COMPANIA NAȚIONALĂ DE CĂI FERATE „CFR" S.A.
Registrul Comerțului J1998009774402, CUI: RO 11054529
Bd. Dinicu Golescu nr.38, sector 1, București, România
www.cfr.ro; e-mail: OfficeCFR@cfr.ro; cod poștal: 010873
Tel.:021 319 24 00; Fax: 021 319 24 01; Tel CFR: 122001

DIRECȚIA TEHNICĂ
Serviciul Tehnic
Nr. 8/1/1482/ 04 . 11 .2025

APROBAT
Director General Adj. Tehnic
Valentin DOROBANȚU

CAIET DE SARCINI

privind achiziționarea serviciilor de audit informatic (conformitate NIS) pentru asigurarea unui nivel ridicat de securitate a rețelelor și a sistemelor informatice

1. INTRODUCERE

Prezentul caiet de sarcini conține specificații tehnice și face parte integrantă din documentația de atribuire în vederea achiziției serviciilor de audit informatic (conformitate NIS) și cuprinde ansamblul cerințelor minime și obligatorii de îndeplinit pe baza cărora fiecare ofertant elaborează propunerea tehnică și financiară.

În cadrul acestei proceduri, Compania Națională de Căi Ferate „CFR"-S.A., cu sediul în București, bd. Dinicu Golescu nr. 38, sector 1, CUI RO 11054529, îndeplinește rolul de Entitate Contractantă, respectiv Achizitor în cadrul Contractului.

2. CONTEXTUL REALIZĂRII ACHIZIȚIEI

2.1. INFORMAȚII DESPRE ENTITATEA CONTRACTANTĂ

Compania Națională de Căi Ferate Române „CFR" S.A., denumită în continuare CFR, a fost înființată la 1 octombrie 1998, prin Hotărârea Guvernului nr. 581/1998 privind înființarea Companiei Naționale de Căi Ferate "C.F.R." - S.A. prin reorganizarea Societății Naționale a Căilor Ferate Române. Potrivit acestei hotărâri, activitățile CFR sunt de interes public național, în vederea realizării nevoilor de transport feroviar public și de apărare ale României.

CFR desfășoară activități de interes public național în scopul realizării transportului feroviar public și al satisfacerii nevoilor de apărare a țării și are, în principal, ca obiect de activitate:

a) gestionarea infrastructurii feroviare și punerea acesteia la dispoziție operatorilor de transport feroviar, în condițiile legii;
b) dezvoltarea și modernizarea infrastructurii feroviare din România în concordanță cu standardele europene, în scopul asigurării compatibilității și interoperabilității cu sistemul de transport feroviar european;
c) organizarea, planificarea, coordonarea și controlul activităților de administrare, exploatare, întreținere și reparare a infrastructurii feroviare;
d) desfășurarea activităților industriale și de servicii conexe pentru asigurarea funcționarii infrastructurii feroviare;
e) gestionarea patrimoniului auxiliar feroviar.

2.2. CONTEXTUL REALIZĂRII ACHIZIȚIEI

Achiziția este necesară ca urmare a aprobării Ordonanței de Urgență nr. 155/2024 *privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil,* se adresează organizațiilor din domeniul public și privat din anumite sectoare de activitate, cum ar fi: energie, transport, sector bancar, infrastructuri ale pieței financiare, sănătate, furnizarea și distribuirea de apă potabilă, care prestează servicii considerate a fi esențiale.

CNCF „CFR" - SA este înscrisă ca Operator de servicii esențiale în Registrul Operatorilor de Servicii Esențiale (ROSE) din luna iunie 2021, pentru sectorul /subsectorul Transport/Transport feroviar (conform Deciziei 5620/II/A/ din 23.06.2021 emisă de Centrul Național de Răspuns la Incidente de Securitate Cibernetică – CERT RO).

La momentul actual, pentru respectarea prevederilor OUG nr. 155/2024, s-au întreprins demersurile necesare, către Directoratul Național de Securitate Cibernetică, pentru înregistrarea companiei în Registrul entităților esențiale și importante.

Potrivit legislației în vigoare, în urma analizei preliminare a sistemelor și a infrastructurilor informatice ale societății au fost identificate în categoria serviciilor esențiale, următoarele sisteme:

- *Controlul și gestionarea traficului feroviar (supravegherea și reglementarea traficului, semnalizarea; planificarea traficului, gestionarea traseului trenurilor) – E11;*

➢ **Sistem informatic "Circulație trenuri"** cu componentele: IRIS – ATLAS – IM, IRIS – CRONOS, IRIS – FOCUS, IRIS – FOCUS – RU, IRIS – CALIPSO, IRIS – INFO – IM, E – TELEX INFOKIOSK, CRONOS VOX, TraficAlert, Hărți DRR, Editare Hărți transparență, Regim de performanță, Accepte Programare, IMComm, Polifem Constanța, Tarife pentru servicii adiționale (T.S.A.), WIMO-IM, Căi Libere.

- *Întreținerea infrastructurii feroviare – E 24;*

➢ **Sistem informatic "Infrastructură feroviară"** cu componentele: IRIS – IMA (MP5i), IRIS – IMA (Harta GIS CFR), Web – INSPIRE, IRIS – IMA (WebSCB), IRIS – IMA (WebSIMC), IRIS – IMA (WebSafety), WebEMM, ENTRAC, Program Cadru Anual IT / ITP, AVI–GABARITE, e–RINF, RegistruActive,

➢ **Sistem informatic IT "Gestiune stocuri și imobilizări corporale" cu următoarele componente: e–MPS, e–SIGMA, eMiFixe;**

- *Întreținerea materialului rulant (locomotive, vagoane etc) – E 25.*

➢ **Sistem informatic "Material rulant"** cu următoarele componente IRIS – RSMA (Spear2000), I – PARC.

3. OBIECTUL CAIETULUI DE SARCINI

Obiectul caietului de sarcini îl reprezintă achiziția unor servicii de audit tehnic și de securitate informatică în conformitate cu prevederile Ordonanței de Urgență nr. 155/2024 *privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil.*

Serviciile de audit tehnic și de securitate informatică trebuie să determine dacă CNCF „CFR" - SA îndeplinește sau trebuie să: implementeze măsuri tehnice și organizatorice, aliniate la standardele naționale și internaționale, care să vizeze cel puțin:

- Managementul drepturilor de acces;
- Conștientizarea și instruirea utilizatorilor;
- Jurnalizarea și asigurarea trasabilității activităților în cadrul rețelelor și sistemelor informatice;
- Testarea și evaluarea securității rețelelor și sistemelor informatice;
- Managementul configurațiilor rețelelor și sistemelor informatice;
- Asigurarea disponibilității serviciilor esențiale și a funcționării rețelelor și sistemelor informatice;
- Managementul continuității funcționării serviciilor esențiale;
- Managementul identificării și autentificării utilizatorilor;
- Răspunsul la incidente;

- Mentenanța rețelelor și sistemelor informatice;
- Managementul suporturilor de memorie externă;
- Asigurarea protecției fizice a rețelelor și sistemelor informatice;
- Realizarea planurilor de securitate;
- Asigurarea securității personalului;
- Analizarea și evaluarea riscurilor;
- Asigurarea protecției produselor și serviciilor aferente rețelelor și sistemelor informatice;
- Managementul vulnerabilităților și alertelor de securitate, etc.

Pentru fiecare activitate de audit, auditorul de securitate cibernetică va furniza un raport de audit cuprinzând recomandări.

3.1. CANTITĂȚILE NECESARE

Nr. Crt.	Denumirea serviciului	Cod CPV	U.M.	Cantitatea
1	Servicii de audit informatic (conformitate NIS).	72810000-1	serviciu	1

3.2. DURATA DE VALABILITATE A CONTRACTULUI

Durata contractului este de 6 luni, valabilitatea acestuia începând de la data semnării sale de către ambele părți.

3.3. LIVRAREA ȘI RECEPȚIA SERVICIILOR

Achizitorul are dreptul de a verifica modul de prestare a serviciilor pentru a stabili conformitatea lor cu prevederilor din propunerea tehnico-financiară. Verificările vor fi efectuate în conformitate cu prevederile legale, achizitorul având obligația de a notifica prestatorului identitatea reprezentanților săi împuterniciți pentru acest scop, în prezența prestatorului. Durata de livrare este diferită de durata contractului, termenul de livrare a serviciilor este de maxim 5 luni.

Recepția se va face pe baza unui *Proces verbal de acceptare a serviciilor*, întocmit de Prestator și semnat de ambele părți prin care va confirma prestarea serviciilor contractate și prezentarea raportului final în termen de maxim șase luni de la semnarea contractului.

3.4. CONDIȚII DE FACTURARE ȘI PLATĂ

Se va emite o singură factură după finalizarea serviciilor de audit informatic care va fi însoțită de procesul verbal de acceptare a serviciilor.

Factura se va emite în lei, iar termenul de plată este de 60 de zile calendaristice de la data primirii facturii în format electronic în sistemul național privind factura electronică RO e-Factura. Data comunicării facturii electronice către CNCF „CFR" - SA se consideră data la care factura electronică este disponibilă pentru descărcare din sistemul național privind factura electronică RO e-Factura.

4. PROPUNEREA TEHNICĂ

Prestatorul de servicii va prezenta conformitatea Propunerii tehnice cu cerințele generale și specifice solicitate prin prezentul Caiet de sarcini, răspunzând punctual pentru fiecare din cerințe.

4.1. CERINȚE GENERALE

Prestatorul de servicii va oferta un serviciu complet de auditare, conform legislației și normelor aplicabile (Ordonanța de Urgență nr. 155/2024, Ordinul nr. 1323/2020, Ordinul nr. 559/2021, Decizia nr. 88/30.04.2020) pentru domeniul de audit detaliat în Anexa 1.

Componentele auditului se realizează de către auditori atestați ANSRSI, conform normelor aplicabile (Regulament SGG din 22 martie 2021) și în baza standardelor enumerate în decizia nr. 88 din 30 aprilie 2020 a CERT-RO.

Oferta tehnică va conține următoarele:

1. Abordarea generală a auditului de securitate a rețelelor și sistemelor informatice.
2. Plan de proiect pe activități și livrabile intermediare raportului de audit.
3. Metodele de asigurare a confidențialității informațiilor.
4. Mijloacele logistice necesare auditorului de securitate cibernetică ce trebuie puse la dispoziția acestuia de către operatorul economic.

Domeniul general de audit este pentru CNCF „CFR" – SA, entitate esențială cu sistemele: E11, E24, E25.

4.2. CERINȚE SPECIFICE

Auditul tehnic și de securitate informatică este definit ca activitatea prin care se realizează o evaluare sistematică a tuturor politicilor, procedurilor și măsurilor de protecție implementate la nivelul rețelelor și sistemelor informatice, în vederea identificării disfuncțiilor și vulnerabilităților și a furnizării unor soluții de remediere a acestora.

4.2.1. Obiectivele auditului stabilite în conformitate cu legislația aplicabilă sunt:

- Verificarea identificării corecte a rețelelor și sistemelor informatice de auditat, precum și inter-dependențele externe ale rețelelor și sistemelor informatice.
- Evaluarea și revizuirea deciziei și mapei de acreditare
- Verificarea plauzibilității metodologiei și tehnicilor utilizate precum și a măsurilor de control implementate în vederea gestionării riscurilor operaționale identificate.
- Identificarea existenței și determinarea eficacității politicilor și procedurilor de operare așa cum sunt acestea specificate în legislație și standardele adoptate de către OSE.
- Identificarea existenței și determinarea eficacității controalelor tehnice.

4.2.2. Tehnicile de audit implicate în timpul misiunii include, pentru activitățile AS1, AS2 și AS5:

i. Examinare: politici, proceduri, instrucțiuni de lucru, cerințe de bune practici sau de la producător, observarea directă a unui proces sau activitate.

ii. Interviuri cu persoanele responsabile de executarea unor activități sau managementul unui proces.

iii. Testarea prin care se asigură că rezultatul unui proces este cel declarat și asumat.

iv. Auditarea cerințelor minime de securitate trebuie să conducă auditorul la obținerea unei asigurări rezonabile cu privire la existența și la funcționarea corespunzătoare a controalelor interne.

v. În acest sens se va utiliza o metodologie de audit prezentată detaliat de ofertant în oferta tehnică, care atinge următoarele puncte:

1. Planificare	2. Testarea proiectării controalelor	3. Testarea eficienței controalelor	4. Raportare
Identificarea rețelelor și sistemelor ce contribuie la asigurarea serviciilor esențiale.	Revizuirea documentației	Identificarea controalelor tehnice	Raport inițial
Identificarea documentației	Testarea conformității/eșantionare	Realizarea testelor de fond (eficiență/eșantionare)	Răspunsul managementului
Identificare participanți interviuri	Evaluarea probelor / conformitate administrativă	Evaluarea probelor/conformitate tehnică	Raport final
Stabilire risc audit			

4.2.3. Activitățile de audit trebuie să determine dacă Entitatea Contractantă implementează sau trebuie să implementeze măsuri tehnice și organizatorice pentru conformitate cu "Normele tehnice privind cerințele minime de asigurare a securității rețelelor și sistemelor informatice aplicabile operatorilor de servicii esențiale" (prevederile Ordinului 1.323 din 9 noiembrie 2020, emis de Secretariatul General al Guvernului și alte norme asociate ulterioare aplicabile în perioada auditului).

Pentru fiecare indicator de control auditorul de securitate cibernetică va furniza un raport de audit cuprinzând evaluarea gradului de conformitate și recomandări.

Activitățile de audit:

i. Suport preliminar auditării
ii. Auditul arhitecturii (AS1)
iii. Auditul de configurare (AS2)
iv. Auditul de penetrare (AS4)
v. Auditul securității organizației (AS5)

4.2.3.1. Suport preliminar auditării:

Anterior activităților de audit auditorul va realiza un set de 3 sesiuni de informare/instruire de minim 4h fiecare, pentru explicarea cerințelor, a parcursului auditului și a categoriilor de informații și dovezi ce trebuie colectate. Cel puțin una din aceste sesiuni va include și o prezentare de bune practici pentru sisteme și aplicații informatice de securizare, potrivite cu nivelul de complexitate al mediului informatic relevant al achizitorului.

4.2.3.2. Auditul arhitecturii (AS1)

Constă în verificarea conformității măsurilor de securitate legate de alegerea, poziționarea și implementarea dispozitivelor hardware/software în rețelele și sistemele informatice, cerințele minime de securitate și politicile interne al Entității Contractante. Auditul poate fi extins la interconectările cu rețele terțe, inclusiv internetul.

Auditorul de securitate cibernetică trebuie să: revizuiască/ auditeze următoarele aspecte relevante pentru serviciile esențiale:

- diagramele arhitecturale (hardware, software, aplicații) și alte documente de arhitectură;
- matricea fluxurilor de informații și a responsabilităților;
- configurarea echipamentelor;
- interconectări cu rețele terțe sau Internet;
- analizele de risc ale rețelelor și sistemelor informatice;
- măsuri tehnice de control a riscurilor;

4.2.3.3. Auditul de configurare (AS2)

Constă în verificarea implementării măsurilor de securitate în conformitate cu stadiul tehnicii, cerințele minime de securitate și politicile de securitate în ceea ce privește configurația dispozitivelor hardware/software componente ale rețelelor și sistemelor informatice. Aceste dispozitive pot fi în special echipamente de rețea, server sau stație de lucru, aplicații/sisteme de operare sau produse de securitate.

Auditorul de securitate cibernetică trebuie să verifice securitatea configurațiilor, în conformitate cu regulile specifice ale OSE aplicarea politicilor de securitate pentru componentele din arhitectura serviciilor esențiale precum:

- echipamente de rețea cu fir sau fără fir
- echipamente de securitate
- sisteme de operare
- sisteme de gestionare a bazelor de date
- servicii de infrastructură
- servere de aplicații
- stații de lucru
- medii de virtualizare

4.2.3.4. Auditul de penetrare (AS4)

Auditul de penetrare se face pe bază de eșantion, agreat în prealabil cu Entitatea Contractantă în cadrul contractului. Informațiile necesare ofertării pentru cuantificarea efortului asociat acestei etape sunt prezentate în Anexa 2.

Auditul se va desfășura în conformitate cu cerințele Regulamentului din 22 martie 2021 al Secretariatului General al Guvernului României pentru atestarea și verificarea auditorilor de securitate

cibernetică. Testele de penetrare se vor realiza prin sondaj prin verificarea unui eșantion reprezentativ de echipamente/aplicații, cu un grad de încredere de 95% și o marjă de eroare de 2%.

Scopurile fiecărei acțiuni de auditare în parte sunt prezentate mai jos:

- Test de penetrare a rețelei care deservesc serviciile esențiale, din exterior: Identificarea IP-urilor publice, scanarea porturilor de rețea, crearea hărții rețelei instituției văzută din exterior.
- Test penetrare a centrului de date în care sunt găzduite cele două sisteme informatice ce deservesc serviciile esențiale, din interior: Scanarea porturilor deschise, crearea hărții centrului de date văzută din interior, identificarea porturilor ce pot permite exploatarea unor vulnerabilități cunoscute sau necunoscute.
- Scanarea vulnerabilităților la nivelul celor două sisteme informatice ce deservesc serviciile esențiale: Scanarea infrastructurii celor două sisteme informatice ce deservesc serviciile esențiale în vederea identificării, analizării și prioritizării nivelului critic al vulnerabilităților cunoscute și necunoscute, folosind instrumente ale Prestatorului (licențiate de acesta pentru astfel de utilizării) sau ale Entității Contractante (OpenVAS).
- Auditare ActiveDirectory - Verificarea conturilor de tip user, admin, conturi de serviciu; verificarea drepturilor conform principiului acordării privilegiilor necesare în vederea desfășurării activității în condiții optime (least privilege), a politicilor de grup (GPOs), a politicii privind parolele (Entitatea Contractantă implementează o soluție tehnică dedicată pentru aceste rapoarte).
- Audit aplicații interne din punct de vedere al securității IT: Verificarea acordării drepturilor de acces organizate din punct de vedere al granularității acestora, pentru aplicațiile ce contribuie la realizarea serviciului esențial.
- Validarea nivelului de securitate al accesului din exterior cu VPN - Identificarea modului de acces de la distanță către rețeaua internă și a măsurilor de verificare.
- Identificarea zonelor cu un risc potențial crescut. Identificarea resurselor informatice critice pentru activitatea organizației.
- Inventarierea metodelor și instrumentelor de securitate existente pentru detecția și răspunsul la incidente.

Test de penetrare din exterior:

Se vor efectua teste specifice de penetrare din exterior (Internet) în conformitate cu standardele de securitate relevante iar tehnicile utilizate vor fi, fără a se limita la:

- Recunoaștere
- Testele firewall-ului
- Identificarea serviciilor disponibile
- Obținerea accesului neautorizat la credențiale
- Exploatarea vulnerabilităților specifice serviciilor expuse extern
- Spargerea unui eșantion reprezentativ din conturile identificate folosind dicționare, tehnice de tip brute-force, tehnici hibride, atacuri de tip MITM.
- Identificarea porților de acces de la distanță prin construcție (back-doors)
- Identificarea punctelor slabe ale arhitecturii
- Identificarea punctelor slabe în implementare/configurare
- Identificarea deficiențelor în proiectarea și implementarea politicilor de securitate
- Analiza specifică a vulnerabilității sistemelor din domeniul de aplicare
- Evaluarea proiectării și implementării VPN și a politicilor de acces la distanță

Test de penetrare din interior:

Se vor efectua teste specifice de penetrare din interior (PC standard) în conformitate cu standardele de securitate relevante iar tehnicile utilizate vor fi, fără a se limita la:

- Ordonanța de Urgență nr. 155/2024 și Regulamentul din 22 martie 2021 pentru atestarea și verificarea auditorilor de securitate cibernetică
- Ordinul nr. 1323/2020 pentru aprobarea Normelor tehnice privind cerințele minime de asigurare a securității rețelelor și sistemelor aplicabile operatorilor de servicii esențiale.
- Penetration Testing Framework
- Penetration Testing Execution Standard
- OWASP

Efectuarea testelor de penetrare, atât din exterior cât și din interior nu trebuie să afecteze integritatea rețelelor sau sistemelor informatice și nici disponibilitatea serviciilor esențiale.

4.2.3.5. Auditul securității organizației (AS5)

Constă în auditarea cu privire la securitatea logică și fizică și urmărește să se asigure că politicile și procedurile de securitate definite de Entitatea Contractantă:

a. Sunt conforme cu nevoile de securitate al organizației, nivelul tehnologic și standardele în vigoare.
b. Completează corect măsurile tehnice implementate
c. Sunt puse efectiv în practică.

Auditorul va verifica:

Organizarea securității rețelelor și sistemelor informatice pe baza standardelor tehnice și de reglementare stabilite în LSSEINIS, în conformitate cu cerințele minime de securitate aplicabile OSE.

Va integra în analiza elementelor legate de securitatea aspectelor fizice ale rețelelor și sistemelor informatice ce deservesc serviciile esențiale, în special, protecția spațiilor care găzduiesc componente ale rețelelor și sistemelor informatice și a datelor/ informațiilor auditate sau controlul accesului la aceste componente.

Auditorul va evalua gradul de conformitate în ceea ce privește modul de implementare al guvernantei securității informatice, protecției cibernetice, apărării cibernetice și rezilienței cibernetice la nivelul OSE.

5. CONFIDENȚIALITATEA INFORMAȚIILOR

Prestatorul va respecta prevederile privind datele cu caracter personal așa cum rezultă din Regulamentul (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date.

Informațiile vor fi folosite numai în scopul îndeplinirii sarcinilor contractuale și nu vor fi divulgate unor terți.

6. DISPOZIȚII FINALE

Cerințele impuse în prezentul caiet de sarcini vor fi considerate ca fiind minimale. În acest sens, orice ofertă de bază prezentată, care se abate de la prevederile caietului de sarcini, va fi luată în considerare, dar numai în măsura în care aceasta presupune asigurarea unor specificații superioare cerințelor minimale din caietul de sarcini, în caz contrar oferta nu va fi luată în considerare.

Anexa nr. 1 Domenii de audit, Anexa nr. 2 Date de eșantionare pentru auditul de penetrare și Anexa nr. 3 Prezentare sisteme informatice sunt parte integrantă din prezentul caiet de sarcini.

Director Direcția Tehnică
Cristian - Florian DOBRESCU

Șef serviciu Tehnic
CARCAN Raluca

Redactat: Mirela - Mădălina OTĂRANU
Data red.: 03.11.2025

Anexa 1 Domenii de audit

Domeniul de audit		AS1 - Auditul arhitecturii	AS2 - Auditul de configurare	AS4 - Audit de penetrare	AS 5 - Cerințe specifice auditului securității organizației
Nivel OSE global	Auditul centrului de date și DMZ	1.1	2.1	4.1	5.1
	Auditul rețelei	1.2	2.2	4.2	
	Auditul nivelului de acces general (stații de lucru, autentificare și autorizare, protecție locală)	1.3	2.3	4.3	
E11- Controlul și gestionarea traficului feroviar (supravegherea și reglementarea traficului, semnalizarea; planificarea traficului, gestionarea traseului trenurilor)	Auditul arhitecturii centrale pentru circulație trenuri	1.4	2.4	4.4	
	Auditul platformelor de virtualizare	1.5	2.5	4.5	
	Auditul nivel de acces dedicat (stații de lucru, autentificare și autorizare, protecție locală)	1.6	2.4		
E 24- Întreținerea infrastructurii feroviare;	Auditul arhitecturii centrale infrastructura feroviară	1.4	2.4	4.4	
	Auditul platformelor de virtualizare	1.5	2.5	4.5	
	Auditul nivel de acces dedicat (stații de lucru, autentificare și autorizare, protecție locală)	1.6	2.4		
E 24- Întreținerea infrastructurii feroviare;	Auditul arhitecturii centrale gestiune stocuri și imobilizări corporale	1.4	2.4	4.4	
	Auditul platformelor de virtualizare	1.5	2.5	4.5	
	Auditul nivel de acces dedicat (stații de lucru, autentificare și autorizare, protecție locală)	1.6	2.4		
E25 - Întreținerea materialului rulant (locomotive, vagoane etc)	Auditul arhitecturii centrale material rulant	1.4	2.4	4.4	
	Auditul platformelor de virtualizare	1.5	2.5	4.5	
	Auditul nivel de acces dedicat (stații de lucru, autentificare și autorizare, protecție locală)	1.6	2.4		

1.1 Centrul de date - Diagramele arhitecturale de nivel 2 și 3 din modelul OSI; Matricea fluxurilor, regulile de filtrare, configurarea echp de rețea; Documentele de arhitectură tehnică

1.2 Rețeaua generală RENTRAD -- Diagramele arhitecturale, metodă alocare și control IP-uri, nivel WAN, acces VPN;

1.3 Control al stațiilor de lucru și al utilizatorilor - arhitectura generală de management, autentificare și autorizare, anti-virus;

1.4 Diagrama și inventarul arhitecturii centrale pentru cele 4 sisteme informatice ce deservesc serviciile esentiale – E11, E24, E25;

1.5 Arhitecturi de virtualizare. Lista administratorilor pe roluri. Configurarea de securitate a platformelor celor 2 sisteme informatice ce deservesc serviciile esențiale - E11, E24, E25;

1.6 Control al stațiilor de lucru și al utilizatorilor - arhitectura dedicată de management, autentificare și autorizare, anti-virus a sistemelor informatice ce deservesc serviciile esențiale - E11, E24, E25

2.1 Audit de configurare - puncte de acces Internet/Rentrad. Servere sensibile (AD, CA, FS, DNS, Mail); Sisteme critice; Firewall intern și extern;

2.2 Configurare de securitate WAN, LAN-Dist, instrumente de management;

2.3 Politica standard CNCF „CFR" - SA. și politica stații privilegiate

2.4 Configurări de securitate pentru cele 4 sisteme informatice ce deservesc serviciile esențiale - E11, E24, E25

2.5 Configurare de securitate și evaluare vulnerabilități platforme de virtualizare pentru cele 4 sisteme informatice ce deservesc serviciile esențiale - E11, E24, E25

4.1 Pentest DMZ-DC, pentest Rentrad-DC - Black, Grey, White;

4.2 Basic blackbox (scanare routere și aplicații de management);

4.3 Blackbox stații de lucru utilizatori privilegiați;

4.4 Black-box/Grey-box servicii publice pentru cele 4 sisteme informatice ce deservesc serviciile esențiale - E11, E24, E25;

4.5 Hypervisor hijacking (mai ales versiuni vechi), în funcție de recomandarea auditorului pentru cele 4 sisteme informatice ce deservesc serviciile esențiale - E11, E24, E25;

5.1 Auditul de securitate a organizației se realizează pentru CNCF „CFR" - SA. în calitate de OSE.

Anexa 2: Date de eșantionare pentru auditul de penetrare

Tip	Categorie / Serviciu Esențial	Nume	Tip test	Cant. Eșant.
Comunicații	Infrastructură comună	Punct de acces internet (NGFW și filtrare trafic)	Extern	1
Server	Infrastructură comună	Active Directory	Intern	2
Cluster Virtualizare	Infrastructură comună	Hyper-V	Intern	1
Comunicații	Infrastructură comună	Soluție reverse proxy și autentificare DMZ (Citrix ADC)	Extern	1
Comunicații	Infrastructură comună	Firewall, IDS/IPS Datacenter	Intern	1
Comunicații	Infrastructură comună	Punct de acces VPN	Extern	2
Comunicații	Infrastructură comună	Router core	Intern	1
Comunicații	Infrastructură comună	Router WAN	Intern	1
Comunicații	Infrastructură comună	Switch L3 Cisco	Intern	2
Comunicații	Infrastructură comună	Router/Switch L3 Edge	Intern	4
Comunicații	Infrastructură comună	Wireless Routers/Aps	Intern	2
Server și interfețe	Serviciul esențial E11	Servicii web Circulație/OTF, IMComm, Accepte Portuare, IRIS2TMS	Extern	5
Stații de lucru și periferice	Serviciul esențial E11	Post de lucru IDM/RC modernizat	Intern	2
Server	Serviciul esențial E24	Bază de date comună Managementul Infrastructurii, aplicații web IRIS-IMA	Intern	4
Server	Serviciul esențial E25	Server iParc, bază de date RSMA	Intern/Extern	2

Anexa 3: Prezentare sisteme informatice

1. Sistemul informatic "Circulație trenuri" acoperă activitățile specifice de programare, monitorizare, analiză și constituirea elementelor de tarifare a circulației trenurilor.

- IRIS – ATLAS – IM, aplicație de programare și analiză a circulației trenurilor, specifică managerului de infrastructură feroviară. Aplicația asigură funcționalitățile necesare programării lunare, decadice și zilnice, în conformitate cu instrucțiile aplicabile la CFR.;

- IRIS – CRONOS, aplicație de raportare a execuției circulației trenurilor de către personalul autorizat al managerului de infrastructură feroviară din stațiile de cale ferată (IDM) și din unitățile teritoriale, regionale și centrale de management trafic (RC – regulatoare de circulație). Aplicația permite raportarea sosirii, expedierii, trecerii fiecărui tren aflat în programul de circulație, direct de la stațiile de cale ferată sau indirect, de la unitățile care au arondate linii neinteroperabile sau secții secundare.

Aplicația permite, de asemenea, raportarea deviațiilor de la program (întârzieri, cu explicații), transmiterea de ordine și mesaje între IDM și RC, raportarea de evenimente; În aplicație se poate configura functionalitatea de informare a publicului calator PIS. Aplicația trebuie să fie în conformitate cu cerințele actuale ale procesului de management al traficului feroviar inclusiv cu cerințele TAF-TSI, TAP-TSI;

- IRIS – FOCUS, aplicație de monitorizare a circulației trenurilor, în unitățile de management de trafic. Aplicația permite vizualizarea circulației efectuate față de programat, cu evidențierea deviațiilor de la program. Aplicația trebuie să asigure conformitatea cu Standardele de Interoperabilitate pentru Aplicații Telematice de Marfă și Pasageri (TAF-TSI, TAP-TSI);

- IRIS – FOCUS – RU, aplicația asigură vizualizarea graficului de circulație realizat, graficelor din baza de date curentă, din arhivă sau din istoric; aplicația funcționează prin internet (nu depinde de rețeaua RENTRAD-CFR);

- IRIS – CALIPSO, aplicație de concentrare, prelucrare și prezentare a elementelor de tarifare a circulației trenurilor către operatorii de transport feroviar (OTF), care plătesc taxa de utilizare a infrastructurii (TUI), pe baza contractelor de acces încheiate cu managerul de infrastructură – C.F.R. Aplicația furnizează în mod automat, pentru fiecare OTF, volumul de tren-km care face obiectul pachetului minim social;

- IRIS – INFO – IM, aplicație de informare privind prestațiile de trafic (circulație trenuri), asigură o informare generală și de detaliu, de tip tablou de bord;

- E – TELEX, aplicație de telegrafie electronică;

- INFOKIOSK, aplicație de informare public călător în stații, la kiosk self-service. Aplicația asigură afișarea informațiilor de mers de tren ale operatorilor de transport care acceptă furnizarea acestora precum și alte informații referitoare la stația de cale ferată și la localitate (ex: obiective turistice, unități de cazare și masă, companii de taximetrie, istorie stație de cale ferată,);

- CRONOS VOX aplicație specifică pentru îndeplinirea obligațiilor de informare a publicului călător în stații de cale ferată, include interfața pentru preluarea datelor de circulație (program, sosiri, plecări) din IRIS, posibilitatea completării cu datele de garare și alte informații, interfața pentru panourile de afișaj și interfața pentru anunțuri vocale în stație;

- TraficAlert, aplicație pentru evidența perturbărilor de trafic, care trebuie să permită culegerea de date privind situațiile generatoare de întreruperi/limitări de trafic feroviar, reprezentarea grafică pe hartă a perturbărilor, pe categorii, obținerea de rapoarte specifice pentru managementul operativ al traficului feroviar;

- Hărți DRR, aplicație pentru realizarea de hărți tematice necesare Declarației de Referință a Rețelei (Network Statement), în vederea evidențierii liniilor interoperabile/neinteroperabile, electrificate/neelectrificate, simple/duble, tipuri de instalații de semnalizare/centralizare electronică/ERTMS;

- Editare Hărți transparență, aplicații pentru actualizarea și editarea atributelor pentru obiectivele de pe cele trei hărți interactive: Harta interactivă cu modernizările trecerilor la nivel, Harta interactivă cu

obiectivele de investiții ale infrastructurii feroviare finanțate de la bugetul de stat și Harta interactivă cu obiectivele de investiții ale infrastructurii feroviare finanțate din fonduri externe;

- Regim de Performanță, serviciu de aplicație pentru calcularea indicatorilor legați de Regimul de Performanță al circulației trenurilor. Aplicația trebuie să primească date legate de programarea circulației trenurilor din aplicația ATLAS, date legate de circulația reală a trenurilor din aplicația CRONOS, date legate de valoarea TUI aferentă trenurilor suplimentare, respectiv a trenurilor anulate din aplicația CALIPSO și să transmită date către aplicația ATLAS. Aplicația trebuie să ofere managerului de infrastructură suport în procesul de urmărire a principalilor indicatori de performanță ce vizează activitatea de programare și circulație a trenurilor. Aplicația trebuie să implementeze Directiva europeană 2012/34/UE transpusă în România prin Legea nr. 202/2016. Aplicația trebuie să reprezinte o platformă colaborativă între managerul de infrastructură și operatorii de transport feroviar, beneficiarul oferind acestora posibilitatea de utilizare a aplicației. Aplicația trebuie să permită OTF validarea datelor înregistrate privind circulația trenurilor suplimentare, anularea circulației trenurilor și întârzierile trenurilor;

- Accepte Programare (include modulele: Accepte Portuare, Calcul Penalități OMTI 8), serviciu de aplicație pentru conducerea și coordonarea eficientă a traficului feroviar de marfă ce are ca origine sau destinație stații ce deservesc complexurile portuare și/sau stații ce deservesc operatori economici de transport al mărfurilor pe calea ferată. Aplicația reprezintă o platformă colaborativă între managerul de infrastructură, operatorii de transport feroviar de marfă, operatorii de manevră și operatorii de exploatare portuară și/sau operatorii economici, după caz, beneficiarul oferind tuturor acestora posibilitatea de utilizare a aplicației. Aplicația preia de la operatorii de transport feroviar informații privind: stația de expediere, stația de destinație a trenului, beneficiarul transportului, numele operatorului (portuar, după caz) care va asigura operarea mărfii în port sau la front, operațiunea din port și/sau de pe liniile industriale de încărcare-descărcare (transbord direct, încărcare, descărcare), respectiv să preia de la operatorii portuari informații privind: numele operatorului de manevră, confirmarea pentru programarea circulației trenurilor stabilind o ordine a primirii trenurilor la destinație;

- IMComm, aplicația oferă managerilor de infrastructură (CFR și MAV) suport în procesul de programare eficientă a trenurilor de călători și marfă ce tranzitează frontierele de stat cu Ungaria. Aplicația trebuie să colecteze în mod automat în timp real date din sistemele de circulație a trenurilor ale celor doi manageri de infrastructură, CFR și MAV, respectiv informații despre operatorii de transport feroviar, trenurile care se expediază și sosesc în stațiile de frontieră, stația de destinație, momentul până la care mecanicii de locomotivă sunt apți de serviciu. Aplicația trebuie să permită emiterea acceptului de primire a trenurilor internaționale de marfă pe rețeaua CFR precum și selectarea trenului pereche din lista de trenuri programate din sens opus, astfel încât să furnizeze informațiile necesare pentru conducerea și coordonarea traficului feroviar de marfă spre rețelele feroviare vecine;

- Polifem Constanța, serviciu de aplicație destinat calculului tarifelor conexe din activitatea de transport feroviar, specific activității complexului feroviar Constanța Port. Aplicația permite culegerea datelor cu privire la mișcările materialului rulant în complexul portuar, să calculeze taxele aferente staționării, manevrei și accesului convoaielor de manevră pe liniile din stațiile complexului Constanța Port, să genereze borderouri cu prestațiile efectuate, precum și rapoarte;

- Tarife pentru servicii adiționale (T.S.A.) fost Polifem, serviciu de aplicație destinat pentru calculul tarifelor conexe din activitatea de transport feroviar. Aplicația trebuie să permită culegerea datelor cu privire la mișcările materialului rulant în stațiile de cale ferată, să calculeze taxele de staționare a vagoanelor în stațiile de cale ferată, să genereze borderouri cu prestațiile efectuate, precum și rapoarte;

- WIMO-IM, serviciu de aplicație pentru stocarea datelor de compunere tren primite de la operatorii de transport feroviar prin intermediul mesajului TAF-TSI Train Composition. Datele tehnice și comerciale ale vagoanelor trebuie să fie păstrate în baza de date WIMO (Wagon and Intermodal Unit Operation).

- Căi Libere, serviciu de aplicație prin care se realizează transmiterea și recepționarea de mesaje tip, cu parametrii, între doi participanți care vorbesc limbi diferite.

2. Sistemul informatic "Infrastructură feroviară" acoperă activitățile specifice de evidență tehnică a elementelor de infrastructură (linii, instalații), evidență a deranjamentelor, respectiv de gestiune a lucrărilor de întreținere a acestora cu componentele:

- IRIS – IMA (MP5i), aplicație de evidență a elementelor de infrastructură feroviară și de gestiune a lucrărilor de întreținere (materiale și manoperă) programate și efectuate;

- IRIS – IMA (Harta GIS CFR), aplicația asigură evidența geografică a elementelor de infrastructură feroviară;

- Web – INSPIRE, serviciu de aplicație care trebuie să asigure introducerea, actualizarea, vizualizarea și interogarea atributelor specifice elementelor de infrastructură feroviară (stații, interstații, treceri la nivel, zone cf aferente stațiilor și interstațiilor, zone de triaj), conform Directivei Inspire 2007/2/CE;

- IRIS – IMA (WebSCB), aplicație de evidență furturi din instalațiile SCB, pe tipuri de aparataj;

- IRIS – IMA (WebSIMC), aplicație de urmărire realizări-imobilizări mașini grele de cale și lucrări manuale;

- IRIS – IMA (WebSafety), aplicație de evidență a accidentelor - incidentelor de cale ferată, disponibilă pentru activitatea de siguranța circulației la nivel central (RGSC);

- WebEMM, aplicația asigură evidența echipamentelor (mijloacelor) de măsură și control, verificate și întreținute în limitele de precizie standardizate și controlate periodic, utilizate în procesul de monitorizare a siguranței circulației pe calea ferată, protecția mediului și a muncii;

- ENTRAC, aplicație pentru defalcarea consumurilor de energie electrică. Aplicația trebuie să asigure și administrarea contractelor de achiziție a energiei electrice la 25 kV respectiv a energiei electrice pentru utilități pentru consumatori și subconsumatori. În modulul pentru evidențierea și gestionarea consumurilor de energie electrică ale subconsumatorilor CFR aplicația trebuie să permită adăugarea, actualizarea, interogarea, listarea datelor despre subconsumatorii CFR cu asocierea acestor puncte de consum la cele aflate în modulul de evidență a energiei electrice de utilități. În modulul economic pentru urmărirea și gestionarea facturilor emise de furnizori aplicația trebuie să permită adăugarea, actualizarea, interogarea, listarea datelor despre facturi și plăți. În modulul de urmărire a încadrării în prevederile contractuale (cumularea situațiilor de consum energie și contravaloarea acesteia pe durata de execuție a contractelor) aplicația trebuie să permită vizualizarea, interogarea, cumularea, listarea datelor;

- Program Cadru Anual IT / ITP pentru realizarea și gestionarea programelor cadru anuale de Inspecție tehnică / Întreținere tehnică preventivă la nivelul fiecărei secții CT;

- AVI–GABARITE, aplicația permite verificarea înscrierii unui transport negabaritic prin lucrările de artă și pe lângă instalațiile și construcțiile aflate lângă linii CF, cu asigurarea rezervelor minime instrucționale prevăzute de Instrucția 328/2008. Pentru realizarea verificării aplicația trebuie să pună la dispoziție funcționalități de culegere/actualizare date despre gabaritele libere reale, culegere/actualizare date despre transporturile negabaritice, selectare rută de deplasare a transportului negabaritic, verificare înscriere transport pe ruta selectată cu respectarea prevederilor Instrucției 328/2008. Aplicația trebuie să permită gestionarea evidenței podurilor cu restricții de tonaj aflate în exploatarea CFR SA și stabilirea condițiilor de circulație pentru grupuri de 2-6 locomotive peste aceste poduri;

- e–RINF, aplicație software care trebuie să asigure colectarea, prelucrarea și gestionarea centralizată a datelor aferente infrastructurii feroviare naționale, compatibilă cu cerințele Registrului de infrastructură feroviară creat la nivel European de către Agenția Uniunii Europene pentru Căile Ferate; Dezvoltările/modificările/actualizările ce implică modificări importante în structura bazei de date și în programele aplicației se vor realiza la solicitarea Beneficiarului, în limita fondurilor alocate, pe bază de comandă și deviz în cadrul lucrărilor suplimentare;

- RegistruActive, aplicație informatică care trebuie să asigure centralizarea datelor de identificare privind evidența mijloacelor fixe, actualizarea permanentă a acestora prin intermediul SRCF 1-8 și monitorizarea, verificarea și listarea informațiilor la nivel central (aplicația nu urmărește evidența mijloacelor fixe din punct de vedere contabil).

3. ***Sistem informatic IT "Gestiune stocuri și imobilizări corporale" cu următoarele componente: e–MPS, e–SIGMA, eMiFixe;***

- e–MPS – aplicația trebuie să permită elaborarea Nomenclatorului unic de materiale (structurat pe serii, grupe și denumiri generice), utilizat pentru gestionarea unitară a materialelor în toate unitățile administrative ale CFR;

- e–SIGMA – aplicația trebuie să permită gestiunea contabilă a stocurilor de materiale și evidența obiectelor de inventar în folosință; trebuie să ofere o imagine centralizată a stocurilor la nivelul unităților CF, SRCF 1-8, Central CFR, prin folosirea de către toate unitățile a unui Nomenclator unic de materiale, asigurându-se astfel condițiile pentru o activitate eficientă de analiză a stocurilor, stabilirea programelor pentru lucrările de reparații curente și întreținerea infrastructurii feroviare, a planurilor de aprovizionare, PAAS, etc. Aplicația trebuie să asigure: obținerea de rapoarte privind stocul pentru un articol, una sau mai multe categorii de articole sau toate articolele; evoluția stocurilor într-o perioada de timp; situația stocurilor la o anumită dată; situația stocurilor fără mișcare, cu mișcare lentă și cu mișcare la o anumită dată.

  Nomenclatorul unic de materiale și piese de schimb, care constituie elementul cheie al gestiunii de stocuri, va fi generat și administrat de aplicația e-SIGMA (Nomenclator Denumiri Comerciale specifice, așa cum figurează în Fișa de magazie) pe baza Nomenclatorului unic cu Denumiri Generice generat si administrat la nivel central CFR prin aplicația e-MPS.

  Pentru realizarea gestiunii unitare a stocurilor prin aplicația e-Sigma este necesar ca beneficiarul să asigure completarea și validarea Nomenclatorului unic cu Denumiri Generice precum și realizarea inventarelor în toate gestiunile cât și refacerea/completarea Fișelor de magazie cu noua codificare a materialelor.

- eMiFixe - aplicație informatică ce asigură evidența, urmărirea și calculul amortizării lunare a imobilizărilor corporale pentru fiecare punct de lucru și centralizat la nivel de societate, și oferă suport pentru activitatea de inventariere anuală a patrimoniului societății prin obținerea listelor de inventar conforme reglementărilor în vigoare precum și a rapoartelor specifice detaliate și/sau centralizate.

4. ***Sistem informatic "Material rulant" cu următoarele componente IRIS – RSMA (Spear2000), I – PARC.***

- IRIS – RSMA (Spear2000), aplicație de gestiune tehnică a parcului de material rulant și a lucrărilor de întreținere a acestuia;
- I – PARC, aplicație pentru Management parc activ/inactiv de material rulant (include funcțiile de istoric date financiare, arhiva fișe reparații, inventarieri anuale, asigurare compatibilitate cu datele necesare TAF-TSI).