 3 ani de la darea în funcțiune a sistemului.

4.4.2.11 Componenta de monitorizare a serviciilor

În configurația preconizată, soluția integrată funcțional hardware și software va include 1 set, iar acesta va include cel puțin 1 echipament de monitorizare a serviciilor, care se va instala la nivelul site-ului principal. Se vor cota separat sub-componenta hardware și, respectiv, sub-componenta software a soluției.

În configurația preconizată, soluția software va include 1 set de licențe, iar licențierea va acoperi utilizarea acesteia în mod concurrent pentru analiza a cel puțin 1Gbps de trafic, respectiv monitorizarea a până la cel puțin 50 de instanțe active de tip server. Monitorizarea și analiza din perspectiva accesării aplicațiilor se va putea asigura pentru până la cel puțin 5000 de utilizatori externi unici pe lună, respectiv pe cel puțin 10 milioane de vizualizări la nivel de pagină web pe an.

Configurația va include garantarea dreptului de utilizare software, precum și de acces al beneficiarului la actualizările și pachetele corective publicate de producător, fără costuri suplimentare, pe durata de viață a produsului, dar nu mai puțin de 3 ani de la darea în funcțiune a sistemului.

Vor fi incluse toate repererele și subansamblurile necesare pentru montarea în rack, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN și/sau SAN (acolo unde este cazul).

4.4.2.12 Componenta de analiză și testare de securitate a aplicațiilor

În configurația preconizată, soluția software va include 1 set de licențe, iar licențierea va acoperi utilizarea acesteia pentru:

- Analizarea statică (SAST) fără restricții de număr de aplicații, în limita a 100,000 linii de cod, respectiv cel puțin pentru cod Java și .Net (C#);
- Analizarea dinamică (IAST/DAST) pentru cel puțin un serviciu de aplicație în tehnologie web targetat, la orice moment dat, inclusiv la nivel de modelare și evaluare de formulare interactive, autentificare și autorizare a accesului și logică de business implementată;
- Minim 2 utilizatori concurenți pentru analiza și raportare.

Configurația va include garantarea dreptului de utilizare software, precum și de acces al beneficiarului la actualizările și pachetele corective publicate de producător, fără costuri suplimentare, pe durata de viață a produsului, dar nu mai puțin de 3 ani de la darea în funcțiune a sistemului.

4.4.2.13 Componenta de analiză și remediere a vulnerabilităților de securitate

În configurația preconizată, soluția software va include 1 set de licențe, iar licențierea va acoperi utilizarea acestora pentru minimum de 500 echipamente sau noduri și servicii active, identificabile în rețea prin adresa IP, scanate simultan într-o singură sesiune.

Configurația va include garantarea dreptului de utilizare software, precum și de acces al beneficiarului la actualizările și pachetele corective publicate de producător, fără costuri suplimentare, pe durata de viață a produsului, dar nu mai puțin de 3 ani de la darea în funcțiune a sistemului.

4.4.2.14 Componenta de analiză a accesării și utilizării resurselor

În configurația preconizată, soluția software va include 1 set de licențe, iar licențierea funcționalităților solicitate va acoperi utilizarea acestora pentru cel puțin 500 de utilizatori, respectiv pe un număr de 500 de echipamente de post lucru individual, fără a introduce alte limitări.

Configurația va include garantarea dreptului de utilizare software, precum și de acces al beneficiarului la actualizările și pachetele corective publicate de producător, fără costuri suplimentare, pe durata de viață a produsului, dar nu mai puțin de 3 ani de la darea în funcțiune a sistemului.

4.4.2.15 Componenta de redistribuția a accesului la serviciile de aplicație

În configurația preconizată, soluția integrată funcțional hardware și software va include 2 seturi cu funcționalități și echipare identice, iar fiecare set va include cel puțin 1 echipament de redistribuție a accesului la serviciile de aplicație.

Atat în site-ul principal cât și în site-ul secundar se va instala câte 1 set, care vor forma un cluster la nivel global. Se vor cota separat sub-componenta hardware și, respectiv, sub-componenta software a soluției.

Fiecare echipament redistribuție a accesului la serviciile de aplicație va fi echipat și configurat pentru a asigura cel puțin:

- 10Gbps throughput, în regim de procesare generală L4/L7;
- 5Gbps procesare criptografică hardware internă integrată;
- 3Gbps compresie software internă integrată;
- 2000 tranzacții pe secundă procesare SSL hardware internă integrată (cu chei 2048bit);
- Procesarea de trafic până la cel puțin 500000 noi cereri L4 HTTP deschise pe secundă;
- Procesarea de trafic până la cel puțin 300000 noi conexiuni L7 deschise pe secundă;
- 4 porturi 1Gbps Ethernet SFP SX;

- 2 porturi 10Gbps Ethernet SFP+ SR;
- 1x 400GB SSD sau HDD;
- 2 module de răcire / ventilare, în configurație redundată;
- 2 surse de alimentare, în configurație redundată.

Configurația va include garantarea dreptului de utilizare software, precum și de acces al beneficiarului la actualizările și pachetele corective publicate de producător, fără costuri suplimentare, pe durata de viață a produsului, dar nu mai puțin de 3 ani de la darea în funcțiune a sistemului.

Vor fi incluse toate reperele și subansamblurile necesare pentru montarea în rack, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN și/sau SAN (acolo unde este cazul).

4.4.2.16 Componenta de protecție a serviciilor de aplicație

În configurația preconizată, soluția integrată funcțional hardware și software va include 4 seturi cu funcționalități și echipare identice, iar fiecare set va include cel puțin 1 echipament gateway de protecție a serviciilor de aplicație.

Atat în site-ul principal cât și în cel secundar se vor instala câte 2 seturi, în configurație de tip cluster. Se vor cota separat sub-componenta hardware și, respectiv, sub-componenta software a soluției.

Fiecare echipament gateway de protecție a serviciilor de aplicație va fi echipat și configurat pentru a asigura cel puțin:

- Suport intern asigurat pentru autentificarea concurrentă a cel puțin 500 utilizatori;
- 10Gbps throughput, în regim de procesare generală L4/L7;
- 8Gbps procesare criptografică hardware internă integrată;
- 5Gbps compresie hardware internă integrată;
- 4000 tranzacții pe secundă procesare SSL hardware internă integrată (cu chei 2048bit);
- Procesarea de trafic până la cel puțin 1000000 noi cereri L4 HTTP deschise pe secundă;
- Procesarea de trafic până la cel puțin 600000 noi conexiuni L7 deschise pe secundă;
- 4 porturi 1Gbps Ethernet SFP SX;
- 2 porturi 10Gbps Ethernet SFP+ SR;
- 1x 400GB SSD sau HDD;
- 2 module de răcire / ventilare, în configurație redundată;
- 2 surse de alimentare, în configurație redundată.

Configurația va include garantarea dreptului de utilizare software, precum și de acces al beneficiarului la actualizările și pachetele corective publicate de producător, fără costuri suplimentare, pe durata de viață a produsului, dar nu mai puțin de 3 ani de la darea în funcțiune a sistemului.

Vor fi incluse toate repererele și subansamblurile necesare pentru montarea în rack, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN și/sau SAN (acolo unde este cazul).

4.4.2.17 Componenta centrală de protecție avansată antimalware

În configurația preconizată, soluția integrată funcțional hardware și software va include 2 seturi cu funcționalități și echipare identice, iar fiecare set va include cel puțin 1 echipament de protecție avansată antimalware.

Atat în site-ul principal cât și în site-ul secundar se va instala câte 1 set. Se vor cota separat sub-componenta hardware și, respectiv, sub-componenta software a soluției.

Fiecare echipament de protecție avansată antimalware va fi echipat și configurat pentru a asigura procesarea a cel puțin 500Mbps de trafic.

Configurația va include garantarea dreptului de utilizare software, precum și de acces al beneficiarului la actualizările și pachetele corective publicate de producător, fără costuri suplimentare, pe durata de viață a produsului, dar nu mai puțin de 3 ani de la darea în funcțiune a sistemului.

Vor fi incluse toate repererele și subansamblurile necesare pentru montarea în rack, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN și/sau SAN (acolo unde este cazul).

4.4.2.18 Componenta de protecție a resurselor la nivel de post de lucru

În configurația preconizată, soluția software va include 1 set de licențe, iar licențierea funcționalităților solicitate va acoperi utilizarea acestora pentru cel puțin 500 de utilizatori, respectiv pe un număr de 500 de echipamente de post lucru individual și pentru un număr de cel puțin 25 de instanțe de tip server, fără a introduce alte limitări.

Configurația va include garantarea dreptului de utilizare software, precum și de acces al beneficiarului la actualizările și pachetele corective publicate de producător, fără costuri suplimentare, pe durata de viață a produsului, dar nu mai puțin de 3 ani de la darea în funcțiune a sistemului.

4.4.2.19 Componenta de management al datelor de audit

În configurația preconizată, soluția software va include 1 set de licențe, iar licențierea funcționalităților solicitate va acoperi utilizarea acestora pentru procesarea unui volum de informație mator de audit (de tip log, sau asimilat) generată susținut de cel puțin 10GB/zi, fără a introduce alte limitări.

Configurația va include garantarea dreptului de utilizare software, precum și de acces al beneficiarului la actualizările și pachetele corective publicate de producător, fără costuri suplimentare, pe durata de viață a produsului, dar nu mai puțin de 3 ani de la darea în funcțiune a sistemului.

4.4.2.20 Componenta portal

Acest subsistem tehnic va susține componenta funcțională de Consultare Online a Buletinului Electronic al Registrului Comertului și va fi dimensionată pentru 5000 de utilizatori externi care vor avea acces la serviciile electronice publicate în componenta Portal, dintre care 1000 concurenți.

Dimensionarea se va realiza astfel încât fiecare centru de date să poată susține încărcarea mai sus menționată în condițiile de performanță ale prezentului caiet de sarcini și de disponibilitate înaltă la nivelul fiecărui centru de date.

Totodată se va avea în vedere și licențierea componentei pentru mediul de testare/dezvoltare.

Configurația va include garantarea dreptului de utilizare software nelimitat în timp, precum și de acces al beneficiarului la actualizările și pachetele corective publicate de producător, fără costuri suplimentare, pe o perioadă de cel puțin 3 ani de la furnizarea licențelor.

4.4.2.21 Componenta server de aplicație

Acest subsistem tehnic va susține cel puțin următoarele componente funcționale:

- Componenta de consultare online a Buletinului Electronic al Registrului Comertului
- Componenta de Colectare și Elaborare a Buletinului Electronic al Registrului Comertului
- Componenta de integrare aplicații

Următoarele elemente cantitative vor fi avute în vedere la dimensionarea acestui subsistem:

1. Minim 500 de utilizatori interni care vor avea acces la funcționalitățile subsistemului, dintre care 250 concurenți;
2. Minim 5000 de utilizatori externi care vor avea acces la serviciile electronice publicate în componenta Portal, dintre care minim 1000 concurenți

3. Incarcarea a minim 10.000 acte in programul de lucru al unei zile, totalizand un volum de date de minim 2 GB.
4. Licentierea trebuie sa acopere cel putin o capacitate de procesare de 48 core-uri de procesor.

Dimensionarea se va realiza astfel incat fiecare centru de date sa poata sustine incarcarea mai sus mentionata in conditiile de performanta ale prezentului caiet de sarcini si de disponibilitate inalta la nivelul fiecarui centru de date.

Totodata se va avea in vedere si licentierea componentei pentru mediul de testare/dezvoltare.

Configurația va include garantarea dreptului de utilizare software nelimitat in timp, precum și de acces al beneficiarului la actualizările și pachetele corective publicate de producător, fără costuri suplimentare, pe o perioada de cel puțin 3 ani de la furnizarea licentelor.

4.4.2.2 Componenta de integrare a aplicatiilor

Licentierea trebuie sa acopere cel putin 8 core-uri de procesor.

Dimensionarea se va realiza astfel incat fiecare centru de date sa poata sustine incarcarea mai sus mentionata in conditiile de performanta ale prezentului caiet de sarcini si de disponibilitate inalta la nivelul fiecarui centru de date.

Totodata se va avea in vedere si licentierea componentei pentru mediul de testare/dezvoltare.

Configurația va include garantarea dreptului de utilizare software nelimitat in timp, precum și de acces al beneficiarului la actualizările și pachetele corective publicate de producător, fără costuri suplimentare, pe o perioada de cel puțin 3 ani de la furnizarea licentelor.

4.4.2.3 Componenta de integrare a datelor

Licentierea pentru componenta de Replicare a datelor trebuie sa acopere nivelul de licentiere al componentei de gestiune a bazei de date cat si al serverelor de baza de date ce va fi implicat in replicarea datelor (clusterul de Oracle RAC existent in Sistemul Informatic Integrat al ONRC).

Licentierea trebuie sa acopere cel putin 8 core-uri de procesor pentru componenta de Transformare a datelor la nivelul fiecarui centru de date.

Dimensionarea se va realiza astfel incat fiecare centru de date sa poata sustine incarcarea mai sus mentionata in conditiile de performanta ale prezentului caiet de sarcini si de disponibilitate inalta la nivelul fiecarui centru de date.

Totodata se va avea in vedere si licentierea componentei pentru mediul de testare/dezvoltare.

Configurația va include garantarea dreptului de utilizare software nelimitat in timp, precum și de acces al beneficiarului la actualizările și pachetele corective publicate de producător, fără costuri suplimentare, pe o perioada de cel puțin 3 ani de la furnizarea licentelor.

4.4.2.24 Componenta de gestiune documente

Acest subsistem tehnic trebuie sa asigure capacitatea de incarcare, stocare, procesare si consultare a documentelor indiferent de componenta prin care acestea ajung in cadrul sistemului informatic, cu respectarea parametrilor de performanta solicitati pentru fiecare componenta in parte.

Suplimentar fata de sustinerea componentelor cu care se integreaza pentru stocarea, procesarea si consultarea documentelor, următoarele elemente cantitative vor fi avute în vedere la dimensionarea acestui subsistem:

1. Minim 40 de utilizatori interni care vor avea acces la toate funcționalitățile subsistemului;
2. stocarea a minim 7.000.000 acte care vor fi publicate în Buletinul Electronic al Registrului Comerțului din care aproximativ 4.500.000 documente existente in prezent; fiecare act are una sau mai multe pagini, în medie 2 pagini pe act.
3. incarcarea anuala a minim 300.000 acte ce totalizeaza aproximativ 20 GB;
4. pentru asigurarea continuității funcționării în caz de dezastru, subsistemul va fi distribuit in 2 centre de date (centru primar si centru secundar).

Dimensionarea se va realiza astfel incat fiecare centru de date sa poata sustine incarcarea mai sus mentionata in conditiile de performanta ale prezentului caiet de sarcini si de disponibilitate inalta la nivelul fiecarui centru de date.

Totodata se va avea in vedere si licentierea componentei pentru mediul de testare/dezvoltare.

Configurația va include garantarea dreptului de utilizare software nelimitat in timp, precum și de acces al beneficiarului la actualizările și pachetele corective publicate de producător, fără costuri suplimentare, pe o perioada de cel puțin 3 ani de la furnizarea licentelor.

4.4.2.25 Componenta de procesare OCR

Licentierea acestei componente va fi dimensionata pentru minim 8 core-uri de procesor la nivelul fiecarui centru de date dar care sa permita o capacitate de procesare totala de minim 145 pagini A4 / minut.

Dimensionarea se va realiza astfel incat fiecare centru de date sa poata sustine incarcarea mai sus mentionata in conditiile de performanta ale prezentului caiet de sarcini si de disponibilitate inalta la nivelul fiecarui centru de date.

Totodata se va avea in vedere si licentierea componentei pentru mediul de testare/dezvoltare.

Configurația va include garantarea dreptului de utilizare software nelimitat in timp, precum și de acces al beneficiarului la actualizările și pachetele corective publicate de producător, fără costuri suplimentare, pe o perioada de cel puțin 3 ani de la furnizarea licentelor.

4.4.2.26 Componenta de dezvoltare aplicatii mobile

Acest subsistem tehnic trebuie sa permita modificarea/depanarea de aplicatii existente sau dezvoltarea de noi aplicatii pentru cel putin 5 dezvoltatori.

Dimensionarea acestei componente se va realiza astfel incat fiecare centru de date sa poata sustine aplicatiile dezvoltate in conditiile de performanta ale prezentului caiet de sarcini si de disponibilitate inalta la nivelul fiecarui centru de date.

Totodata se va avea in vedere si licentierea componentei pentru mediul de testare/dezvoltare.

Configurația va include garantarea dreptului de utilizare software nelimitat in timp, precum și de acces al beneficiarului la actualizările și pachetele corective publicate de producător, fără costuri suplimentare, pe o perioada de cel puțin 3 ani de la furnizarea licentelor.

4.4.2.27 Componenta de gestiune baze de date

Următoarele elemente cantitative vor fi luate în considerare în dimensionarea acestui subsistem tehnic:

1. Licentiere pentru cel puțin 16 core;
2. Instrumentele de administrare incluse trebuie sa acopere toate masinile pe care vor fi instalate servere de baze de date si sa fie licentiate pentru cel puțin 5 administratori.
3. pentru asigurarea continuității funcționării în caz de dezastru, subsistemul va fi distribuit in 2 centre de date (centru primar si centru secundar).

Dimensionarea se va realiza astfel incat fiecare centru de date sa poata sustine incarcarea mai sus mentionata in conditiile de performanta ale prezentului caiet de sarcini si de disponibilitate inalta la nivelul fiecarui centru de date.

Totodata se va avea in vedere si licentierea componentei pentru mediul de testare/dezvoltare.

Configurația va include garantarea dreptului de utilizare software nelimitat în timp, precum și de acces al beneficiarului la actualizările și pachetele corective publicate de producător, fără costuri suplimentare, pe o perioadă de cel puțin 3 ani de la furnizarea licențelor.

4.4.2.28 Componenta de gestiune a proiectelor

Următoarele elemente cantitative vor fi luate în considerare în dimensionarea acestui subsistem tehnic:

4. 500 de utilizatori interni care vor avea acces la funcționalitățile subsistemului, dintre care 100 manageri (manageri de proiect, manageri de departamente); estimăm ca maxim 250 utilizatori pot fi concurenți;
5. Minim 10 utilizatori interni vor avea acces pentru testarea subsistemului;
6. pentru asigurarea unei disponibilități sporite, serverele trebuie grupate în cluster activ-activ pentru distribuția cererilor;
7. pentru asigurarea continuității funcționării în caz de dezastru, subsistemul va fi distribuit în 2 centre de date (centru primar și centru secundar).

Dimensionarea se va realiza astfel încât fiecare centru de date să poată susține încărcarea mai sus menționată în condițiile de performanță ale prezentului caiet de sarcini și de disponibilitate înaltă la nivelul fiecărui centru de date.

Totodată se va avea în vedere și licențierea componentei pentru mediul de testare/dezvoltare.

Configurația va include garantarea dreptului de utilizare software nelimitat în timp, precum și de acces al beneficiarului la actualizările și pachetele corective publicate de producător, fără costuri suplimentare, pe o perioadă de cel puțin 3 ani de la furnizarea licențelor.

4.4.2.29 Componenta de colaborare a echipelor

Următoarele elemente cantitative vor fi luate în considerare în dimensionarea acestui subsistem tehnic:

1. 500 de utilizatori interni care vor avea acces la funcționalitățile subsistemului, dintre care 250 concurenți;
2. Minim 10 utilizatori interni vor avea acces pentru testarea subsistemului;
3. pentru asigurarea unei disponibilități sporite, serverele trebuie grupate în cluster activ-activ pentru distribuția cererilor;
4. pentru asigurarea continuității funcționării în caz de dezastru, subsistemul va fi distribuit în 2 centre de date (centru primar și centru secundar).

Dimensionarea se va realiza astfel incat fiecare centru de date sa poata sustine incarcarea mai sus mentionata in conditiile de performanta ale prezentului caiet de sarcini si de disponibilitate inalta la nivelul fiecarui centru de date.

Totodata se va avea in vedere si licentierea componentei pentru mediul de testare/dezvoltare.

Configurația va include garantarea dreptului de utilizare software nelimitat in timp, precum și de acces al beneficiarului la actualizările și pachetele corective publicate de producător, fără costuri suplimentare, pe o perioada de cel puțin 3 ani de la furnizarea licentelor.

4.4.2.30 Componenta de gestiune a ciclului de viata al aplicatiilor

Următoarele elemente cantitative vor fi luate în considerare pentru dimensionarea acestui subsistem tehnic:

1. 50 de utilizatori interni care vor avea acces la funcționalitățile componentei, din care maxim 20 concurenti;
2. folosirea a doua instante de servere distribuite in 2 centre de date (centru primar si centru secundar).

Dimensionarea se va realiza astfel incat fiecare centru de date sa poata sustine incarcarea mai sus mentionata in conditiile de performanta ale prezentului caiet de sarcini si de disponibilitate inalta la nivelul fiecarui centru de date.

Totodata se va avea in vedere si licentierea componentei pentru mediul de testare/dezvoltare.

Configurația va include garantarea dreptului de utilizare software nelimitat in timp, precum și de acces al beneficiarului la actualizările și pachetele corective publicate de producător, fără costuri suplimentare, pe o perioada de cel puțin 3 ani de la furnizarea licentelor.

4.4.2.31 Componenta de instalare si integrare continua a aplicatiilor

Următoarele elemente cantitative vor fi luate în considerare pentru dimensionarea acestui subsistem tehnic:

1. folosirea unui numar de minim 50 de agenti ;
2. folosirea a doua instante de servere distribuite in 2 centre de date (centru primar si centru secundar).

Dimensionarea se va realiza astfel incat fiecare centru de date sa poata sustine incarcarea mai sus mentionata in conditiile de performanta ale prezentului caiet de sarcini.

Totodata se va avea in vedere si licentierea componentei pentru mediul de testare/dezvoltare.

Configurația va include garantarea dreptului de utilizare software nelimitat in timp, precum și de acces al beneficiarului la actualizările și pachetele corective publicate de producător, fără costuri suplimentare, pe o perioada de cel puțin 3 ani de la furnizarea licentelor.

4.4.2.32 Componenta de testare automata a aplicatiilor

Următoarele elemente cantitative vor fi luate în considerare pentru dimensionarea acestui subsistem tehnic:

1. o echipa IT de 50 de persoane va avea acces la testarea sistemului, dintre care 5 persoane vor avea acces in mod concurrent;
2. solutia trebuie sa permita testarea sistemului pentru aplicatii de tip desktop, web si mobile;
3. trebuie sa poata fi rulate teste concurente, pe masini fizice si virtuale;
4. trebuie sa poata fi rulate un numar nelimitat de teste;
5. trebuie sa fie permisa rularea testelor pe browsere multiple.

Dimensionarea se va realiza astfel incat fiecare centru de date sa poata sustine incarcarea mai sus mentionata in conditiile de performanta ale prezentului caiet de sarcini.

Totodata se va avea in vedere si licentierea componentei pentru mediul de testare/dezvoltare.

Configurația va include garantarea dreptului de utilizare software nelimitat in timp, precum și de acces al beneficiarului la actualizările și pachetele corective publicate de producător, fără costuri suplimentare, pe o perioada de cel puțin 3 ani de la furnizarea licentelor.

4.4.2.33 Componenta de testare de performanta a aplicatiilor

Următoarele elemente cantitative vor fi luate în considerare pentru dimensionarea acestui subsistem tehnic:

1. testele de performanta trebuie sa permita asigurarea unei incarcari de cel putin 1000 de utilizatori virtuali

2. echipa IT ce va fi desemnata de catre ONRC pentru gestiunea si rulara cazurilor de test va fi de minim 5 persoane care pot lucra concurrent;
3. trebuie sa poata fi create un numat nelimitat de teste;
4. solutia trebuie sa permita testarea sistemului pentru incarcarea maxima a sa.

Dimensionarea se va realiza astfel incat fiecare centru de date sa poata sustine incarcarea mai sus mentionata in conditiile de performanta ale prezentului caiet de sarcini.

Totodata se va avea in vedere si licentierea componentei pentru mediul de testare/dezvoltare.

Configurația va include garantarea dreptului de utilizare software nelimitat in timp, precum și de acces al beneficiarului la actualizările și pachetele corective publicate de producător, fără costuri suplimentare, pe o perioada de cel puțin 3 ani de la furnizarea licentelor.

4.5 Cerințe de livrare și implementare

Ofertantul declarat castigator (Prestatorul) va fi responsabil atât cu livrarea, instalarea și configurarea echipamentelor hardware și a sistemelor software de bază în site-urile autoritatii contractante (centrele de date), cât și cu dezvoltarea noilor componente.

Prestatorul va fi responsabil de toate activitățile necesare pentru punerea în producție a sistemului incluzând, fără a se limita la: analiză detaliată, proiectare detaliată, dezvoltare de cod, testare unitară, testare de integrare, testare pentru punerea în producție, instalarea și configurarea pentru punerea în producție, sprijin pentru Beneficiar în vederea punerii în producție, garanție, management de proiect.

Codul sursă pentru componentele noi dezvoltate în cadrul proiectului va deveni proprietatea Beneficiarului.

În cazul în care echipamentele componente ale soluției tehnice vor fi furnizate de mai mulți producători, va fi asigurată integritatea și funcționalitatea întregului sistem. Funcționalitatea componentelor sistemului nu va fi în nici un fel afectată de integrarea în ansamblul soluției oferite.

Echipamentele, componentele și produsele software care fac obiectul prezentului caiet de sarcini vor fi instalate la sediul principal al autoritatii contractante sau la centrul de date secundar.

Instalarea echipamentelor, componentelor și a produselor software care fac obiectul prezentului caiet de sarcini va fi efectuată de catre personalul de specialitate al Prestatorului. Acestea vor fi instalate, configurate, parametrizate, testate și integrate în sistemul informatic existent de catre personalul de specialitate al Prestatorului.

Echipamentele hardware livrate trebuie să fie noi și să beneficieze de suport din partea producătorului (nu se accepta echipamente uzate moral, ce nu se mai află în linia de fabricație).

4.6 Organizarea și coordonarea proiectului

4.6.1 Servicii de management de proiect

În vederea implementării cu succes a sistemului, Prestatorul va asigura servicii de management de proiect prin alocarea unui Manager de Proiect dedicat pentru executia acestui proiect, pe toată durata implementării.

Durata de implementare a achiziției (semnarea acceptanței finale) va fi de maxim 15 luni de la data semnării contractului. Această perioadă include livrarea, instalarea și punerea în funcțiune a echipamentelor precum și proiectarea, dezvoltarea, testarea, instruirea și acceptanța sistemului.

Ofertantii vor avea în vedere următoarele termene maximale pentru finalizarea activităților de implementare:

- Livrare infrastructura HW și SW standard – 2 luni de la semnarea contractului
- Instalare infrastructura HW și SW standard – 4 luni de la semnarea contractului
- Analiza – 4 luni de la semnarea contractului
- Proiectare – 5 luni de la semnarea contractului
- Dezvoltare / testare prestator – 10 luni de la semnarea contractului
- Instalarea și configurarea particulară a soluției – 12 luni de la semnarea contractului
- Testare funcțională și de integrare – 13 luni de la semnarea contractului
- Instruire administratori și utilizatori – 15 luni de la semnarea contractului
- Punere în funcțiune sistem (inclusiv datele migrate/incarcate) și obținere acceptanță finală – 15 luni de la semnarea contractului

Totodată, în planul de proiect se va avea în vedere realizarea următoarelor recepții:

1. Cantitative – prin intermediul cărora se livrează produsele HW, pachetele SW standard și livrabilele serviciilor prestate din punct de vedere cantitativ.
2. Calitative – prin intermediul cărora Beneficiarul verifică parametrii de calitate ai livrărilor cantitative. Acestea pot fi:
 - a. Recepții calitative parțiale – sunt recepții calitative ce privesc anumite componente și/sau servicii ce fac obiectul contractului de achiziție. În baza acestor recepții calitative intermediare, beneficiarul poate realiza plăți parțiale aferente produselor / serviciilor recepționate. Sunt acceptate recepții calitative parțiale pentru:

- Livrarea si instalarea produselor HW - in urma testelor de acceptanta a instalarii produselor HW
 - Livrarea si instalare pachetelor SW de baza – in urma testelor de acceptanta a instalarii pachetelor SW de baza
 - Serviciile de analiza – in urma aprobarii documentului de analiza
 - Serviciile de proiectare – in urma aprobarii documentului de proiectare
 - Servicii de dezvoltare si testare – in urma testarii functionale si de performanta a sistemului
 - Serviciile de instruire – in urma acceptarii serviciilor de instruire prestate
- b. Receptie finala – care este realizata dupa finalizarea tuturor activitatilor proiectului si punerea in functiune a intregului sistem informatic.

Ofertantul are obligatia sa respecte urmatoarele termene maxime pentru realizarea receptiilor calitative in cadrul proiectului:

Denumire produs/serviciu	Livrabile	Document receptie calitativa	Termen receptie calitativa (luni de la semnarea contractului)
Infrastructura HW	Infrastructura HW Raport instalare si configurare infrastructura HW si produse SW standard Scenarii de testare a infrastructurii HW si produse SW standard	Proces verbal receptie calitativa infrastructura HW si produse SW standard	5
Produse SW standard	Produse SW standard Raport instalare si configurare infrastructura HW si produse SW standard	Proces verbal receptie calitativa infrastructura HW si produse SW standard	5

	Scenarii de testare a infrastructurii HW si produse SW standard		
Livrarea si instalarea infrastructurii HW	Raport instalare si configurare infrastructura HW si produse SW standard Scenarii de testare a infrastructurii HW si produse SW standard	Proces verbal receptie calitativa infrastructura HW si produse SW standard	5
Livrarea si instalarea produselor SW standard	Raport instalare si configurare infrastructura HW si produse SW standard Scenarii de testare a infrastructurii HW si produse SW standard	Proces verbal receptie calitativa infrastructura HW si produse SW standard	5
Servicii de analiza	Document analiza de business Scenarii de testare functionala si de testare integrare	Proces verbal receptie calitativa servicii analiza	5
Servicii de proiectare	Document proiectare detaliata Scenarii de testare non-functionala	Proces verbal receptie calitativa servicii proiectare	6
Servicii de dezvoltare si testare	Kit de instalare Procedura de instalare Manuale de utilizare si instalare Ghid de testare functionala si de testare integrare	Proces verbal receptie calitativa servicii dezvoltare si testare	14
Servicii de instalare si configurare	Raport instalare si configurare particulara a solutiei	Proces verbal receptie calitativa servicii de instalare	14

particulara a soluției		si configurare particulara a soluției	
Servicii de instruire	Materiale instruire utilizatori Materiale instruire administratori Rapoarte privind participarea la cursurile de instruire	Proces verbal receptie calitativa servicii instruire	15
Sistem informatic integrat	Raport de punere in functiune a sistemului informatic (GOLIVE) Codul sursa al aplicatiilor dezvoltate Procedura de compilare a codului sursa Rapoartele de monitorizare si control al proiectului Certificat de garantie pentru sistemul informatic	Proces verbal de receptie calitativa finala	15

Librabilele se predau beneficiarului pe baza de procese verbale de receptie cantitativa. Receptiile calitative se realizeaza pe baza proceselor verbale de receptie cantitativa aferente livrabilelor mentionate in tabelul de mai sus si a inspectiilor / verificarilor realizate de catre beneficiar in conformitate cu prevederile prezentului document.

Ofertantii vor evidentia toate milestone-urile si activitatile importante, duratele acestora si resursele ce vor fi alocate, in cadrul graficului de proiect ce va fi inclus in oferta tehnica.

4.6.1.1 Planificare, monitorizare si control / Planul de proiect

Ofertantul va prezenta împreună cu oferta un plan de proiect în care se vor detalia toate activitățile planificate în cadrul proiectului, milestone-urile aferente furnizării livrabilelor si ale acceptării acestora de către Autoritatea Contractanta, responsabilitățile cu privire la fiecare activitate în parte și persoanele responsabile din cadrul echipei de proiect pentru realizarea fiecărei activități.

Planul de proiect va include, după caz, livrarea unui pilot pentru soluția implementată, care va fi pus în producție, astfel încât la finalizarea fazei pilot, soluția să fie ajustată pentru o funcționare optimă și conformă cu cerințele. Durata fazei pilot va fi agreată de către părți la fiecare soluție implementată. Controlul proiectului se va realiza cu ajutorul unei structuri de evaluare care va include:

- sesiunea lunară de evaluare a stadiului întregului proiect
- sesiuni regulate de evaluare a diferitelor zone funcționale ale proiectului
- sesiuni de evaluare la finalizarea unor etape de proiect
- sesiuni de evaluare a riscului
- sesiuni ad-hoc de rezolvare a unor probleme specifice

Aceste sesiuni vor fi conduse de către expertul Manager de Proiect, iar rezultatele sesiunilor vor fi documentate în Minute de Sesiune care vor fi păstrate în cadrul Dosarului de Proiect.

4.6.1.2 Raportarea

Se vor întocmi rapoarte de progres pe întreaga perioadă de derulare a proiectului.

Prestatorul trebuie să transmită Beneficiarului cel puțin următoarele rapoarte:

- Rapoarte periodice prezentate de către Managerul de Proiect către Comitetul de Conducere al proiectului
- Rapoarte de Excepție (rapoarte ad-hoc care vor fi elaborate ori de câte ori vor apărea excepții de la activitățile planificate, excepții care necesită o decizie din partea Comitetului de Conducere al proiectului)
- Raport Final (la finalizarea contractului)
- Rapoarte ad-hoc elaborate de către Managerul de Proiect, ori de câte ori acest lucru este necesar, la solicitarea Comitetului de Conducere al proiectului.

4.6.1.3 Metodologia de proiect

Ofertantul va descrie metodologia de abordare și conducere a proiectului, precum și fiecare fază a proiectului în conformitate cu metodologia de proiect propusă.

Ofertantul va detalia metodele și instrumentele folosite pentru:

- managementul proiectului
- monitorizarea evoluției proiectului
- managementul calitatii
- managementul riscurilor
- managementul schimbării

Managementul calitatii

Calitatea în mediul de proiect se definește ca fiind totalitatea cerințelor de ordin tehnic, funcțional, a obiectivelor cantitative și calitative ale proiectului, precum și metodologia și procedurile de management de proiect stabilite la nivelul proiectului, care trebuie atinse și respectate pentru finalizarea cu succes a proiectului.

Ofertantul va avea în vedere cel puțin furnizarea următoarelor livrabile pe durata implementării:

- Livrabile de management (planuri, proceduri, rapoarte):
 - Echipa de proiect și Comitetul de conducere al proiectului;

- Planul proiectului;
- Rapoarte de monitorizare și control al proiectului;
- Livrabile tehnice ale proiectului:
 - Documentul de analiză de business – a proceselor existente și a celor care vor fi implementate;
 - Documentul de proiectare detaliată HW/SW – ce include arhitectura sistemului și aspectele non-funcționale;
 - Scenarii de testare funcțională și non-funcțională;
 - Echipamentele hardware și software standard contractate și livrate;
 - Documentul care certifică instalarea și configurarea echipamentelor hardware;
 - Documentul care certifică corectitudinea funcționalităților dezvoltate în cadrul sistemului informatic;
 - Documentul care certifică instalarea și configurarea finală a sistemului informatic;
 - Documentul care certifică instruirea utilizatorilor sistemului informatic;
 - Documentul care certifică instruirea personalului care va utiliza/administra echipamentele hardware și software;
 - Kitul de instalare a aplicației dezvoltate (include release note și instrucțiuni de instalare)
 - Codul sursă al aplicației dezvoltate
 - Materiale de instruire
 - Manuale de utilizare/administrare/configurare ale sistemului informatic;
 - Manuale de instalare și configurare a echipamentelor și software-ului de bază;
 - Manuale de administrare a sistemului/soluției;
 - Manuale de utilizare a componentelor sistemului/soluției;
 - Documentația funcțională a componentelor sistemului/soluției;
 - Documentația tehnică a componentelor sistemului/soluției;
 - Documentațiile tehnice ale echipamentelor și software-ului de bază, furnizate de producători;
 - Alte manuale/documentații stabilite în urma perioadei de analiză, proiectare, dezvoltare sau urmare derulării proiectului.
 - Proceduri de lucru cu / administrare a sistemul(ui) informatic;
 - Certificate de garanție.

Implementatorul va furniza toate manualele și documentațiile în limba română, cu excepția documentațiilor tehnice ale echipamentelor și software-ului de bază, furnizate de producători, care pot fi în limba engleză.

Manualele și documentațiile, cu excepția celor elaborate de producător, vor fi livrate pe suport electronic (CD, DVD) și vor fi revizuite la fiecare schimbare de versiune software.

Odată cu predarea sistemului împreună cu toate documentațiile aferente, Ofertantul cedează și drepturile de proprietate intelectuală/drepturile de autor asupra aplicațiilor dezvoltate care constituie componente ale sistemului.

Cerinte de calitate pentru fiecare livrabil:

- pentru echipamente:

- tip
- cerinte tehnice
- standarde
- dimensiuni
- consum energetic etc.
- pentru software:
 - cerinte functionale
 - cerinte tehnice
 - cerinte de capacitate, timp de raspuns
- pentru servicii
 - cerinte, specialisti, activitati
 - specificatiile livrabilelor rezultante

Procedura de management al calității va prevedea metodele concrete prin care se va monitoriza și controla evoluția calității livrabilelor, pe întreaga durată a proiectului. În mod concret, se va realiza la nivelul proiectului o strategie de testare și acceptanță care va indica, pentru fiecare tip de livrabil în parte, etapele procesului de verificare a calității (testare), criteriile de acceptanță și modalitatea de documentare a acestui proces.

Pentru monitorizarea aspectelor legate de calitate, se va întreține la nivelul proiectului un Registru de Calitate și se vor organiza ședințe periodice de management al calității, în cadrul cărora se vor discuta aspecte legate de calitate, se vor stabili acțiuni și se va actualiza Registrul de calitate. În Registrul de calitate se vor înregistra toate testele și acceptanțele din cadrul proiectului, data și rezultatele obținute. Orice disfuncționalitate sau neconformitate va fi ulterior tratată, până la rezolvare. Concluzia finală se va înregistra, de asemenea, în Registrul de Calitate al proiectului.

Managementul riscurilor

Riscurile la adresa obiectivelor proiectului vor fi identificate și documentate în Registrul Riscurilor, împreună cu modul în care acestea pot fi ținute sub control. De asemenea, se vor prevedea măsuri de rezerva pentru situația în care riscul devine activ. Registrul Riscurilor și planurile asociate pentru controlul acestor riscuri vor fi revazute în mod regulat în timpul ședințelor de evaluare a riscurilor.

Pe durata derulării proiectului, în momentul identificării unui nou risc sau al manifestării unui risc planificat, persoana din echipa de proiect care a identificat riscul îl comunică Managerului de Proiect. Acesta realizează o analiză preliminară și, dacă riscul este real, întocmește un Raport de Risc pe care îl transmite Comitetului de Conducere al proiectului în vederea aprobării măsurilor propuse în cadrul Raportului.

Prestatorul va fi responsabil pentru livrarea unui sistem informatic perfect integrat, care să includă toate funcționalitățile prevăzute în proiectul tehnic și care să permită atingerea tuturor obiectivelor specifice ale proiectului, conform cerințelor din Caietul de Sarcini.

Ofertantul va include în echipa sa de proiect doi specialiști în securitate, care vor defini/monitoriza/verifica cerințele de implementare din perspectiva asigurării securității datelor și a sistemelor. De asemenea, la finalizarea implementării tehnice a proiectului și înainte de testarea finală a soluției, Prestatorul va trebui să realizeze teste de securitate și să prezinte un raport cu privire la problemele identificate. Acestea vor fi analizate, se vor stabili acțiuni de remediere care vor fi implementate și ulterior se va face o nouă verificare a securității.

Managementul schimbarii

În cadrul oricărui proiect care are un ciclu mai lung de viață (peste 1 an) între momentul inițializării și cel al finalizării implementării, este posibil ca pe durata derulării sale anumite procese de lucru, cerințe tehnice și funcționale sau priorități să se modifice. Este esențial ca în astfel de situații proiectul să se poată adapta acestor schimbări, iar aceasta poate însemna modificarea diferitelor planuri, specificații și livrabile ale proiectului pe durata implementării proiectului.

Toate aceste schimbări vor fi gestionate prin intermediul Procedurii de Management al Schimbarii. Schimbarile survenite sau propuse vor fi analizate din punct de vedere al implicațiilor asupra diferitelor elemente ale proiectului (obiective, cerințe, buget, resurse, termene de implementare, riscuri etc.) și se vor stabili cele mai bune strategii pentru gestionarea lor. Schimbarile care au implicații asupra livrabilelor proiectului vor fi documentate și supuse aprobării Comitetului de Conducere al proiectului.

4.6.2 Servicii de implementare

4.6.2.1 Analiza

Echipa de analiză a Prestatorului trebuie să analizeze cerințele împreună cu experții Beneficiarului pentru a înțelege corect modificările legislative/nevoile utilizatorilor înainte de proiectarea și dezvoltarea noilor funcționalități.

Livrabilele de analiză includ descrierea componentelor care trebuie dezvoltate/adaptate. Livrabilele acestei etape sunt următoarele:

- Document de analiză de business - cu specificațiile funcționale pentru componentele dezvoltate/adaptate
- Cazuri și scenarii de testare funcționale și respectiv de integrare, pentru componentele dezvoltate/adaptate conform cerințelor din prezentul document

În vederea derulării etapei de proiectare și dezvoltare software, livrabilele mai sus menționate vor fi aprobate de către persoanele responsabile din cadrul ONRC.

4.6.2.2 Proiectare și dezvoltare software

Ofertantul va descrie metodologia de dezvoltare software folosită în cadrul proiectului.

Serviciile de proiectare și dezvoltare software se vor realiza pe baza documentelor rezultate și aprobate în faza de analiză software. Aceste servicii includ: proiectarea, dezvoltarea și integrarea efectivă a funcționalităților, conform specificațiilor aprobate în faza de analiză. Etapa de proiectare și dezvoltare se va încheia cu testarea internă realizată de Prestator, în vederea livrării către ONRC a funcționalităților dezvoltate în cadrul prezentului contract.

Livrabilele acestei etape sunt următoarele:

- Codul sursă al aplicației comentat la nivel de clasă (Java), funcție (PL/SQL) și proceduri (PL/SQL), codul XML, codul fișierelor de configurare
- Rezultatele testelor Prestatorului
- Procedura de compilare a codului sursă
- Document de proiectare detaliată – include Modelul funcțional și de date (UML 2.0) și aspectele non-funcționale specifice componentelor ce asigură monitorizarea și securitatea sistemului
- Manuale de utilizare

- Orice alte informatii relevante, la cerinta ONRC

Inainte de predarea unui release nou (sau a unui patch) spre testare catre ONRC, Prestatorul va realiza propria etapa de testare interna, ca parte a procedurilor sale de asigurare a calitatii.

Echipele Prestatorului alocate pentru realizarea acestor servicii va fi responsabila pentru intretinerea permanenta pe durata acestui acord cadru a codului sursa al tuturor dezvoltarilor realizate in cadrul sistemului informatic al carui proprietar este ONRC. Orice dezvoltare noua a sistemului informatic ONRC, realizata ca urmare a acestui acord cadru, va deveni proprietatea exclusiva a ONRC.

Echipele Prestatorului va avea sarcina de a actualiza codul sursa al aplicatiilor, precum si procedurile necesare pentru compilarea si utilizarea acestui cod sursa. Procedura de compilare a codului sursa va fi astfel documentata incat sa permita restaurarea aplicatiilor din cadrul sistemului informatic in caz de dezastru si de indisponibilitate a copiilor de siguranta. Procedura va prezenta pas cu pas activitatile necesare pentru restaurarea aplicatiilor plecand de la codul sursa al acestora.

4.6.2.3 Instalare și configurare soluție

Ofertantul va fi responsabil pentru realizarea soluției oferite asigurând:

- compatibilitate maximă cu soluția existentă;
- valorificarea infrastructurii existente;
- garantarea unei maxime disponibilități.

Ofertantul va asigura următoarele servicii:

Implementarea soluției

Implementarea subsistemelor/soluțiilor va cuprinde cel puțin următoarele faze/activități:

- transportul și manipularea până la sediul beneficiarului, după caz;
- furnizarea cerințelor necesare a fi asigurate de beneficiar pentru instalarea în bune condiții;
- realizarea planului detaliat al activităților ce vor fi realizate și agrearea acestuia cu beneficiarul, în vederea evitării oricărei întreruperi în funcționarea aplicațiilor din producție;
- analiza cerințelor, pregătirea specificațiilor funcționale și validare de către beneficiar;
- proiectarea detaliată a soluțiilor solicitate și validare de către beneficiar. După validarea acestui document de către Beneficiar se va trece la executarea serviciilor necesare aferente;
- instalarea și configurarea tuturor produselor software, după caz;
- instalarea și configurarea tuturor echipamentelor în scopul implementării soluției, după caz;
- realizarea tuturor configurațiilor necesare pentru asigurarea tuturor serviciilor solicitate;
- dezvoltarea soluției software;
- realizarea testării funcționale a soluției pe mediul de dezvoltare/testare;
- instalarea și configurarea produselor software, după caz;
- configurarea produselor software existente în scopul implementării soluțiilor, după caz;
- realizarea tuturor configurațiilor necesare pentru asigurarea tuturor serviciilor solicitate;
- actualizarea configurațiilor ca urmare a unor modificări survenite pe cel puțin unul din sistemele din locațiile implementate;
- realizarea testării funcționale a sistemului implementat pe mediul de dezvoltare/testare la fiecare modificare de configurație;
- livrarea documentelor cu specificațiile pentru soluțiile implementate;

- livrarea procedurilor de lucru detaliate pentru serviciile implementate;
- livrarea procedurilor de back-up și restore, după caz.

Prestatorul va asigura serviciile de instalare / configurare în afara orelor programului de lucru ale ONRC, cel puțin pentru serviciile care implica centrul principal (productiv, la nivel central și teritorial), reconfigurările aferente testării și orice alte configurări care implica sistemul aflat în producție. Metodologia de implementare propusă trebuie să fie de tip iterativ.

Instalare / configurare subsisteme/soluții

Ofertantul va fi responsabil pentru realizarea subsistemelor/soluțiilor asigurând:

- compatibilitate cu soluția existentă;
- valorificarea infrastructurii existente;
- garantarea unei maxime disponibilități.

Serviciile de instalare/configurare vor cuprinde:

- instalare software aplicativ la nivel central și teritorial după caz;
- configurare și monitorizare.

4.6.2.4 Testarea și testele de acceptanță

Realizarea cu succes a testelor este condiție pentru obținerea acceptanței finale asupra soluțiilor livrate. Testele se consideră a fi încheiate cu succes dacă este posibilă furnizarea serviciilor solicitate în condiții optime conform cerințelor.

Planul de testare va fi propus de Prestator și agreeat de Beneficiar.

Testele vor include dar nu se vor limita la următoarele:

- Testare funcțională pe date relevante
- Testare de performanță (timp de răspuns corespunzător profilului de utilizator)
- Teste de stres (volum de date, număr de utilizatori concurenți)
- Teste de identificare a problemelor cu menționarea zonei de cod care trebuie optimizată (clasă, funcție, procedură, instrucțiune)
- Testare pentru acceptanța finală.

Ofertantul trebuie să prezinte în cadrul propunerii tehnice metodologia de testare după care se vor realiza activitățile de testare în timpul desfășurării proiectului.

Planul detaliat de testare, însoțit de scenariile de testare, va fi realizat de către Prestator și aprobat de Beneficiar înainte de fiecare etapă de testare agreeată prin planul de proiect.

Beneficiarul (cu asistența Prestatorului) va rula toate scenariile pentru testele de acceptanță ale componentei livrate. Testele de acceptanță se vor derula în conformitate cu Planul de Testare.

4.6.2.5 Intrarea în producție

Ofertanții trebuie să prezinte planul care va fi utilizat la trecerea în producție a sistemului.

Planul prezentat trebuie să țină cont de legăturile logice între subsisteme astfel încât să se asigure o trecere în producție coerentă și cu impact minim asupra activităților zilnice ale angajaților Beneficiarului.

4.6.3 Servicii de garanție și suport

Cerințele de garanție și suport exprimate în continuare sunt cerințe minime obligatorii.

Perioada de garanție și suport pentru sistemul informatic va fi asigurată pentru:

Minim 3 ani pentru hardware de la data semnării procesului verbal de recepție cantitativă.

Garanția produselor hardware asigură înlocuirea oricărei componente defecte, costurile înlocuirii fiind suportate de către furnizorul echipamentului.

În perioada de garanție, Prestatorul se obligă să asigure constatarea defecțiunilor hardware și remedierea defectelor on-site.

Remedierea defectelor se va face la sediul ONRC, iar în cazul unor defecte mai grave, echipamentele se vor transporta de către furnizor la sediul acestuia, asigurându-se însă continuitatea serviciilor informatice ale ONRC.

- În situația în care este necesară transportarea echipamentelor în afara sediului ONRC, toate mijloacele de stocare a datelor vor fi reținute de către beneficiar (hard-discurile vor fi scoase din echipamente și păstrate la sediul ONRC).
- La finalizarea fiecărei intervenții în cadrul perioadei de garanție se va întocmi o fișă de intervenție care va conține următoarele detalii: data intervenției, descrierea intervenției, modalitatea de rezolvare a intervenției (reparație/înlocuire), durata de intervenție și confirmarea recepției prin semnăturile Prestatorului și beneficiarului.

Minim 2 ani pentru produse software standard (inclusiv SO, software de cluster, dacă este cazul) de la data semnării procesului verbal de recepție cantitativă. Garanția produselor software va cuprinde:

- Acces la ultima versiune, patch-uri, fix-uri publicate de producător;
- Acces la documentația tehnică;
- Analiza problemelor;
- Prioritizarea problemelor după severitatea acestora;
- Comunicarea cererilor de asistență către un centru de suport tehnic;

Minim 2 ani garanție pentru aplicațiile dezvoltate de la data punerii în funcțiune a sistemului informatic cu toate funcționalitățile acestuia.

Aceste servicii obligă ofertantul/furnizorul noului sistem să rezolve orice neconformitate a sistemului informatic, în concordanță cu specificațiile acestuia.

În cazul în care sunt necesare modificări, implementatorul este obligat:

- să modifice/actualizeze aplicațiile componente ale sistemului;
- să modifice/actualizeze și documentația acestor aplicații;
- să predea codul sursă, executabilele și kit-urile de instalare ale aplicațiilor modificate.

Aplicațiile vor respecta specificațiile funcționale, vor fi fără erori și vor rula fără întreruperi sau probleme de funcționare, în caz contrar Ofertantul având obligația de a remedia erorile în cauză.

În perioada de garanție, Ofertantul va remedia erorile de funcționare ale sistemului livrat. Aplicațiile implementate nu vor avea vulnerabilități privitoare la atacuri sau intruziuni în sistem. Aceste aspecte vor fi detaliate de către Ofertant în documentul de specificații tehnice ale aplicațiilor informatice;

Nivel Criticitate	Timp de raspuns	Timp solutionare temporara	Timp solutionare finala
Critic	1 oră lucratoare	4 ore lucratoare	2 zile lucratoare
Mediu	4 ore lucratoare	2 zile lucratoare	4 zile lucratoare
Minor	2 zile lucratoare	4 zile lucratoare	8 zile lucratoare

1) Fereastra de suport tehnic / garanție:

a) L-V/ zile de lucru nelucrătoare declarate ca fiind lucrătoare în sistemul administrației publice/ 08:00 – 18:00

2) Tipurile incidentelor:

- a) **Critic:** una sau mai multe resurse din mediul productiv sunt nefuncționale sau profund degradate iar impactul acestui incident duce la imposibilitatea utilizării sistemului
- b) **Mediu:** impactul produs de degradarea uneia sau mai multor resurse duce la scăderea performanței sau afectarea parțială a unor funcționalități ale sistemului. Sistemul este funcțional pentru cea mai mare parte a scenariilor de utilizare.
- c) **Minor:** impactul produs de degradarea uneia sau mai multor resurse este redus sau există soluție temporară.

Prestatorul va asigura o garanție de minim 2 ani după finalizarea implementării proiectului și punerea în funcțiune a sistemului pentru toate funcționalitățile acestuia, care trebuie să rămână nealterate pe întreaga perioadă de garanție.

Depășirile timpilor de răspuns/soluționare asumați prin propunerea tehnică pentru perioada de garanție și suport dau dreptul achizitorului de a calcula și aplica penalizări. Acestea sunt cuantificate prin puncte de penalizare, astfel:

- Pentru depășirea termenului de răspuns și a termenului de soluționare temporară/finală aferente defectelor critice, se vor aplica 3 puncte de penalizare pentru fiecare oră de depășire a termenului;

- Pentru depășirea termenului de răspuns și a termenului de soluționare temporară/finală a defectelor medii se vor aplica 2 puncte de penalizare pentru fiecare oră de depășire a termenului

- Pentru depășirea termenului de răspuns și a termenului de soluționare temporară/finală a defectelor minore se va aplica 1 punct de penalizare pentru fiecare oră de depășire a termenului

Un punct de penalizare valorează 0,001% din valoarea contractului.

Garanția se va asigura fără costuri suplimentare din partea ONRC.

Perioada de garanție se va majora cu timpul de nefuncționare al echipamentelor/subsistemelor informatice în intervalul de reparare a acestora.

Toate serviciile menționate vor fi prestate în baza metodologiei de asistență, suport tehnic și garanție ce va fi descrisă de către ofertanți în cadrul propunerii lor.

Înștiințarea cu privire la o disfuncționalitate a sistemului informatic implementat va fi realizată de către beneficiar prin următoarele metode (care vor fi puse la dispoziție de către furnizor odată cu punerea în funcțiune a sistemului):

- Aplicație informatică de gestiune a incidentelor în perioada de garanție
- Utilizând sistemul de poștă electronică (la o adresă de poștă electronică dedicată pusă la dispoziție de către furnizor).
- Printr-un apel telefonic al ONRC la un număr dedicat pus la dispoziție de către furnizor.
- Prin transmiterea unui fax de către ONRC la un număr de fax dedicat pus la dispoziție de către furnizor.

Remedierea defectelor se va face la sediul ONRC, iar în cazul unor defecte mai grave, echipamentele se vor transporta de către furnizor la sediul acestuia, asigurându-se însă continuitatea serviciilor informatice ale ONRC.

- În situația în care este necesară transportarea echipamentelor în afara sediului ONRC, toate mijloacele de stocare a datelor vor fi reținute de către beneficiar (Hard-discurile vor fi scoase din echipamente și păstrate la sediul ONRC).
- La finalizarea fiecărei intervenții în cadrul perioadei de garanție se va întocmi o fișă de intervenție care va conține următoarele detalii: data intervenției, descrierea intervenției, modalitatea de rezolvare a intervenției (reparație/inlocuire), durata de intervenție și confirmarea recepției prin semnăturile Prestatorului și beneficiarului.
- Perioada de garanție se va majora cu timpul de nefuncționare al echipamentelor/subsistemelor informatice în intervalul de reparare a acestora.

4.6.4 Instruire

Instruirea utilizatorilor, administratorilor de sistem, rețea, comunicații și securitate și administratorilor de aplicații joacă un rol esențial în garantarea acceptanței sistemului livrat precum și în întreținerea și dezvoltarea acestuia.

În cadrul proiectului, activitățile de instruire au în vedere instruirea/cursarea a 50 utilizatori, angajați ai ONRC, atât de la nivel central cât și teritorial (ORCT), 5 administratori de sistem, rețea, comunicații și securitate și 5 administratori de aplicații.

Cerințele de instruire exprimate în continuare sunt cerințe minime obligatorii.

Procesul de instruire este adresat utilizatorilor finali, administratorilor de rețea, comunicații și securitate precum și administratori de aplicații și va include tematici cu privire la utilizarea, administrarea și dezvoltarea noului sistem implementat.

Prestatorul va organiza mai multe tipuri de cursuri de instruire, în funcție de audiența vizată și anume:

A. Cursuri destinate utilizatorilor finali care includ tematici cu privire la utilizarea, în condiții de siguranță, a noului sistem implementat de către personalul de la nivel central și teritorial:

A.1. Instruire personal implicat în colectarea, analiza datelor și actelor persoanelor supuse obligației de înregistrare în registrul comerțului, raportarea către ONRC, publicarea în Buletinul Electronic al Registrului Comerțului și utilizarea datelor din Buletinul Electronic al Registrului Comerțului:

- 50 persoane (1 persoană de la fiecare ORCT, 5 persoane de la ORCTB și 4 persoane de la ONRC), organizate în 3 grupe;
- instruirea va fi organizată în 3 grupe;
- cursurile vor avea loc la București, într-o locație asigurată de Prestator dotată corespunzător necesar susținerii cursurilor;
- Prestatorul va asigura cazarea (într-o unitate hotelieră de minim 3 stele sau similar, în regim de camera single), transportul și masa (mic dejun, prânz și cină);
- durata cursurilor va fi de 4 zile/ 4 nopți pentru fiecare grupă
- pentru serviciile de cazare va fi decontată contravaloarea serviciilor efectiv prestate, pe baza documentelor justificative privind numărul de participanți efectiv cazați și a listei cu participanții semnată în original
- în vederea bunei desfășurări a cursului prestatorul va asigura pentru fiecare sesiune 1 formator
- formatorul va presta un număr de 32 ore de pregătire/sesiune de formare (care vor include și orele aferente evaluării)
- Orele de pregătire și evaluare vor fi evidențiate în cadrul fișei de pontaj pentru fiecare categorie de activitate.

Serviciile de transport vor fi asigurate de operatorul economic (dus/întors) pentru numărul de participanți care provin din toate zonele țării, ținând seama de organizarea instituției registrului comerțului la nivelul țării, prin decontarea cheltuielilor aferente transportului dus/întors pentru numărul de participanți, în limita a 400 lei, fără TVA/participant, în pretul ofertei.

Decontarea transportului se va face de către prestator individual către aceste persoane, pe baza documentelor justificative prezentate. Decontarea transportului se va efectua pentru deplasare dus-întors, la data prezentării participantului la locul desfășurării cursului. Prestatorul va asigura participanților decontarea acestui tip de cheltuială de transport din fonduri proprii, pe baza documentelor justificative, cu respectarea dispozițiilor H.G. 1860/2006 cu modificările și completările ulterioare, luând în considerare distanța disponibilă pe website-ul www.distanta.ro și în raport de prevederile cuprinse în Ghidul Beneficiarului astfel:

Pentru transport cu autoturismul personal:

- Decontul se va realiza pe baza bonurilor fiscale de combustibil cu menționarea numărului de înmatriculare al mașinii pe verso și numele participantului. Bonurile fiscale vor reflecta cantitatea de combustibil cu care s-a făcut alimentarea mijlocului de transport personal și trebuie să fie emis într-o perioadă apropiată deplasării;
- Se decontează contravaloarea 7,5 l combustibil/100 km cu documente justificative și ordin de deplasare/delegație înregistrat la angajator, completat cu perioada deplasării și scopul acesteia, semnat și ștampilat de angajator, cu număr și dată, cu precizarea "Se deplasează cu auto personal". Valoarea bonului fiscal de combustibil trebuie să fie cel mult egală cu valoarea efectiv calculată pentru decont. În cazul în care valoarea bonului fiscal este mai mare decât valoarea calculată, se va deconta suma calculată conform H.G. 1860/2006 cu modificările și completările ulterioare, luând în considerare distanța disponibilă pe website-ul www.distanta.ro.
- Distanța luată în calcul la decontarea carburantului reprezintă suma distanțelor de la localitatea din care provine instituția la locul de desfășurare a sesiunilor de instruire și retur. Se va lua în calcul distanța cea mai scurtă conform datelor disponibile pe website-ul www.distanta.ro

Pentru transport cu tren/autobuz/microbuz:

- Biletele de tren/autobuz/microbuz sau alte documente relevante corespunzătoare perioadei de desfășurare a cursului, astfel încât să se asigure participarea;
- Decontul se va face pe baza biletului de tren/autobuz/microbuz dus – întors în original. Pentru tren, în cazul în care deplasarea, pe timp de noapte peste 300 km, se face cu vagon de dormit, ordinul de deplasare va include precizarea "Se deplasează cu vagon de dormit." Transportul cu trenul se decontează clasa a-II a pentru distanțe mai mici de 300 km și clasa I pentru distanțe mai mari de 300 km, conform H.G. 1860/2006 cu modificările și completările ulterioare.

Ordinele de deplasare trebuie să fie semnate și ștampilate de către instituția de la care provine participantul, precum și de către unitatea de cazare la care a fost cazat acesta, și să nu depășească perioada de desfășurare a sesiunii respective;

Ofertantul va propune un program de cursare ce va fi agreat de către Autoritatea Contractantă pentru cursurile menționate mai sus, cu precizarea următoarelor informații:

- descrierea programului de curs, a tematicii și a conținutului acestuia;
- detalii de organizare a cursului (săli folosite, unități de cazare, durată, număr de sesiuni, număr de formatori și calificarea acestora, număr participanți etc);
- descrierea rezultatelor așteptate;
- resurse puse la dispoziție de Prestator;
- resurse necesare din partea ONRC.

Ofertantul va prezenta în oferta care va fi depusă descrierea detaliată a procedurilor de susținere a cursurilor pe care le propune în cadrul proiectului care vor evidenția în mod obligatoriu următoarele:

- modalitatea de planificare a cursurilor;
- modalitatea de desfășurare a cursurilor;
- modalitatea de evaluare a rezultatelor cursurilor;
- modalitatea de evaluare a performanțelor instructorilor.

ONRC, împreună cu Prestatorul, vor stabili de comun acord modalitatea de prestare a serviciilor pe baza planificării proiectului și disponibilității cursanților.

Prestatorul va elabora un plan de instruire cuprinzând numărul de zile alocate pentru fiecare curs din cele menționate mai sus și, eventual, cursuri suplimentare pe care le consideră necesare pentru implementarea și acceptanța noului sistem. Fiecare curs va trata una sau mai multe componente ale sistemului, grupate de obicei după funcționalitate.

ONRC va stabili, la nivel intern, lista participanților la cursurile de instruire și va comunica Managerului de Proiect din partea Prestatorului lista de cursanți.

Desfășurarea cursurilor

Cursurile se vor desfășura conform planului de instruire stabilit și agreat contractual. Cursurile se vor tine în limba română, utilizând metode interactive combinate cu metode clasice de către formatori din partea Prestatorului. Acesta va asigura infrastructura hardware, software și suportul de curs în limba română.

Cursurile se vor face pe baza suportului de curs, livrat de Prestator fiecărui participant. Acest suport de curs va conține exemple practice pentru o mai bună înțelegere a modului de funcționare și administrare a sistemului, precum și alte detalii legate de acesta.

Încheierea cursurilor se va efectua prin testarea participanților. În urma acestei testări se va efectua certificarea/atestarea participanților. Testarea se va face pe formulare tipizate, cu întrebări de tip grilă și/sau răspuns liber.

Pentru instruirea utilizatorilor finali vor fi utilizate suporturi de curs, create special în acest sens.

Ședințele de instruire constau din:

- prezentarea conceptelor de către formator;
- ședințe practice, pentru mai bună înțelegere și utilizare a sistemului / produselor software (sisteme de operare, sisteme de gestiune a bazelor de date etc.) / echipamentelor hardware;

La sfârșitul cursului, formatorul va cere cursanților să completeze un Chestionar de Evaluare a Cursului.

În cadrul fiecărei sesiuni de cursare va fi inclusă o prezentare a temei orizontale „Dezvoltare durabilă, egalitate de șanse și protecția mediului” pentru a conștientiza participanții de importanța acestor subiecte în activitatea lor curentă. Astfel, prezentarea va include:

- o secțiune cu privire la importanța protecției mediului și dezvoltării durabile, problemele de mediu și tema schimbărilor climatice;
- o secțiune de promovare a egalității de șanse între femei și bărbați, a egalității de șanse pentru toți, fără discriminare în funcție de gen, rasă, origine etnică, religie, handicap, vârstă, orientare sexuală.

B. Servicii de instruire a administratorilor:

a) **de sistem, rețea, comunicații și securitate** care cuprind tematici privind administrarea sistemului, administrarea bazelor de date, administrarea utilizatorilor și a drepturilor de acces, administrarea comunicațiilor, asigurarea securității, monitorizarea performanțelor, asistență acordată utilizatorilor etc:

- 5 persoane
- instruirea va fi organizată pe o perioadă de 25 zile
- instruirea va avea loc la sediul Autorității contractante, într-o sala dotată corespunzător serviciilor de instruire.

b) **de aplicații** care au ca obiect prezentarea aplicațiilor sistemului, a instrumentelor de dezvoltare și tehnicilor de programare utilizate în cadrul proiectului:

- 5 persoane
- instruirea va fi organizată pe o perioadă de 10 zile
- instruirea va avea loc la sediul Autorității contractante, într-o sala dotată corespunzător serviciilor de instruire.

Administratorii de sistem, rețea, comunicații și securitate vor fi astfel instruiți de către Prestator astfel încât să poată asigura funcționarea sistemului cu o asistență minimă din partea Prestatorului sau independent de acesta, începând cu perioada post-implementare.

În plus, ofertantul va trebui să includă în propunerea tehnică și instruire din mers (on-the-job-training) pentru utilizatorii cheie ai ONRC, prin implicarea lor în diferite etape ale proiectului. În acest sens, ofertantul va trebui să prezinte în propunerea tehnică **metodologia prin care va asigura implicarea utilizatorilor cheie ai ONRC în derularea proiectului.**

Ofertantul va propune un program de instruire ce va fi agreat de către Autoritatea Contractantă pentru toate serviciile de instruire menționate mai sus, cu precizarea următoarelor informații:

- descrierea programului de instruire, a tematicii și a conținutului acestora;
- detalii de organizare a programului de instruire
- descrierea rezultatelor așteptate;
- resurse puse la dispoziție de Prestator;
- resurse necesare din partea ONRC.

Ofertantul va prezenta în oferta care va fi depusă descrierea detaliată a procedurilor de instruire pe care le propune în cadrul proiectului care vor evidenția în mod obligatoriu următoarele:

- modalitatea de planificare a instruirii;
- modalitatea de desfășurare a instruirii;
- modalitatea de evaluare a rezultatelor instruirii;
- modalitatea de evaluare a performanțelor instructorilor.

ONRC, împreună cu Prestatorul, vor stabili de comun acord modalitatea de instruire pe baza planificării proiectului și disponibilității cursanților.

Prestatorul va elabora un plan de instruire cuprinzând numărul de zile alocate pentru fiecare program de instruire din cele menționate mai sus și, eventual, programe de instruire suplimentare pe care le consideră necesare pentru implementarea și acceptanța noului sistem. Fiecare program de instruire va trata una sau mai multe componente ale sistemului, grupate de obicei după funcționalitate.

ONRC va stabili, la nivel intern, lista participanților la cursurile de instruire și va comunica Managerului de Proiect din partea Prestatorului lista de cursanți.

Desfășurarea instruirii

Instruirea se va desfășura on-site, la sediul central al ONRC, precum și off-site, conform planului de instruire stabilit și agreat contractual. Instruirea se va tine în limba română/engleză, utilizând metode interactive combinate cu metode clasice de către instructori din partea Prestatorului. Acesta va asigura infrastructura hardware, software și suportul de curs în limba română/engleză.

Instruirea se va face pe baza suportului de curs, livrat de Prestator fiecărui participant. Acest suport de curs va conține, după caz, exemple practice pentru o mai bună înțelegere a modului de funcționare și administrare a sistemului, precum și alte detalii legate de acesta.

Încheierea instruirii se va efectua prin testarea participanților. În urma acestei testări se va efectua certificarea/atestarea participanților. Testarea se va face pe formulare tipizate, cu întrebări de tip grilă și/sau răspuns liber.

Pentru instruire vor fi utilizate suporturi de curs, create special în acest sens.

Ședințele de instruire constau din:

- prezentarea conceptelor de către formator;
- ședințe practice, pentru mai bună înțelegere și utilizare a sistemului / produselor software (sisteme de operare, sisteme de gestiune a bazelor de date etc.) / echipamentelor hardware;

La sfârșitul programului de instruire, formatorul va cere participanților să completeze un Chestionar de Evaluare a Cursului.

În cadrul fiecărei sesiuni de instruire va fi inclusă o prezentare a temei orizontale „Dezvoltare durabilă, egalitate de șanse și protecția mediului” pentru a conștientiza participanții de importanța acestor subiecte în activitatea lor curentă. Astfel, prezentarea va include:

- o secțiune cu privire la importanța protecției mediului și dezvoltării durabile, problemele de mediu și tema schimbărilor climatice;
- o secțiune de promovare a egalității de șanse între femei și bărbați, a egalității de șanse pentru toți, fără discriminare în funcție de gen, rasă, origine etnică, religie, handicap, vârstă, orientare sexuală.

4.7 Riscuri identificate

În elaborarea ofertelor tehnice, operatorii economici trebuie să ia în calcul următoarele riscuri, care pot interveni în derularea contractului:

- Surse de ordin instituțional – factori care aparțin organizației ONRC;
- Surse de mediu legislativ – factori care provin din contextul legislativ național (legislația actuală aplicabilă);
- Surse de ordin tehnic – factori care provin din constrângeri (limitări) de tip tehnic.

Prin urmare, prezentăm o analiză calitativă a riscurilor aferente proiectului, în care s-a identificat riscul, precum și măsurile de atenuare a riscului, având în vedere impactul estimat (mic, mediu, semnificativ) și consecințele materializării riscului.

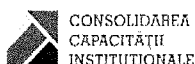
În ceea ce privește riscurile de mediu și legate de schimbările climatice, precizăm că nu există o vulnerabilitate a proiectului referitor la aceste aspecte.

Nr. crt.	Risc identificat	Măsuri de atenuare ale riscului
1.	Se schimbă Managerul de Proiect al Ofertantului sau Autorității Contractante pe durata derulării proiectului Probabilitate: mică	Impact: semnificativ Consecințe: apariția unor disfuncționalități în gestionarea proiectului și în coordonarea echipei de proiect. Acțiuni preventive: Desemnarea unui adjunct de manager de proiect care să cunoască toate aspectele operaționale ale

Nr. crt.	Risc identificat	Masuri de atenuare ale riscului
		proiectului si care sa poata prelua aceasta functie in cazul indisponibilitatii Managerului de Proiect desemnat initial. Responsabili: Director General ONRC / Manager de Proiect Ofertant
2.	Descompletarea echipelor pe durata ciclului de viața al proiectului Probabilitate: medie	Impact: mediu Consecințe: un posibil impact asupra activităților proiectului, livrabilelor cheie, finalizării etapelor proiectului. Pierderea unor abilitați cheie în momente critice. Acțiuni corective: Înlocuirea personalului/expertiilor cât mai curând posibil sau alocarea unei perioade de tranziție, atunci când este posibil. Acțiuni preventive: Pregătirea și derularea unui program intern de instruire. Responsabili: Manager de Proiect ONRC, Manager de Proiect Ofertant
3.	Rezistența personalului beneficiarului la schimbare Probabilitate: medie	Impact: mediu Consecințe: Probleme operaționale. Beneficiile sistemului nu pot fi valorificate complet din cauza folosirii practicilor vechi de lucru. Acțiuni corective: problema va fi escaladată către Comitetul Director al Proiectului. Ar putea fi necesare programe de instruire suplimentare. Acțiuni preventive: obținerea angajamentului conducerii beneficiarului că personalul său va fi informat despre importanța proiectului. Responsabili: Manager de Proiect ONRC, Manager de Proiect Ofertant
4.	Modificări în aria de cuprindere a proiectului Probabilitate: medie	Impact: mediu Consecințe: Posibile reevaluări ale obiectivului, costurilor si/sau etapelor proiectului. Acțiuni corective: Reprogramarea componentelor non-critice ale proiectului pentru etapa ulterioară. Acest proces va fi desfășurat în concordanță cu procedura de control a modificărilor. Acțiuni preventive: Asigurarea acordului tuturor factorilor decizionali importanți în privința acoperirii sistemului din faza inițială a proiectului. Responsabili: Manager de Proiect ONRC, Manager de Proiect Ofertant
5.	Lipsa cooperării din partea utilizatorilor	Nivelul de implicare a utilizatorilor este esențial atât pentru succesul sistemului cât și pentru acceptanța finală.



Nr. crt.	Risc identificat	Masuri de atenuare ale riscului
	Probabilitate: mica	Impact: mediu Consecințe: costuri suplimentare pentru proiect, cauzate de eventuala apariție a unor noi cerințe. Definirea eronată a unor cerințe funcționale. Acțiuni corective: Escaladarea către nivelurile conducerii superioare și obținerea unui angajament puternic din partea Comitetului Director. Acțiuni preventive: Utilizatorii trebuie implicați în activitățile proiectului. Dacă este necesar se vor efectua analize ale proiectului. Responsabili: Manager de Proiect ONRC, Manager de Proiect Ofertant
6.	Nu se respecta termenul de implementare tehnică al proiectului. Probabilitate: medie	Impact: mediu Consecințe: imposibilitatea respectării termenului de implementare specificat în Contractul de finanțare Acțiuni preventive: Respectarea perioadei de analiză pentru stabilirea tuturor detaliilor pentru desfășurarea dezvoltării în parametri stabiliți. Verificarea periodică a taskurilor în derulare. Acțiuni corective: stabilirea măsurilor pentru recuperarea timpului pierdut în etapele anterioare. Încheierea de acte adiționale la contractul de finanțare. Responsabili: Manager de Proiect ONRC, Manager de Proiect Ofertant
7.	Soluția finală nu respecta întocmai cerințele clientului Probabilitate: medie	Riscul apare atunci când Prestatorul nu a înțeles exact ce dorește clientul sau când nu sunt respectate specificațiile funcționale ale proiectului. Impact: Semnificativ Acțiuni preventive: Validarea tuturor etapelor intermediare, astfel încât să se poată observa cât mai rapid orice deviație și pentru a se putea lua măsurile necesare pentru corectarea deviațiilor. Responsabili: Manager de Proiect ONRC, Manager de Proiect Ofertant
8.	Soluția finală nu funcționează corespunzător Probabilitate: medie	Impact: Mediu Acțiuni preventive: stabilirea unei etape de testare internă a fiecărei componente livrate, apoi a unei testări integrate. Acțiuni corective: Asigurarea unei marje de timp pentru rezolvarea bugurilor sau problemelor apărute, existența unei echipe de testare care să descopere toate bugurile/problemele existente.



PM AGS

Nr. crt.	Risc identificat	Masuri de atenuare ale riscului
		Responsabili: Manager de Proiect ONRC, Manager de Proiect Ofertant
9.	Neagrearea unui plan formal pentru testarea functionala a sistemului informatic, bazat pe scenarii clare de testare, ceea ce poate duce la prelungirea excesiva a perioadei de testare, sau la aparitia unor noi cerințe introduse sub formă de observatii de testare. Prolungirea perioadelor de testare afecteaza si planificarea activitatilor expertilor pentru managementul proiectului. Probabilitate: medie	Impact: Mediu Actiuni preventive: Urmărirea strategiei de testare si acceptanta pentru sistemul informatic prezentată de către Prestator. Intocmirea unor scenarii de testare si acceptanta agreate de ambele parti, care sa usureze activitatea de testare. Stabilirea unei strategii de testare si acceptanta imediat dupa demararea proiectului de implementare a solutiei informatice. Responsabili: Manager de Proiect ONRC, Manager de Proiect Ofertant
10.	Existenta unor divergente de opinie de natura tehnica între expertii ONRC si expertii tehnici ai Prestatorului, care sa determine intarzierea finalizarii unor activitati din proiect. Probabilitate: medie	Impact: Mediu Actiuni preventive: Stabilirea exacta a responsabilitatilor si a nivelului de autoritate pentru fiecare din expertii / specialistii celor doua organizatii. Derularea unor intalniri in care sa fie prezentate si discutate opiniile expertilor si specialistilor celor doua organizatii. Derularea unei sesiuni de instruire preliminară pentru prezentarea tehnologiilor utilizate în proiect. Actiuni corective: Implicarea Managerului de Proiect al ONRC si a Managerului de Proiect al Ofertantului pentru medierea eventualelor dispute. Responsabili: Manager de Proiect ONRC, Manager de Proiect Ofertant

Ofertantul va identifica și alte riscuri față de cele principale, relevate mai sus. În oferta se vor prezenta recomandări/propuneri de reducere sau eliminare a riscurilor menționate și a celor identificate de către Ofertant și care ar putea afecta implementarea proiectului.

4.8 Cerințe specifice

Pentru toate componentele software dezvoltate si/sau pentru toate aplicatiile software propuse pentru desfasurarea contractului, Prestatorul va respecta urmatoarele cerinte:

- Toate licentele software necesare implementarii sistemului vor fi perpetue, in proprietatea ONRC pentru totdeauna de la momentul platii, respectiv orice componenta software furnizata va putea

sa fie folosita in mod legal pentru o perioada nedefinita de timp, in care cerintele/functionalitatile minimale din prezentul document trebuie sa ramana active, pentru sistemele oferite si pentru un numar nelimitat de utilizatori. Nu se accepta alte tipuri de licentiere software, inclusiv nu se accepta urmatoarele: leasing, inchiriere, licentiere temporara indiferent de perioada de timp oferita, licentiere cloud, etc.

- Toate componentele software se vor instala pe echipamentele prezentate in caietul de sarcini, fara a exista nici o componenta in afara sistemului prezentat in cadrul acestui caiet de sarcini. Nu se vor accepta aplicatii sau sisteme care interactioneaza cu entitati din afara rețelei ONRC, inclusiv nu se accepta sisteme care sa interactioneze cu sistemele producatorilor, sisteme de tip cloud public (extern ONRC), etc. Exceptie fac cazurile in care pentru buna functionare si mentenanta aplicatiilor si componentelor oferite si pentru buna indeplinire a cerintelor tehnice, este nevoie de interactiunea cu site-urile producatorilor sau alte site-uri (de exemplu: site-uri de update-uri pentru sistemul de operare sau aplicatii, site-uri de unde este nevoie de componente sau versiuni noi ale aplicatiilor furnizate, site-uri de firmware, BIOS, drivere, knowledge base ale producatorilor de echipamente – in orice situatie este obligatoriu ca aceste site-uri sa fie cele oficiale indicate de producatori). De asemenea, la exceptii se incadreaza si conectivitatea specifica sistemului, asa cum este prezentata in acest document.

Pe parcursul desfasurarii contractului, cat si in timpul perioadei de garantie si a asigurarii suportului pentru platforma software, ONRC isi rezerva dreptul sa verifice oricand orice livrabil realizat de Prestator, inclusiv cod sursa, proceduri de instalare, modificari in sisteme, documentatie, etc. Pentru orice neconcordanta, Prestatorul este obligat sa remedieze problema semnalata si eventual sa updateze documentele aferente.

Criteriile de acceptanță de la fiecare nivel de testare vor fi stabilite în acord cu Autoritatea Contractantă într-un plan de testare care va fi propus de prestator si validat de Autoritatea Contractanta, astfel încât să se asigure conformitatea implementarii solutiei cu specificațiile functionale stabilite.

Receptii si teste de acceptanta:

- Receptii cantitative a componentelor sistemului informatic (echipamente hardware, produse software, alte componente software, instruire)
- Punerea in functiune a infrastructurii hardware si a platformei de virtualizare si receptia calitativa prin teste de baza a functionarii acestora
- Receptie finala a sistemului informatic prin testarea intregului sistem integrat pe baza unui plan de testare agreeat;

4.9 Evaluarea performantei Contractantului

Performanta Contractantului va fi evaluata pe durata implementarii proiectului pe baza urmatoarelor indicatori de performanta. Aceste informatii vor fi utilizate inclusiv pentru eliberarea documentului constatator la finalul prestării serviciilor.

Contractantul va ține evidența valorilor asociate indicatorilor de performanță și va include informații referitoare la nivelul de performanță înregistrat în toate rapoartele și documentele întocmite pentru realizarea întâlnirilor de pe durata derulării Contractului, așa cum sunt acestea descrise în Caietul de Sarcini.

Astfel, Autoritatea Contractantă va utiliza indicatori de performanță menționați în Anexa 2 a prezentului caiet de sarcini. Performanța finală a Contractantului va fi calculată ca medie aritmetică a indicatorilor.

5 Cerințe experti cheie

5.1 Structura echipei de proiect

Prestatorul va asigura o echipă formată din experții solicitați, care vor fi responsabili de realizarea activităților din cadrul contractului, în conformitate cu cerințele beneficiarului.

Prestatorul poate suplimenta numărul de resurse alocate activităților pe perioada derulării proiectului, fără însă a solicita modificarea valorii contractului.

Echipa de proiect a Prestatorului va trebui să conțină cel puțin experți care să acopere următoarele roluri:

1. **Manager de proiect** – pentru gestionarea și controlul proiectului, urmărirea dezvoltării și rezultatelor proiectului, măsuri corective, dacă și unde este necesar – rol acoperit de un expert certificat;
2. **Manager de proiect adjunct** – pentru suplینirea managerului de proiect când acesta nu este disponibil sau în situațiile în care este necesară prezența acestuia în activități importante desfășurate în paralel – rol acoperit de un expert certificat;
3. **Arhitect soluție** – pentru designul soluției, inclusiv generarea și aprobarea specificațiilor de design – rol acoperit de un expert certificat;
4. **Coordonator analiza** – pentru coordonarea tehnică a echipei de analiză – rol acoperit de un expert certificat;
5. **Analist de business** – care să înțeleagă sistemul, tipul de informații existente în el și structura acestora, să extragă cerințele detaliate și să elaboreze specificațiile funcționale – rol acoperit de experți certificați;
6. **Expert integrare** – pentru analiza sistemelor existente, elaborarea specificațiilor și riscurilor specifice, instalarea și configurarea produselor aferente subsistemelor – rol acoperit de un expert certificat;
7. **Expert implementare software** – pentru implementarea soluțiilor software oferite – rol acoperit de un expert certificat;
8. **Expert baze de date** – pentru managementul bazelor de date folosite pentru proiect, inclusiv al structurii acestora – rol acoperit de un expert certificat;
9. **Coordonator dezvoltare software** – pentru coordonarea tehnică a echipei care va realiza dezvoltarea componentelor funcționale care nu pot fi implementate utilizând produse comerciale existente – rol acoperit de un expert certificat;

10. **Expert dezvoltare aplicatii software** – pentru dezvoltarea componentelor software – rol acoperit de experți certificați;
11. **Expert dezvoltare aplicatii mobile** – pentru dezvoltarea componentelor software aferente aplicatiilor mobile – rol acoperit de un expert certificat;
12. **Coordonator testare** – pentru coordonarea tehnica a echipei care va realiza testarea – rol acoperit de un expert certificat;
13. **Expert testare software** – pentru testarea componentelor dezvoltate și asigurarea calității componentelor – rol acoperit de experți certificați;
14. **Expert infrastructura / virtualizare** – pentru instalarea, configurarea si managementul sistemului de virtualizare oferat si al componentelor de infrastructura – rol acoperit de un expert certificat;
15. **Expert comunicatii** – pentru prestarea de activitati specifice proiectarii si implementarii din punct de vedere securitate a comunicatiilor sistemului informatic – rol acoperit de un expert certificat;
16. **Expert testare de securitate** – pentru testarea de securitate a componentelor dezvoltate si a sistemului in ansamblu sau si identificarea vulnerabilitatilor – rol acoperit de un expert certificat;
17. **Expert securitatea informatiei** – pentru crearea, configurarea si implementarea solutiilor de securitate a datelor și a sistemelor informatice – rol acoperit de experți certificați;
18. **Expert instruire** – pentru organizarea structurii instruirii, crearea materialelor de instruire și a cursurilor, sustinerea cursurilor – rol acoperit de un expert certificat;
19. **Coordonator suport tehnic** – pentru gestionarea serviciilor de suport tehnic pe perioada de garantie a sistemului informatic ce va fi implementat – rol acoperit de un expert certificat;
20. **Expert suport tehnic** – pentru activitati de suport si asistenta tehnica – rol acoperit de experți certificați;

ONRC va oferi suport tehnic pentru implementare prin intermediul personalului propriu, punând la dispoziția Prestatorului informațiile necesare despre infrastructura existentă și, de asemenea, cu privire la sursele și specificul datelor existente în cadrul organizației.

Echipele de proiect din partea ONRC se va implica în întregul proces de implementare, pentru a acumula experiența practică necesară pentru operarea și administrarea ulterioară a sistemului informatic.

5.2 Responsabilitatile expertilor cheie

5.2.1 Manager de proiect – 1 persoana

Responsabilitati:

- Activitati specifice de management de proiect (legat de obiectul contractului)
- Punct principal de contact in relația cu beneficiarul
- Managementul contractului
- Managementul proiectului in ansamblu sau, managementul ariei de cuprindere, managementul schimbarilor, planificarea generala a proiectului, managementul riscurilor, managementul problemelor, managementul comunicarii
- Asigurarea resurselor proiectului
- Managementul, organizarea, alocarea si planificarea echipei de proiect
- Identificarea riscurilor si propunere de solutii pentru diminuarea/evitarea riscurilor

- Rezolvarea problemelor in scopul evitarii situațiilor de criza
- Urmărirea respectării tuturor termenelor conform planului de proiect
- Analiza modalității prin care livrabilele proiectului corespund cerințelor de business
- Realizarea rapoartelor periodice / ad-hoc ale proiectului.
- Elaborarea planurilor de calitate
- Verificarea și asigurarea calitatii livrabilelor

5.2.2 Manager de proiect adjunct – 1 persoana

Responsabilitati:

- Activități specifice de management de proiect (legat de obiectul contractului), atunci când managerul de proiect nu este disponibil
- Punct secundar de contact în relația cu beneficiarul
- Rezolvarea problemelor in scopul evitarii situațiilor de criza
- Urmărirea respectării tuturor termenelor conform planului de proiect
- Analiza modalității prin care livrabilele proiectului corespund cerințelor de business
- Verificarea și asigurarea calitatii livrabilelor

5.2.3 Arhitect soluție – 1 persoana

Responsabilitati:

- Definirea arhitecturii generale a soluției
- Definirea, împreună cu coordonatorul tehnic, a soluțiilor detaliate pentru componentele sistemului
- Definirea arhitecturii de integrare a componentelor
- Definirea modelului de date al subsistemului și pentru procesele de extragere, transformare și încărcare în noile structuri de date
- Identificarea riscurilor și problemelor tehnice și a soluțiilor de rezolvare

5.2.4 Coordonator analiza – 1 persoana

Responsabilitati:

- Coordonează activitățile de analiză a cerințelor de business, elaborare a documentelor de specificații funcționale și a scenariilor de testare
- Activități de implementare, asistență și suport tehnic
- Suport acordat utilizatorilor cheie pentru testarea de acceptanță a sistemului

5.2.5 Analist de business – 3 persoane

Responsabilitati:

- Analiza cerințele de business
- Realizarea documentelor de specificații funcționale și a scenariilor de testare
- Activități de implementare, asistență și suport tehnic
- Suport acordat utilizatorilor cheie pentru testarea de acceptanță a sistemului

5.2.6 Expert integrare – 1 persoana

Responsabilitati:

- activitati specifice integrării noului sistem in cadrul sistemului actual ONRC;
- activitati specifice implementării bazelor de date aferente noului sistem;
- asistenta si suport tehnic;
- adaptări/actualizări/îmbunătățiri/extinderi ale interfetelor existente sau dezvoltate între componentele sistemului;
- testarea interfetelor, testarea sistemului;
- crearea/ actualizarea documentatiilor de administrare;

5.2.7 Expert implementare software – 1 persoana

Responsabilitati:

- Activitati specifice de instalare si configurare a produselor software oferitate
- Crearea si actualizarea documentatiilor de administrare a produselor software
- Activitati de implementare, asistenta si suport tehnic

5.2.8 Expert baze de date – 1 persoana

Responsabilitati:

- Activitati specifice de instalare si administrare baze de date in arhitecturi redundante
- Activitati specifice replicării datelor din baza de date
- Asistenta si suport tehnic
- Testare
- Crearea/ actualizarea documentatiilor de administrare

5.2.9 Coordonator dezvoltare software – 1 persoana

Responsabilitati:

- Coordonarea echipei si a activitatilor de dezvoltare de aplicatii software
- Asigura suport tehnic in activitățile de implementare
- Rezolva disfunctionalitati software (bug-uri)
- Asigura suport tehnic in perioada de garantie
- crearea/ actualizarea documentatiilor

5.2.10 Expert dezvoltare aplicatii software – 6 persoane

Responsabilitati:

- Activitati specifice privind dezvoltarea de aplicatii software, pe baza documentelor de analiza, specificatii functionale, specificatii tehnice, arhitectura sistem
- Testare unitara (interna)
- Suport in activitățile de implementare
- Rezolvarea disfunctionalitatilor software (bug-uri)
- Asigurarea suportului tehnic in perioada de garantie
- Crearea/ actualizarea documentatiilor

5.2.11 Expert dezvoltare aplicatii mobile – 1 persoana

Responsabilitati:

- Activitati specifice privind dezvoltarea de aplicatii mobile
- Rezolvarea disfunctionalitatilor software (bug-uri)
- Asigurarea suportului tehnic in perioada de garantie
- Crearea/ actualizarea documentatiilor

5.2.12 Coordonator testare – 1 persoana

Responsabilitati:

- Coordonarea echipei si activitatilor de testare
- Activitati specifice testarii de aplicatii software
- Implementarea planurilor, scenariilor si cazurilor de test
- Activitati de testare componente si testare functionala
- Intocmirea si livrarea rapoartelor de testare si implementare

5.2.13 Expert testare software – 2 persoane

Responsabilitati:

- Prestarea de activitati specifice testarii de aplicatii software
- Implementarea planurilor, scenariilor si cazurilor de test
- Activitati de testare componente si testare functionala
- Intocmirea si livrarea rapoartelor de testare si implementare

5.2.14 Expert infrastructura / virtualizare – 1 persoana

Responsabilitati:

- activitati specifice implementarii infrastructurii / sistemului de virtualizare aferente sistemului;
- asistenta si suport tehnic;
- adaptări/actualizări/îmbunătățiri/extinderi/ configurari ale sistemului de virtualizare;
- testarea sistemului de virtualizare;
- crearea/ actualizarea documentatiilor de administrare;

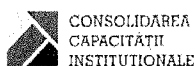
5.2.15 Expert comunicatii – 1 persoana

Responsabilitati:

- Activitati specifice proiectarii si implementarii din punct de vedere securitate a comunicatiilor sistemului informatic implementat, atat din punct de vedere software, cat si hardware
- Activitati de proiectare, instalare si configurare retele de comunicatie redundante
- Asistenta si suport tehnic
- Crearea/ actualizarea/ verificarea documentatiilor

5.2.16 Expert testare de securitate – 1 persoana

Responsabilitati:



Proiect cofinanțat din Fondul Social European prin
Programul Operațional Capacitate Administrativă 2014-2020!

- Prestarea activitatilor specifice testarii de securitate a sistemelor informatice
- Testarea eficientei controalelor de securitate implementate in proiect
- Identificarea vulnerabilitatilor existente la nivelul sistemului
- Implementarea planurilor, scenariilor si cazurilor de test
- Activitati de testare componente si testare functionala
- Intocmirea si livrarea rapoartelor de testare si implementare

5.2.17 Expert securitatea informatiei – 1 persoana

Responsabilitati:

- Definirea solutiei de securitate in etapa de analiza
- Configurarea din punct de vedere al securitatii a sistemelor informatice
- Consultanta de specialitate pentru echipa de proiect in timpul derularii proiectului
- Realizarea planului de securitate a sistemului informatic
- Realizarea planurilor de continuitate si recuperare in caz de dezastru
- Instructaj pentru administratorii sistemului informatic
- Instructaj privind constientizarea securitatii pentru utilizatorii sistemului informatic
- Intocmirea si livrarea rapoartelor de testare si implementare

5.2.18 Expert instruire – 1 persoana

Responsabilitati:

- Organizarea structurii de instruire
- Derularea activitati de instruire utilizatori;
- Pregatirea materialelor de curs si a testelor;
- Pregatirea raportului de curs.

5.3 Cerinte minime obligatorii ale expertilor cheie

Numarul minim de persoane necesar pentru fiecare expert este mentionat in dreptul acestuia. Fiecare dintre persoanele propuse trebuie sa indeplineasca integral toate cerintele minime aferente expertului (profilului de persoana) pentru care au fost nominalizate. Nu se accepta indeplinirea cerintelor minime aferente unui expert prin cumul de catre mai multe persoane.

5.3.1 Manager de proiect – 1 persoana

- Absolvent studii superioare finalizate cu diploma de licenta
- Competente privind managementul de proiect dovedite prin certificare recunoscuta la nivel national / international
- Experienta specifica in cel putin un proiect sau contract in care a indeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

5.3.2 Manager de proiect adjunct – 1 persoana

- Absolvent studii superioare finalizate cu diploma de licență
- Competențe privind managementul de proiect dovedite prin certificare recunoscută la nivel național / internațional
- Experiența specifică în cel puțin un proiect sau contract în care a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

5.3.3 Arhitect soluție – 1 persoana

- Absolvent studii superioare finalizate cu diploma de licență
- Competențe în domeniul arhitecturilor de tip Enterprise dovedite prin certificare recunoscută la nivel național / internațional
- Experiența specifică în cel puțin un proiect sau contract de dezvoltare/ implementare/ extindere sistem informatic în care a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

5.3.4 Coordonator analiză – 1 persoana

- Absolvent studii superioare finalizate cu diploma de licență
- Competențe privind analiza de business dovedite prin certificare în domeniu
- Competențe privind managementul și modelarea proceselor de business dovedite prin certificare în domeniu
- Experiența specifică în cel puțin un proiect sau contract de dezvoltare/ implementare/ extindere sistem informatic în care a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

5.3.5 Analist de business – 3 persoane

- Absolvent studii superioare finalizate cu diploma de licență
- Competențe privind analiza de business dovedite prin certificare în domeniu
- Experiența specifică în cel puțin un proiect sau contract în care a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

5.3.6 Expert integrare – 1 persoana

- Absolvent studii superioare finalizate cu diploma de licență
- Competențe în domeniul arhitecturilor de tip Enterprise, dovedite prin certificare recunoscută la nivel național/ internațional
- Competențe privind platforma de gestiune a arhivei utilizată în cadrul SAE dovedite prin certificare/diploma recunoscută la nivel național/ internațional
- Competențe privind administrarea bazelor de date dovedite prin certificare/diploma recunoscută la nivel național/ internațional
- Experiența specifică în cel puțin un proiect sau contract de dezvoltare/ implementare/ extindere sistem informatic în care a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

5.3.7 Expert implementare software – 1 persoana

- Absolvent studii superioare finalizate cu diploma de licență
- Competențe în domeniul IT pentru cel puțin 2 din următoarele domenii: sisteme de operare / aplicații software / portal / servere de aplicație, dovedite prin certificări recunoscute la nivel național / internațional
- Experiența specifică în cel puțin un proiect sau contract de dezvoltare/ implementare/ extindere sistem informatic în care a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

5.3.8 Expert baze de date – 1 persoana

- Absolvent studii superioare finalizate cu diploma de licență;
- Competențe privind administrarea bazelor de date în configurație cluster dovedite prin certificare în domeniu recunoscută la nivel național/ internațional
- Competențe privind optimizarea performanței bazelor de date dovedite prin certificare în domeniu recunoscută la nivel național/ internațional
- Experiența specifică în cel puțin un proiect sau contract de dezvoltare/ implementare/ extindere sistem informatic în care a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

5.3.9 Coordonator dezvoltare software – 1 persoana

- Absolvent studii superioare finalizate cu diploma de licență
- Competențe privind o metodologie de dezvoltare software, recunoscută la nivel național/ internațional, dovedite prin certificare în domeniu
- Competențe privind dezvoltarea de software dovedite prin certificare în domeniu obținute la nivel național sau internațional (pentru absolvenții de studii superioare la facultăți cu profil informatic/calculatoare, este suficientă diploma de absolvire).
- Experiența specifică în cel puțin un proiect sau contract de dezvoltare/ implementare/ extindere sistem informatic în care a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

5.3.10 Expert dezvoltare aplicații software – 6 persoane

- Absolvent studii superioare finalizate cu diploma de licență
- Competențe privind dezvoltarea de software dovedite prin certificare în domeniu obținute la nivel național sau internațional (pentru absolvenții de studii superioare la facultăți cu profil informatic/calculatoare, este suficientă diploma de absolvire)
- Experiența specifică în cel puțin un proiect sau contract de dezvoltare/ implementare/ extindere sistem informatic în care a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

5.3.11 Expert dezvoltare aplicatii mobile – 1 persoana

- Absolvent studii superioare finalizate cu diploma de licenta
- Competente privind dezvoltarea de aplicatii mobile pentru iOS / Android dovedite prin certificare in domeniu
- Experiența specifica in cel puțin un proiect sau contract de dezvoltare/ implementare/ extindere sistem informatic in care a indeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

5.3.12 Coordonator testare – 1 persoana

- Absolvent studii superioare finalizate cu diploma de licenta
- Competente privind testarea sistemelor informatice, dovedite prin certificare in domeniu recunoscuta la nivel national/ international
- Experiența specifica in cel puțin un proiect sau contract de dezvoltare/ implementare/ extindere sistem informatic in care a indeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

5.3.13 Expert testare software – 2 persoane

- Absolvent studii superioare finalizate cu diploma de licenta
- Competente privind testarea sistemelor informatice, dovedite prin certificare in domeniu recunoscuta la nivel national/ international
- Experiența specifica in cel puțin un proiect sau contract de dezvoltare/ implementare/ extindere sistem informatic in care a indeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

5.3.14 Expert infrastructura / virtualizare - 1 persoana

- Absolvent studii superioare finalizate cu diploma de licenta;
- Competente in domeniul sistemelor de operare de tip Enterprise, dovedite prin certificare recunoscuta la nivel national/ international
- Competente in domeniul IT pentru cel puțin unul din urmatoarele domenii: servere / sisteme de stocare , dovedite prin certificari recunoscute la nivel national / international
- Competente privind sisteme de virtualizare, dovedite prin certificare recunoscuta la nivel national/ international
- Experiența specifica in cel puțin un proiect sau contract de dezvoltare/ implementare/ extindere sistem informatic in care a indeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

5.3.15 Expert comunicatii – 1 persoana

- Absolvent studii superioare finalizate cu diploma de licenta;
- Competente privind implementarea, administrarea si depanarea tehnologiilor avansate de rutare si switching, dovedite prin certificare recunoscuta la nivel national/ international

- Competențe privind administrarea și gestiunea securitatea rețelelor dovedite prin certificare recunoscută la nivel național/ internațional
- Experiența specifică în cel puțin un proiect sau contract de dezvoltare/ implementare/ extindere sistem informatic în care a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

5.3.16 Expert testare de securitate – 1 persoană

- Absolvent studii superioare finalizate cu diploma de licență
- Competențe privind testarea de securitate a sistemelor informatice, dovedite prin certificare recunoscută la nivel național/ internațional
- Experiența specifică în cel puțin un proiect sau contract în care a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

5.3.17 Expert securitatea informației – 1 persoană

- Absolvent studii superioare finalizate cu diploma de licență;
- Competențe privind securitatea datelor și a sistemelor informatice, dovedite prin certificare recunoscută la nivel național/ internațional
- Experiența specifică în cel puțin un proiect sau contract de dezvoltare/ implementare/ extindere sistem informatic în care a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

5.3.18 Expert instruire – 1 persoană

- Absolvent studii superioare finalizate cu diploma de licență
- Competențe de instruire, dovedite prin diploma de formator
- Experiența specifică în cel puțin un proiect sau contract în care a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

Ofertanții trebuie să prezinte în oferta tehnică, pentru fiecare expert solicitat următoarele informații/documente:

- Numele persoanei propuse pentru fiecare poziție (de exemplu pentru dezvoltator software sunt cerute minim 2 poziții și pentru fiecare dintre acestea trebuie nominalizată câte o persoană),
- Declarația de disponibilitate semnată de persoana propusă (în cazul în care aceasta nu este angajat al Prestatorului)
- CV
- Documente justificative relevante care demonstrează îndeplinirea cerințelor:
- copiile documentelor relevante care demonstrează îndeplinirea cerințelor referitoare la studiile, expertiza și experiența specifică relevantă solicitată și prezentată în CV, cum ar fi:
 - copii diplome de studii, certificări, alte diplome relevante,
 - copii ale recomandărilor emise de beneficiarii finali ai proiectelor, semnate sau contrasemnate de către Autoritatea Contractantă/beneficiarul privat în calitate de

beneficiar final, sau alte documente edificatoare, din care sa reiasa activitatile desfasurate si care sa evidentieze experienta profesionala specifica similara

Copiile documentelor trebuie sa fie confirmate pentru conformitate cu originalul documentelor respective. Certificatele/ diplomele/ documentele justificative emise in alta limba decat limba română vor fi prezentate in limba de origine, insotite de traducerea autorizata in limba română.

Ofertantul are obligatia ca in cadrul ofertei depuse, sa mentioneze cel putin urmatoarele elemente pentru a demonstra experienta minima in proiecte a personalului propus:

- Denumirea proiectului, beneficiarul și perioada de realizare a proiectelor în care a acumulat experiența solicitată, precum și obiectivele proiectului respectiv.
- Date de contact ale unei persoane de la beneficiarul final al proiectului care poate confirma experienta similara
- Activitatile prestate de catre persoana propusa
- Perioada de timp in care persoana propusa a desfasurat activitatile mentionate in cadrul proiectului propus

Autoritatea Contractantă are dreptul de a verifica exactitatea informațiilor și a dovezilor furnizate de ofertanți si de a solicita și alte documente/ informații care să clarifice experiența similara respectiva.

In urma verificarii exactitatii informațiilor și a dovezilor furnizate de catre ofertanți, Autoritatea Contractantă poate solicita și alte documente/informații care să clarifice experiența profesionala solicitata. De asemenea, Autoritatea Contractantă isi rezerva dreptul de a contacta beneficiarii finali ai proiectelor prezentate la experienta profesionala, in vederea confirmarii celor prezentate de catre ofertanti.

Persoanele propuse vor fi de preferat vorbitori de limba romana la un nivel avansat. In cazul persoanelor care nu sunt vorbitori de limba română, prestatorul va pune la dispoziție interpreți/ traducători autorizați in domeniul IT în vederea comunicării cu personalul autorității contractante și în vederea traducerii livrabilelor ce trebuie predate autorității contractante în limba română. Ofertantul declarat castigator este responsabil de acoperirea tuturor cheltuielilor referitoare la interpreți/ traducători/ traduceri.

Pentru persoanele propuse care au calitatea de salariați ai ofertantului, se va prezenta în mod obligatoriu orice document prin care sa se demonstreze relatia contractuala dintre persoanele nominalizate si ofertant (extras Revisal/ contract de munca, etc.). În cazul în care se propune personal care nu este salariat al Prestatorului, fiecare astfel de persoana va completa si va semna o declarație de disponibilitate semnata de aceasta, cu referire stricta la obiectul contractului ce face obiectul prezentei proceduri.

6 Modalitatea de întocmire a ofertei

Pentru fiecare componentă, hardware sau software, se va preciza în mod clar denumirea, producătorul, cantități, capacități, referințe la materiale din care să reiasă în mod clar soluția oferată.

Pentru toate echipamentele hardware, ofertanții vor include în ofertă configurațiile propuse astfel încât să poată fi verificat fiecare subsistem (exemplu tipul de procesor propus sau tipul de memorie propus).

Nicio componentă software din cele ofertate nu trebuie să aibă vreo limitare de timp de licențiere care să prevină folosirea acesteia după o anumită perioadă de timp sau să condiționeze continuarea folosirii acesteia de achiziționarea de suport sau servicii suplimentare.

9. Descrierea părților de contract subcontractate, a interacțiunii dintre ofertant și subcontractor/i, precum și o descriere detaliată a serviciilor ce vor fi subcontractate.
10. Oferta financiară va fi prezentată detaliat și va conține prețurile unitare pentru fiecare echipament, produs software sau serviciu inclus în propunerea tehnică.
11. Propunerea tehnică va conține și alte informații considerate semnificative de ofertant sau orice alte constrângeri, pentru evaluarea corespunzătoare a propunerii tehnice.
12. Ofertantul are obligația de a detalia modul de abordare și gestionare a relației cu subcontractorii, în raport cu activitățile subcontractate (daca este cazul).

Notă - condiții generale și particulare:

1. Prin depunerea unei oferte, ofertantul acceptă în prealabil condițiile generale și particulare care guvernează acest contract, după cum sunt acestea prezentate în Documentația de atribuire, ca singură bază a acestei proceduri de atribuire, indiferent care sunt condițiile proprii de vânzare ale ofertantului.
2. Ofertanții au obligația de a analiza cu atenție documentația de atribuire și să pregătească oferta conform tuturor instrucțiunilor, formularelor, prevederilor contractuale și Caietului de sarcini conținute în această documentație.
3. Niciun cost suportat de operatorul economic pentru pregătirea și depunerea ofertei nu va fi rambursat. Toate aceste costuri vor fi suportate de către operatorul economic ofertant, indiferent de rezultatul procedurii.
4. Presumpția de legalitate și autenticitate a documentelor prezentate: ofertantul își asumă răspunderea exclusivă pentru legalitatea și autenticitatea tuturor documentelor prezentate în original și/sau copie în vederea participării la procedură.
5. Analizarea de către comisia de evaluare a documentelor prezentate de ofertanți nu angajează din partea acestora nicio răspundere sau obligație față de acceptarea acestora ca fiind autentice sau legale și nu înlătură răspunderea exclusivă a ofertantului sub acest aspect.

7 Criterii de atribuire

Criteriul de atribuire este cel mai bun raport calitate-pret.

ALGORITM DE CALCUL

Evaluarea ofertelor se va face în ordinea descrescătoare a punctajului total obținut din punctajul tehnic și financiar, pe baza ponderilor prezentate în fișa de date a achiziției, pentru fiecare dintre criteriile respective.

Oferta care obține cel mai mare număr de puncte va fi declarată câștigătoare.

Evaluarea ofertelor se va realiza pe baza următoarelor criterii și a punctajul aferent obținut de fiecare oferta evaluată.

Punctajul total acordat pentru fiecare ofertă se calculează pe baza formulei:

Punctaj Total Ofertant A = Punctaj „Prețul ofertei” Ofertant A + Punctaj „Propunerea tehnică - Experiența profesională a personalului” Ofertant A + Punctaj “Propunerea tehnică – Capabilitati solutie tehnica” Ofertant A + Punctaj „Propunerea tehnică - Demonstrarea unei metodologii adecvate de implementare a contractului” Ofertant A

Soluția propusă nu trebuie să aibă alte limitări de licențiere sau de altă natură care să prevină folosirea acesteia în scopul în care a fost achiziționată.

Oferta se va prezenta într-un format în care să permită copierea textului cu formatare.

Oferta va cuprinde obligatoriu fisele tehnice, manualele sau/și ghidurile de prezentare sau orice alte documente relevante pentru toate echipamentele, componentele și produsele software prezentate, astfel încât să rezulte faptul că acestea respecta cerințele minime din prezentul caiet de sarcini.

Propunerea tehnică va fi elaborată astfel încât să rezulte că sunt îndeplinite în totalitate cerințele aferente Caietului de sarcini. Propunerea tehnică trebuie să reflecte asumarea de către ofertant a tuturor cerințelor și obligațiilor prevăzute în Caietul de sarcini.

Propunerea tehnică va respecta obligatoriu următoarele cerințe:

- 1. Ofertantul va prezenta o singură ofertă cu respectarea cerințelor Caietului de Sarcini.*
- 2. Propunerea tehnică va fi întocmită în conformitate cu solicitările din caietul de sarcini, acestea fiind considerate minime și obligatorii.*
- 3. Ofertantul va detalia modul în care echipamentele, componentele și produsele software oferite răspund la fiecare dintre cerințele enumerate în parte, specificând în clar identificatorul unic producător asociat fiecărui echipament, numărul de echipamente oferite pentru fiecare tip de echipament, configurația, funcționalitățile și opțiunile acestora. Separat, vor fi prezentate de asemenea și funcționalitățile suplimentare, dacă este cazul. Nu se acceptă echipamente scoase din fabricație sau la finalul ciclului de vânzare. Se acceptă livrarea doar de echipamente noi.*
- 4. Ofertantul va detalia lista licențelor propuse în propunerea tehnică, specificând în clar numele licenței de la producător, ediția, producătorul, cantitatea și unitățile de licențiere specifice producătorului, precum și corelarea acestora cu cerințele caietului de sarcini.*
- 5. Prezentarea modului de îndeplinire a cerințelor funcționale și tehnice solicitate în caietul de sarcini: ofertantul va prezenta sub forma tabelară, explicațiile, valorile și documentele doveditoare pentru toate caracteristicile solicitate în caietul de sarcini (matrice de complianță), răspunzând punct cu punct la toate cerințele prezentei documentații și detaliind soluția oferită într-un mod care să permită verificarea cu ușurință a conformității.*
- 6. Propunerea tehnică va conține descrierea metodologiei de implementare ce va fi aplicată pe durata proiectului, care trebuie să fie de tip iterativ și bazată pe o metodologie recunoscută la nivel internațional. Dacă este cazul se va prezenta contribuția fiecărui membru al grupului de operatori economici/subcontractant, precum și distribuția și interacțiunea sarcinilor și responsabilităților dintre acestia.*
- 7. Propunerea tehnică va conține descrierea procedurii de gestiune a schimbării.*
- 8. În cadrul propunerii tehnice, se va prezenta obligatoriu un grafic de execuție, în format Gantt în care trebuie să includă cel puțin toate activitățile necesare pentru implementarea cu succes a proiectului, inclusiv dependențele dintre acestea, respectiv rezultatele acestora, pentru fiecare activitate a proiectului, se vor menționa resursele umane alocate, precum și nivelul de implicare al fiecărei resurse în activitățile proiectului (pentru fiecare activitate în parte), precizând fazele/subfazele de bază de realizare a activităților, evidențiindu-se reperele de referință, succesiunea activităților și numărul de zile/om de implicare în proiect pentru experți.*

Criteriile de evaluare propuse sunt:

Nr. crt.	Factori de evaluare	Pondere %
1.	Pretul ofertei	50
2.	Propunere tehnică – Capabilitati solutie tehnica	30
3.	Propunerea tehnica – Experiența profesionala a personalului	15
4.	Propunerea tehnică – Demonstrarea unei metodologii adecvate de implementare a contractului	5
Total		100

Notă: toate calculele se vor face cu 4 zecimale, iar rotunjirile se vor face la 2 zecimale, conform funcției ROUND din Microsoft Excel – ROUND(formula, 2) – pentru fiecare din calculele aferente evaluării ofertelor. Funcția ROUND se va aplica pentru întreaga formula de calcul, pentru fiecare etapă a calculului. Pentru criteriile de evaluare 3 și 4, fiecare subfactor va fi apreciat în funcție de calificativul foarte bine/bine, acceptabil. Comisia de evaluare va acorda calificativul luând în considerare liniile directorare prezentate în tabele aferente. Punctajul tehnic total al ofertei se calculează prin însumarea punctajelor tehnice obținute în urma aplicării fiecărui subfactor de evaluare. Punctajul aferent unui subfactor de evaluare va fi obținut prin acordarea notei corespunzătoare calificativului obținut de oferta respectivă la evaluarea aceluia subfactor.

În cazul în care mai multe oferte eligibile obțin același punctaj total (tehnic + financiar), atunci se va solicita o nouă ofertă financiară ofertanților clasati pe primul loc.

7.1 Descrierea modalitatii de punctare a factorului de evaluare “Pretul ofertei”

Factor de evaluare	Modalitate de punctare	Punctaj maxim
1. Pretul ofertei	Punctajul financiar se acordă astfel: a. Pentru cel mai mic dintre prețurile oferite se acordă 50 de puncte; b. Pentru alt preț decât cel prevăzut la litera a) se acordă punctaj astfel:	50 puncte
	Punctaj Financiar Ofertant A = Pret minim ofertat ÷ Pret Ofertant A × 50	
	Se vor compara prețurile fara TVA prezentate în propunerea financiara.	

7.2 Descrierea modalitatii de punctare a factorului de evaluare “Propunerea tehnică – Capabilitati solutie tehnica”

Numar maxim de puncte: 30 puncte.

Acordare punctajului „Capabilitati solutie tehnica” se va face în felul urmator:

Element evaluat	Punctaj
Componenta de replicare captureaza si replica modificarile la sursa in momentul in care acestea au loc, fara sa astepte finalizarea tranzactiei. Acest procedeu este utilizat si de baza de date Oracle (procesul dbwriter) pentru a reduce semnificativ necesarul de banda utilizat, memoria consumata de procesul de replicare (deoarece nu se pastreaza tranzactia la sursa pana la finalizarea acesteia) si din acelasi motiv, pentru a reduce semnificativ intarzierea aplicarii datelor la destinatie.	1.5
Componenta de replicare include funcționalități de comparare și reparare ale datelor, astfel încât să fie facila introducerea de noi tabele în replicare si repararea sincronizarii tabelor existente în replicare.	1.5
Componenta de gestiune a documentelor permite stocarea compresata si criptata a fisierelor in depozitul de documente vor sta in forma compresata pentru economisirea spatiului si criptat cu standard AES256 sau echivalent	1.5
Componenta de gestiune a documentelor include la nivelul de depozitului de documente functii de realizare a conformitatii cu standardul GDPR cum ar fi dar fara a se limita la: pseudonimizare, anonimizare, scopul preluarii datelor, nivel de securitate, categorii de date din punct de vedere GDPR, audit la nivel de inregistrare	1.5
Interfata web a componentei de gestiune a documentelor utilizatorului rezultatele căutării sub forma unei liste care cuprinde documente corespunzatoare criteriului selectat si permite cautari specifice in subsetul rezultat din cautare	1.5
Componenta de dezvoltare aplicatii mobile sa permita actualizarea in timp real a aplicatiilor instalate pe dispozitive (inclusiv corectii rapide ale aplicatiei) fara a fi necesara actualizarea in magazinul de aplicatii (app store)	1.5
Componenta de dezvoltare aplicatii mobile sa permita monitorizarea in timp real a problemelor / erorilor aparute la nivelul aplicatiilor instalate pe dispozitivele mobile cu corelarea erorii cu codul sursa al aplicatiei dezvoltate si notificarea dezvoltatorului in cazul aparitiei de erori neasteptate.	1.5
Componenta gestiune a ciclului de viata a aplicatiilor permite integrarea cu componenta testare performanta pentru gestiunea testelor de performanta	1.5
Componenta gestiune a ciclului de viata a aplicatiilor permite integrarea cu componenta testare automata pentru gestiunea si automatizarea testelor functionale	1.5
Componenta de testare automata permite reducerea timpului de testare prin executia simultana de teste distribuite;	1.5
Componenta de testare de performanta permite rularea testelor definite la nivel de API in componenta de testare automata a aplicatiilor (pentru testarea incarcarii);	1.5
Componenta de testare de performanta permite obtinerea de analize comparative intre mai multe rulari de teste cu scopul de dimensionare a capacitatii sistemului sau de testare intre versiuni diferite de software.	1.5

<p>Componenta de testare de performanta permite localizarea, extragerea si inlocuirea valorilor dinamice din cadrul paginilor web precum id-ul de sesiune, authentication token, customer id, etc asigurand astfel acceptarea cererilor de catre serverele web supuse testarii</p>	1.5
<p>Componenta centrala de protectie avansata antimalware permite compararea comportamentului manifestat de rularea software-ului malițios pe diferite configurații ale mașinilor virtuale de analiză (de exemplu: versiuni diferite ale sistemului de operare, ale aplicațiilor uzuale, configurări diferite ale sistemelor de operare, actualizări aplicate sistemelor de operare, patch-uri sau service pack-uri), in vederea evaluarii cat mai exacte a impactului acestora la nivelul sistemelor aflate in exploatare</p>	1.5
<p>Componenta centrala de protectie avansata antimalware permite personalizarea facila a mecanismului de sandbox-ing prin operatiuni de import/export a sistemelor de operare/setului de aplicatii disponibil in mediul de tip sandbox, inclusiv prin incarcarea integrala a unor imagini de sistem de operare standard (gold image), in scopul reflectarii realitatii relevante din mediul productiv al Autoritatii Contractante la un moment dat.</p>	1.5
<p>Componenta de protectie a resurselor la nivel de post de lucru permite asigurarea protectiei impotriva amenintarilor de tip ransomware cu recuperarea datelor din backup. Astfel solutia trebuie sa ofere mecanisme automatizate de salvare a datelor in momentul detectiei unui element de tip ransomware, respectiv sa blocheze procesul de criptare initiat de elementul de tip ransomware si sa recupereze datele in eventualitatea in care procesul de criptare a fost declansat</p>	1.5
<p>Componenta de redistributie a accesului la serviciile de aplicatie permite extinderea functionalitatilor native prin limbaj de scripting care sa ofere suport pentru :</p> <ul style="list-style-type: none"> ▪ folosirea declaratiilor conditionale (if/then) si a buclelor (for, while); ▪ generarea de alerte si executia de script-uri pe baza diferitelor tipuri de evenimente; ▪ alterarerea cererii sau a raspunsului pe baza de: origine, tip, semnatura sau datele continute in cerere/raspuns <p>in scopul personalizarii solutiei pentru nevoi punctuale ce vor fi identificate in dreularea proiectului</p>	1.5
<p>Componenta de management a datelor de audit ofera mecanisme integrate de anonimizare si mascare a datelor confidentiale din afisarea rezultatelor de cautare asupra seturilor de date de audit, in scopul respectarii reglementarilor legale in vigoare, inclusiv a conformitatii cu GDPR</p>	1.5
<p>Componenta de management a datelor de audit include mecanisme de analiza bazata pe algoritmi matematici (Machine Learning), respectiv permite definirea propriilor modele algoritmice de analiza plecand de la modelele componente si/sau prin integrarea de limbaje Opensource dedicate (unelte de tip SDK, Toolkit, etc integrate), in scopul minimizarii</p>	1.5

efortului de valorificare a informatiei si a asigurarii unei flexibilitati sporite in gestiunea datelor de audit	
Componenta de management al datelor de audit permite colectarea, analiza si corelarea datelor de la toate sistemele, aplicatiile si serviciile din infrastructura, fara a se baza pe un sistem de baza de date suport, depasind astfel limitarile de performanta generate de structurarea datelor intr-un sistem relational de baza de date	1.5
Total	30

Ofertantii vor descrie in detaliu in cadrul ofertei modul de functionare a componentelor sistemului cu referire la aspectele supuse evaluarii acestui criteriu de atribuire. In cazul in care descrierea tehnica este incompleta (adica nu acopera aspectele ce vor fi evaluate sau nu sunt punctate functionalitatile utilizate in acest sens de la nivelul componentelor software de baza), Achizitorul isi rezerva dreptul de a nu acorda punctajul aferent in cadrul acestui criteriu de atribuire. Doar simpla mentiune, nejustificata in detaliu din punct de vedere tehnic in cadrul ofertei, ca solutia indeplineste cerintele nu va fi luata in considerare de catre Achizitor.

7.3 Descrierea modalitatii de punctare a factorului de evaluare "Propunerea tehnica - Experiența profesionala a personalului"

Prin acest factor se va realiza evaluarea experientei profesionale a persoanelor propuse pentru anumite pozitii de experti solicitate in Caietul de sarcini. Persoanele pentru care se va face evaluarea vor avea responsabilitatea realizarii efective a activitatilor si proceselor de executie aferente derularii contractului. Factorul de evaluare este experienta profesionala a personalului ofertantului concretizata in numarul de proiecte in care personalul a indeplinit acelasi tip activitati ca cele pe care urmeaza sa le indeplineasca in viitorul contract.

Numar maxim de puncte: 15.

Acordarea punctajului „Experiența profesionala a personalului” se va face in felul urmator:

Expert cheie	Numar maxim de puncte
Manager de proiect	2
Arhitect solutie	1
Coordonator analiza	2
Expert integrare	1
Expert baza de date	1
Coordonator dezvoltare software	2
Coordonator testare	2
Expert infrastructura/virtualizare	1
Expert testare de securitate	1
Expert securitatea informatiei	1

Expert instruire	1
Total	15

Punctajul aferent experienței persoanelor propuse ca experți-cheie pentru pozițiile Arhitect soluție, Coordonator analiza, Expert integrare, Expert baza de date, Coordonator dezvoltare software, Coordonator testare, Expert infrastructura/virtualizare și Expert securitatea informației se va acorda pentru fiecare în parte, astfel:

a) pentru experiența constând în implicarea între 2 și 4 proiecte sau contracte dezvoltare/ implementare/ extindere sistem informatic în care a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract a persoanei propuse se acordă 1/4 din punctajul maxim alocat poziției respective în caietul de sarcini;

b) pentru experiența constând în implicarea între 5 și 7 proiecte sau contracte dezvoltare/ implementare/ extindere sistem informatic în care a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract a persoanei propuse se acordă 1/2 din punctajul maxim alocat poziției respective în caietul de sarcini;

c) pentru experiența constând în implicarea în minim 8 proiecte sau contracte dezvoltare/ implementare/ extindere sistem informatic în care a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract a persoanei propuse se acordă punctajul maxim alocat poziției respective în caietul de sarcini;

Punctajul aferent experienței persoanei propuse pentru pozițiile de Manager de proiect, Expert testare de securitate și Expert instruire se va acorda astfel:

- pentru experiența constând în implicarea între 2 și 4 proiecte în care a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract a persoanei propuse se acordă 1/4 din punctajul maxim alocat poziției respective în caietul de sarcini;
- pentru experiența constând în implicarea între 5 și 7 proiecte în care a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract a persoanei propuse se acordă 1/2 din punctajul maxim alocat poziției respective în caietul de sarcini;
- pentru experiența constând în implicarea în minim 8 proiecte în care a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract a persoanei propuse se acordă punctajul maxim alocat poziției respective în caietul de sarcini;

Nu se accepta persoane propuse pe poziții de experți fara nici un fel de experiență, respectiv fara demonstrarea implicării în cel puțin un proiect sau contract în care a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract.

Nu va fi punctată experiența profesională a unor persoane propuse pe poziții de experți suplimentare față de cele menționate în tabelul de mai sus, chiar dacă acestea îndeplinesc cerințele minime și dovedesc experiență similară așa cum este descrisă în acest caiet de sarcini.

Pentru demonstrarea experienței profesionale solicitate, Ofertantii trebuie să prezinte în cadrul ofertei tehnice documente relevante cum ar fi: recomandări emise de beneficiarul final al proiectului, semnate sau contrasemnate de către Autoritatea Contractantă/beneficiarul privat în calitate de beneficiar final al

proiectului sau alte documente edificatoare semnate de acesta. Pentru fiecare document propus, se va prezenta o persoana de contact din partea beneficiarului final al proiectului (nume, pozitie, adresa de mail, numar de telefon), in masura sa confirme cele prezentate in recomandari (sau alte documente). In urma verificarii exactitatii informațiilor și a dovezilor furnizate de catre ofertanți, Autoritatea Contractantă poate solicita și alte documente/informații care să clarifice experiența profesionala solicitata. De asemenea, Autoritatea Contractantă isi rezerva dreptul de a contacta beneficiarii finali ai proiectelor prezentate la experienta profesionala, in vederea confirmarii celor prezentate de catre ofertanti. Punctajul va fi acordat numai pentru proiectele sau contractele pentru care documentele prezentate dovedesc experienta solicitata pentru fiecare persoana propusa pentru o anumita pozitie de expert.

7.4 Descrierea modalitatii de punctare a factorului de evaluare "Propunerea tehnică - Demonstrarea unei metodologii adecvate de implementare a contractului"

Prin acest criteriu se va realiza evaluarea masurii in care ofertantii inteleg specificul proiectului si a maturitatii metodologiei de implementare propuse de acestia (a proceselor si procedurilor specifice).
Numar maxim de puncte: 5 puncte.

Acordare punctajului „Demonstrarea unei metodologii adecvate de implementare a contractului” se va face in felul urmator:

Element evaluat	Calificativ	Punctaj
Abordarea propusă se bazează în mare măsură pe o serie de metodologii, metode și/sau instrumente testate anterior de ofertant, recunoscute la nivel national / international și care demonstrează o foarte bună înțelegere a contextului, respectiv a particularității sarcinilor stabilite în caietul de sarcini, în corelație cu aspectele-cheie, precum și cu riscurile și ipotezele identificate	Foarte bine	5
Abordarea propusă se bazează parțial pe metodologii, metode și/sau instrumente testate anterior de ofertant, recunoscute la nivel national / international și care demonstrează parțial înțelegerea contextului, respectiv a particularității sarcinilor stabilite în caietul de sarcini, în corelație cu aspectele-cheie, precum și cu riscurile și ipotezele identificate.	Bine	3
Abordarea propusă nu are la bază metodologii, metode și/sau instrumente testate anterior de ofertant, recunoscute la nivel national/international și arată o înțelegere limitată a contextului, respectiv a particularității sarcinilor stabilite în caietul de sarcini.	Acceptabil	1

Ofertantul va prezenta organizarea și metodologia pentru realizarea sistemului informatic conform Anexa 5 – Formular propunere tehnică.

8 Cerinte pentru sesiunea demonstrativa

Avand in vedere complexitatea sistemului ce trebuie implementat si importanta respectarii termenului de implementare mentionat in prezentul document, asumat si prin contractul de finantare, Autoritatea Contractanta va solicita ofertantilor prezentarea capabilitatii solutiei tehnice propuse in cadrul unei sesiuni

demonstrative, demonstrand modalitatea in care produsele software incluse in solutia tehnica propusa raspund nativ, fara a fi necesare dezvoltari suplimentare, la unele cerinte minime din caietul de sarcini si la functionalitatile suplimentare ce vor fi punctate de autoritatea contractanta in cadrul factorului de evaluare „Propunere tehnica – Capabilitati solutie tehnica”.

Astfel, in timpul sesiunii demonstrative vor fi prezentate urmatoarele capabilitati ale solutiei oferite:

1. Va fi prezentata interfata web de management pentru componenta de gestiune a documentelor, evidentiind urmatoarele functionalitati disponibile in platforma:
 - a. Permite definirea securitatii (drepturilor de acces) pentru roluri, foldere si documente.
 - b. Permite incarcarea de documente in depozitul de documente cel putin prin urmatoarele modalitati:
 - i. drag & drop, bulk upload, copy & paste in windows explorer,
 - ii. monitorizare casuta de email si incarcare directa in depozitul de documente a tuturor fisierelor atasate care se trimit la acea casuta de email, fara nici o interventie umana
 - c. Permite utilizatorilor adaugarea de medatate speciale in afara de cele standard ale tipului de document, metadata valabile doar pe acea instanta de document;
 - d. Permite conversia automată a documentelor de tip MS Office sau OpenOffice în formate web (HTML, PDF), pentru o publicare facilă a acestora;
 - e. Va permite crearea automata de structuri de foldere in functie de valori ale metadatelor documentelor;
2. Vor fi prezentate urmatoarele functionalitati cheie ale componentei de dezvoltare aplicatii mobile:
 - a. Sa permita scrierea de aplicatii o data si sa poata rula pe oricare din dispozitivele mobile importante (iOS, Android, Windows).
 - b. Sa foloseasca tehnologii web (HTML, CSS, Javascript) in procesul de dezvoltare aplicatii mobile
 - c. Sa asigure acces la functionalitati importante din sistemul de operare in care aplicatia va rula precum: baterie, camera si localizare
3. Vor fi prezentate urmatoarele functionalitati cheie ale componentei de testare performanta:
 - a. permite adaugarea/eliminarea de utilizatori virtuali in timpul executiei testelor;
 - b. permite monitorizarea fara agenti;
 - c. permite rularea de teste de incarcare la nivelul API (SOAP, REST), la nivelul componentelor sau la nivelul microservicilor;
 - d. permite analiza performantei sistemului dupa rularea unui test pe baza datelor colectate din straturile arhitecturale relevante;
 - e. permite rularea de rapoarte de analiza a performantei pe diferite nivele de detaliu (de tip sumar sau la nivel de tranzactie) si rapoarte pentru determinarea incadrarii performantei intr-un SLA predefinit

- f. permite localizarea, extragerea și înlocuirea valorilor dinamice din cadrul paginilor web precum id-ul de sesiune, authentication token, customer id, etc asigurând astfel acceptarea cererilor de către serverele web supuse testării
4. Vor fi prezentate următoarele funcționalități cheie ale componentei de testare automată
 - a. permite convertirea facilă în script-uri a testelor înregistrate în interfața grafică utilizator;
 - b. permite folosirea unui limbaj de programare standard (Javascript, Vbscript, Jscript, Python) pentru crearea de teste pe interfața utilizator sau îmbunătățirea înregistrărilor testelor existente;
 - c. permite automatizarea testării funcționale pentru multiple tehnologii desktop (de exemplu Windows / Java / .NET / Oracle Forms);
 - d. permite separarea datelor de comenzi de test și modificarea datelor de intrare pentru lărgirea ariei de testare;
 - e. permite rularea de teste de tip cross-browser;
 5. Vor fi prezentate toate funcționalitățile pentru care ofertantul consideră că propunerea tehnică trebuie punctată în cadrul factorului de evaluare "Propunere tehnică – Capabilități soluție tehnică" cu excepția funcționalităților aferente componentelor din categoria infrastructura de securitate și anume: componenta de redistribuire a accesului la servicii, componenta de protecție avansată anti-malware, componenta de protecție a resurselor la nivel de post de lucru și componenta de management a datelor de audit. Funcționalitățile aferente componentelor din categoria infrastructura de securitate vor fi validate în etapa de evaluare tehnică a ofertelor doar pe baza documentelor justificative prezentate ca parte a ofertei tehnice (documentații tehnice, datasheet-uri, screenshot-uri ale interfețelor aplicațiilor, etc), urmând ca Ofertantul câștigător să le prezinte practic Autorității Contractante în perioada de implementare a proiectului, în urma instalării acestora pe mediile Autorității Contractante (test sau productiv).

Prezentarea capabilităților soluției propuse în cadrul sesiunii demonstrative se va baza pe prezentarea practică a produselor software oferite (de ex. a interfețelor expuse de acestea, a fișierelor de configurare ale acestora, etc) în cadrul unor medii demonstrative și nu doar pe descrieri ale producătorilor (de ex. datasheet-uri, manuale de administrare, alte documentații tehnice).

În cazul în care un Ofertant nu poate demonstra în cadrul sesiunii demonstrative îndeplinirea unei cerințe minime din caietul de sarcini, va duce la respingerea ofertei acestuia ca neconformă.

În cazul în care un Ofertant nu poate demonstra în cadrul sesiunii demonstrative funcționalitățile declarate ca fiind disponibile out-of-the-box în cadrul soluției pentru a fi punctate în cadrul factorului de evaluare "Propunere tehnică – Capabilități soluție tehnică", funcționalități ce intră în scopul declarat al sesiunii demonstrative, Autoritatea Contractantă va acorda punctajul minim (0 puncte) pentru funcționalitățile respective chiar dacă în oferta tehnică au fost prezentate ca fiind incluse în soluție.

Personalul nominalizat de către Ofertanți pentru participare la sesiunea demonstrativă va fi desemnat din echipa propusă în propunerea tehnică pentru implementarea proiectului.

Sesiunea demonstrativa va fi sustinuta de catre fiecare Ofertant la sediul Autoritatii Contractante in urma invitatiei de participare din partea acesteia.

Cu minim 2 zile lucratoare inainte de data planificata pentru sesiunea demonstrativa, Ofertantul are obligatia sa transmita Autoritatii Contractante lista participantilor la sesiunea demonstrativa in care se mentioneaza rolul in timpul sesiunii si relatia pe care acestia o au cu Ofertantul – participantii vor fi dintre cei expertii propusi in oferta tehnica. Autoritatea Contractanta nu va accepta in sesiunea demonstrativa decat persoanele nominalizate de ofertant in lista participantilor si care figureaza in lista de experti cheie mentionati in oferta depusa.

Ofertantul va pune la dispozitia expertilor sai resursele necesare (de ex. laptop-uri, modem-uri de date, servere pentru sustinerea demonstratiei, etc) pentru derularea in bune conditii a sesiunii demonstrative.

Pe durata sesiunii demonstrative, Autoritatea Contractanta va solicita realizarea de screenshot-uri cu interfetele aplicatiilor utilizate in demonstrarea fiecărei functionalitati ce intra in scopul sesiunii demonstrative. Aceste screenshot-uri vor fi incluse in anexa procesului verbal aferent sesiunii demonstrative ce va fi incheiat de catre Autoritatea Contractanta si Ofertant la finalul sesiunii demonstrative.

Refuzul de a semna procesul verbal aferent sesiunii demonstrative, consemnandu-se astfel in scris rezultatele obtinute in cadrul sesiunii demonstrative, va duce la respingerea ofertei ca neconforma.

9 Drepturi de proprietate intelectuală

Orice documente sau materiale elaborate ori compilate de către executant sau de către personalul său salariat ori contractat în executarea prezentului contract, vor deveni proprietatea exclusivă a achizitorului. După încetarea prezentului contract, executantul nu va păstra copii ale documentelor și/sau materialelor realizate și nu le va utiliza 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 lucrari în cursul executării altor lucrari pentru terți și nu va divulga nicio informație 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 așa cum va considera de cuviință, fără limitare geografică ori de altă natură, cu excepția situațiilor în care există deja asemenea drepturi de proprietate intelectuală ori industrială.

10 Modalitatea de înlocuire a personalului de specialitate nominalizat pentru îndeplinirea contractului.

1. Prestatorul se obligă să pună la dispoziție numărul de experți necesari în realizarea contractului.
2. În cazul în care pe parcursul derulării contractului apar situații care impun înlocuirea unui membru din echipa de proiect atunci această înlocuire trebuie notificată și aprobată de achizitor, prin act adițional.
3. Prestatorul poate să propună din proprie inițiativă înlocuirea unui membru al personalului – expert cheie, numai în următoarele condiții:
 - a) în cazul decesului, în cazul îmbolnăvirii sau în cazul accidentării unui membru al personalului
 - b) dacă se impune înlocuirea unui membru al personalului pentru orice alt motiv care nu este sub controlul prestatorului (ex. demisia, etc.)
4. Înlocuirea personalului de specialitate nominalizat pentru îndeplinirea contractului se realizează numai cu acceptul autorității contractante, și nu reprezintă o modificare substanțială, așa cum este aceasta definită în art. 221 din Lege, decât în următoarele situații:
 - a) noul personal de specialitate nominalizat pentru îndeplinirea contractului nu îndeplinește cel puțin cerințele din cadrul documentației de atribuire;
 - b) noul personal de specialitate nominalizat pentru îndeplinirea contractului nu obține cel puțin același punctaj ca personalul propus la momentul aplicării factorilor de evaluare.
5. Contractantul are obligația de a transmite pentru noul personal documentele solicitate prin documentația de atribuire fie în vederea demonstrării îndeplinirii cerințelor, fie în vederea calculării punctajului aferent factorilor de evaluare.
6. Achizitorul nu va purta nicio răspundere față de eventualele pretenții ale persoanei înlocuite, singurul responsabil de legalitatea înlocuirii fiind prestatorul. Costurile suplimentare generate de înlocuirea personalului revin în mod obligatoriu prestatorului.

11 Modalitatea de plată

Plata se va efectua în 3 tranșe, după cum urmează:

- Prima tranșă reprezentând 60% din valoarea aferentă livrării, instalării și configurării infrastructurii hardware și software prevăzută la alin. (1) lit. a) se va efectua după aprobarea raportului de progres intermediar care va avea ca anexă procesele-verbale de recepție cantitativă și calitativă care atestă livrarea, instalarea și configurarea infrastructurii hardware și livrarea, instalarea și configurarea infrastructurii software de bază.
- A doua tranșă reprezentând 40% din valoarea aferentă serviciilor de analiză, proiectare, dezvoltare și testare software prevăzută la alin. (1) lit. b) se va efectua după aprobarea raportului de progres intermediar care va avea ca anexă procesele-verbale de recepție cantitativă și calitativă a serviciilor de analiză, proiectare dezvoltare, testare software

- A treia tranșă însumând 40 % din valoarea aferentă livrării, instalării și configurării infrastructurii hardware și software prevăzută la alin. (1) lit. a) și 60 % din valoarea aferentă serviciilor de analiză, proiectare, dezvoltare și testare software prevăzută la alin. (1) lit. b) se va efectua după aprobarea raportului final care va avea ca anexă procesul-verbal de acceptanță finală a tuturor activităților proiectului și punerea în funcțiune a întregului sistem informatic, inclusiv plata în procent de 100% pentru serviciile de instruire/cursare utilizatorilor/administratorilor.

Plățile se vor face numai după aprobarea rapoartelor/semnarea proceselor-verbale de livrare și punere în funcțiune a produselor/serviciilor, însoțite de rapoartele financiare aferente/livrabile/fișe tehnice/licențe/certificate de garanție, etc..

Facturile vor fi emise numai după aprobarea rapoartelor/semnarea proceselor verbale de livrare și punere în funcțiune a produselor/serviciilor.

Plata facturilor emise de prestator se efectuează în termen de 30 de zile de la înregistrarea acestora la beneficiar, însoțite de documentele justificative aprobate de beneficiar.

Documentele care necesită a fi aprobate de beneficiar, în vederea efectuării plăților în funcție de etapele de implementare, sunt:

1. **Raport de progres intermediar nr. 1** care va cuprinde descrierea etapelor de recepție cantitativă și calitativă a produselor livrate, instalare și configurare infrastructură hardware și livrare, instalare și configurare infrastructură software de bază, care include și raport financiar. Acesta va fi transmis oficial în termen de 10 zile de la sfârșitul perioadei de raportare, aceasta fiind de maxim 8 luni de la data semnării contractului.
2. **Raport de progres intermediar nr. 2** care va cuprinde descrierea etapelor de recepție cantitativă și calitativă a serviciilor de analiză, proiectare, dezvoltare și testare software aplicativ, care include și raport financiar. Acesta va fi transmis oficial în termen de 10 zile de la sfârșitul perioadei de raportare, aceasta fiind de 15 luni de la data semnării contractului.
3. **Raport final** - document elaborat de prestator la finalul contractului care va descrie modul în care s-a desfășurat implementarea contractului din punct de vedere tehnic/financiar, inclusiv acceptanța finală prin care se vor recepționa toate activitățile proiectului și punerea în funcțiune a întregului sistem informatic, inclusiv instruirea utilizatorilor/administratorilor.

Aprobarea documentelor sau notificarea cu privire la neconformitățile identificate de beneficiar se va efectua în maxim 10 zile lucratoare de la primirea acestora. Prestatorul va revizui și retransmite documentele în maxim 5 zile lucratoare de la notificare.

Plățile pentru serviciile efectuate/bunurile livrate se vor efectua cu încadrarea în creditele bugetare aprobate.

Executarea contractului nu trebuie să genereze alte servicii/produse decât cele cuprinse în contract și/sau cheltuieli comerciale neuzuale în afara celor înscrise în bugetul contractului și menționate în caietul de sarcini. Dacă totuși apar astfel de cheltuieli, achizitorul nu va fi răspunzător și nu va suporta cheltuielile comerciale în afara celor înscrise în bugetul contractului.

12 Informatii finale

În situația în care comisia de evaluare constată că elemente de preț ale unei oferte sunt aparent neobișnuit de scăzute, prin raportare la prețurile pieței, comisia de evaluare va solicita ofertantului care a depus oferta în cauză explicații cu privire la posibilitate îndeplinirii contractului în condițiile de calitate impuse prin documentația de atribuire. Explicațiile aduse de ofertant vor fi însoțite de dovezi concludente privind elementele prevăzute la art. 210 alin. (2) din Legea 98/ 2016, precum și, după caz, documente privind prețurile ce pot fi obținute de la furnizori, modul de organizare și metodele utilizate în cadrul procesului de lucru, nivelul de salarizare al personalului ofertantului, performanțele și costurile implicate de anumite utilaje sau echipamente de lucru.

În cazul în care ofertantul nu prezintă comisiei de evaluare informațiile și/sau documentele solicitate sau acestea nu justifică în mod corespunzător nivelul scăzut al prețului sau al costurilor propuse, oferta va fi considerată inacceptabilă.

Ofertanții trebuie să întocmească propunerea tehnică și financiară cu respectarea prevederilor stabilite în cadrul prezentului caiet de sarcini.

Ofertantul trebuie să răspundă punctual la toate cerințele cuprinse în prezentul caiet de sarcini și să detalieze în cadrul propunerii tehnice metodologia de lucru și mijloacele concrete prin care sistemul informatic ofertat îndeplinește aceste cerințe, planul de lucru, personalul utilizat și organizarea acestuia, astfel încât comisia de evaluare să aibă posibilitatea evaluării acestuia în mod obiectiv.

Simpla copiere a conținutului caietului de sarcini în Propunerea Tehnică nu reprezintă îndeplinirea cerințelor de conformitate anterior enunțate.

Propunerea tehnică se va întocmi într-o manieră organizată, astfel încât procesul de evaluare a ofertelor să permită identificarea facilă a corespondenței informațiilor cuprinse în ofertă cu specificațiile tehnice din prezentul caiet de sarcini. Oferta tehnică trebuie să fie prezentată și într-un format editabil care să permită selectarea textului, copierea acestuia, precum și cu toate referințele (link-urile) către site-uri în format hyperlink, „gata de click” (în acest sens solicităm prezentarea ofertei tehnice și în format Microsoft Word sau într-un format care să permită copierea textului către Microsoft Word cu pastrarea formatarei acestuia).

Ofertanții au obligativitatea prezentării pentru fiecare dintre membrii personalului care va face parte din echipa de proiect, conform poziției de expert pe care este alocat, toate documentele necesare evaluării, în mod ordonat, pentru a facilita procesul de evaluare.

Omisinea sau neîndeplinirea corespunzătoare a oricărei dintre cerințele prezentului caiet de sarcini va duce la respingerea ofertei ca neconformă. De asemenea, un simplu răspuns (afirmație) de confirmare din partea operatorului economic cu privire la respectarea cerințelor din caietul de sarcini, fără precizarea exactă a modalității de îndeplinire, va conduce la respingerea ofertei. În acest sens se solicită din partea

ofertantilor și intră în răspunderea acestora prezentarea dovezilor concrete în sprijinul oricăror afirmații care se pot încadra în categoria exemplului anterior menționat.

Toate livrabilele furnizate în cadrul proiectului de către Prestator vor fi în limba română.

Specificatiile tehnice definite în cadrul prezentului caiet de sarcini corespund necesitatilor și exigentelor autorității contractante. Având în vedere specificitatea acestui proiect, Autoritatea Contractantă a descris sistemul informatic ce va fi achiziționat la nivelul de detaliu necesar operatorilor economici interesați, permițând identificarea obiectului acestui contract de achiziție publică.

Orice referire la producători / mărci comerciale / denumiri de produse sau părți componente / tipuri / standarde / procedee / tehnologii / proceduri / producții și elemente specifice / origini / certificări prezentate în caietul de sarcini sunt menționate doar pentru identificarea cu ușurință a tipului de produs și vor fi considerate ca purtând mențiunea "**sau echivalent**", chiar dacă nu este efectiv precizată în cadrul respectivei cerințe.

AUTORITATEA CONTRACTANTĂ



Proiect cofinanțat din Fondul Social European prin
Programul Operațional Capacitate Administrativă 2014-2020!

Anexa 1 - Lista locațiilor semnificative la nivelul proiectului – ONRC, ORCT București și ale ORCT Brașov

Lista locațiilor – ONRC și ale ORCT semnificative la nivelul proiectului, reprezentanți autorizați din partea ONRC

Nr. crt.	Locație	Adresă	Telefon fix, mobil	Fax	E-mail	Persoane de contact personal tehnic
1.	Oficiul Național al Registrului Comerțului (ONRC)	București, Unirii nr. 74, sector 3	Bd. 021-316.08.04	021-316.08.03	onrc@onrc.ro	Stefan CRETIOIU 021-316.08.17/123 E-mail: stefan.cretioiu@onrc.ro Dan TĂNASE 021-316.08.17/123 Mobil: 0752 011 492 E-mail: dan.tanase@onrc.ro
2.	Oficiul Registrului Comerțului de pe lângă Tribunalul (ORCT) BUCUREȘTI	București, Intrarea de Sectorului nr. 1, pe lângă sector 3	021-316.08.28	021-316.08.23 021-316.08.25	orcb@b.onrc.ro	Maria Tănase maria.tanase@b.onrc.ro 0752-011469 Adrian Cărășel adrian.carasel@b.onrc.ro 0756-067 145
3.	ORC de pe lângă Tribunalul BRAȘOV	Brașov, str. Zizinului, nr. 106A	0268-311.992, 0268-319.027	0268-318.616	orcbv@bv.onrc.ro	Rodica Tatiana TOMA – Director orcbv@bv.onrc.ro , 0752-011 328 Florin Razvan Lupsa Tataru florin.lupsa@bv.onrc.ro , 0752-011 330

Anexa 2 – Indicatori de performanta pentru realizarea activitatilor din contract

[Handwritten signatures]

Indicator de performanță	Referința în Contract / Caiet de Sarcini -	Nivelul de performanță așteptat (conform Contract / Caiet de Sarcini)	Ce se măsoară	Modalitate de evaluare	Scop
Documentie de analiza adecvata pentru scopul utilizării	Error! Reference source not found. Error! Reference source not found. Document analiza de business	Documentația de analiza este livrată conform cerințelor stabilite în Caietul de Sarcini	Nivelul de acuratețe al documentației livrate după "peer review" (pondere informații inexacte /	Foarte satisfăcător (5 puncte) – Documentația livrată include îmbunătățiri semnificative față de cerințele minime stabilite în Caietul de Sarcini în special prin luarea în considerare a noilor tendințe din industrie și respectarea aspectelor de mediu și sociale. Documentația a fost folosită pentru realizarea achiziției și pentru construcția cum a fost prezentată. Satisfăcător (4 puncte) – Documentația livrată include unele îmbunătățiri și nu include	Evaluarea aplicabilității și relevanței documentației de analiza



Indicator de performanță	Referința în Contract / Caiet de Sarcini -	Nivelul de performanță așteptat (conform Contract / Caiet de Sarcini)	Ce se măsoară	Modalitate de evaluare	Scop
			sub nivelul de calitate agreat în informațiile furnizate)	<p>neconformități/inexacități față de nivelul agreat. Documentația a fost folosită pentru realizarea achiziției și pentru construcția cum a fost prezentată. Au fost necesare doar ajustări nemateriale.</p> <p>Acceptabil (3 puncte) - Documentația livrată nu include neconformități/inexacități față de nivelul agreat însă nu include nici elemente suplimentare care să aducă o valoare adăugată semnificativă proiectului sau nu a fost acordată o atenție specială aspectelor de mediu sau sociale.</p> <p>Documentația a putut fi folosită pentru realizarea achiziției și/sau construcției după ce a fost corectată de câteva ori de Consultant.</p>	

Handwritten signature



Indicator de performanță	Referința în Contract / Caiet de Sarcini -	Nivelul de performanță așteptat (conform Contract / Caiet de Sarcini)	Ce se măsoară	Modalitate de evaluare	Scop
				<p>Nu au existat întârzieri semnificative ca urmare a corecturilor.</p> <p>Nesatisfăcător (2 puncte) - Documentația transmisă a inclus neconformități / inexactități față de nivelul agreat sau a folosit tehnologii/metode complet învechite care erau în principal abandonate de industrie, iar aceste aspecte nu au putut fi corectate în totalitate într-o perioadă rezonabilă (ex. au cauzat întârzieri semnificative în realizarea activităților din calendarul general al proiectului), dar cu toate acestea au fost corectate de către Consultant, fără costuri suplimentare pentru Autoritatea Contractantă.</p> <p>Foarte nesatisfăcător (1 punct) – Documentația livrată a inclus neconformități / inexactități majore față</p>	



[Handwritten signatures]

Indicator de performanță	Referința în Contract / Caiet de Sarcini -	Nivelul de performanță așteptat (conform Contract / Caiet de Sarcini)	Ce se măsoară	Modalitate de evaluare	Scop
Documentie de proiectare adecvata pentru scopul utilizării	Error! Reference source not found. - Document proiectare detaliata	Documentația de proiectare este livrată conform cerințelor	Nivelul de acuratețe al documentației livrate după "peer	de nivelul agreat sau a folosit tehnologii/metode complet învechite care erau, în principal, abandonate de industrie, iar aceste aspecte nu au putut fi corectate de către Consultant. Autoritatea Contractantă a trebuit să mobilizeze alte resurse pentru a remedia problemele, ceea ce a condus la costuri suplimentare semnificative pentru Autoritatea Contractantă și/sau a cauzat întâzieri semnificative în realizarea activităților din calendarul general al proiectului.	Evaluarea aplicabilității și relevanței documentației de proiectare
				Foarte satisfăcător (5 puncte) – Documentația livrată include îmbunătățiri semnificative față de cerințele minime stabilite în Caietul de Sarcini în special prin luarea în considerare a noilor tendințe din industrie și respectarea aspectelor de mediu și sociale.	



Handwritten signatures and initials at the bottom of the page.

Indicator de performanță	Referința în Contract / Caiet de Sarcini -	Nivelul de performanță așteptat (conform Contract / Caiet de Sarcini)	Ce se măsoară	Modalitate de evaluare	Scop
		stabilite în Caietul de Sarcini	review" (pondere informații inexacte / sub nivelul de calitate agreat în informațiile furnizate)	<p>Documentația a fost folosită pentru realizarea achiziției și pentru construcția cum a fost prezentată.</p> <p>Satisfăcător (4 puncte) – Documentația livrată include unele îmbunătățiri și nu include neconformități/inexactități față de nivelul agreat.</p> <p>Documentația a fost folosită pentru realizarea achiziției și pentru construcția cum a fost prezentată. Au fost necesare doar ajustări nemateriale.</p> <p>Acceptabil (3 puncte) - Documentația livrată nu include neconformități/inexactități față de nivelul agreat însă nu include nici elemente suplimentare care să aducă o valoare adăugată semnificativ proiectului sau nu a fost acordată o atenție specială aspectelor de mediu sau sociale.</p>	

[Handwritten signatures]



Indicator de performanță	Referința în Contract / Caiet de Sarcini -	Nivelul de performanță așteptat (conform Contract / Caiet de Sarcini)	Ce se măsoară	Modalitate de evaluare	Scop
				<p>Documentația a putut fi folosită pentru realizarea achiziției și/sau construcției după ce a fost corectată de câteva ori de Consultant.</p> <p>Nu au existat întâzieri semnificative ca urmare a corecturilor.</p> <p>Nesatisfăcător (2 puncte) - Documentația transmisă a inclus neconformități / inexactități față de nivelul agreat sau a folosit tehnologii/metode complet învechite care erau în principal abandonate de industrie, iar aceste aspecte nu au putut fi corectate în totalitate într-o perioadă rezonabilă (ex. au cauzat întâzieri semnificative în realizarea activităților din calendarul general al proiectului), dar cu toate acestea</p>	

[Handwritten signatures]



Indicator de performanță	Referința în Contract / Caiet de Sarcini -	Nivelul de performanță așteptat (conform Contract / Caiet de Sarcini)	Ce se măsoară	Modalitate de evaluare	Scop
				<p>au fost corectate de către Consultant, fără costuri suplimentare pentru Autoritatea Contractantă.</p> <p>Foarte nesatisfăcător (1 punct) – Documentația livrată a inclus neconformități / inexactități majore față de nivelul agreat sau a folosit tehnologii/metode complet învechite care erau, în principal, abandonate de industrie, iar aceste aspecte nu au putut fi corectate de către Consultant. Autoritatea Contractantă a trebuit să mobilizeze alte resurse pentru a remedia problemele, ceea ce a condus la costuri suplimentare semnificative pentru Autoritatea Contractantă și/sau a cauzat întâzieri semnificative în realizarea activităților din calendarul general al proiectului.</p>	

Be Anis De S de An

Indicator de performanță	Referința în Contract / Caiet de Sarcini -	Nivelul de performanță așteptat (conform Contract / Caiet de Sarcini)	Ce se măsoară	Modalitate de evaluare	Scop
Livrabil final în termenul agreat	Error! Reference source not found. Error! Reference source not found.	Sistemul informatic a fost pus în funcțiune conform termenului în contract	Livrarea la timp a rezultatelor	Foarte satisfăcător (5 puncte) – livrate în termenele convenite în contract, Satisfăcător (4 puncte) – livrate imediat după încheierea termenelor convenite în Contract însă fără întârzierea activităților din calendarul general al proiectului Acceptabil (3 puncte) – livrate după încheierea termenelor convenite în Contract conducând la întârzieri ale activităților din calendarul general al proiectului ce pot fi neglijate. Nesatisfăcător (2 puncte) – livrate cu mult după încheierea termenelor convenite în Contract conducând la întârzieri ale activităților din calendarul general al proiectului, ex. mai mult de 60 de zile.	Evaluarea finalizării la timp punerii în funcțiune a sistemului informatic

[Handwritten signatures]

Indicator de performanță	Referința în Contract / Caiet de Sarcini -	Nivelul de performanță așteptat (conform Contract / Caiet de Sarcini)	Ce se măsoară	Modalitate de evaluare	Scop
				<p>Foarte nesatisfăcător (1 puncte) – livrate cu mult după încheierea termenelor convenite în Contract conducând la întârzieri majore ale activităților din calendarul general al proiectului, ex. mai mult de 120 de zile</p>	

[Handwritten signature]

