OFERTĂ TEHNICĂ

Servicii de elaborare şi implementare a unui nou sistem informaţional „Protecţia Socială” pentru anii 2026-2028.

Digitally signed by Cojocari Andrei
Date: 2026.05.22 08:16:58 EEST
Reason: MoldSign Signature
Location: Moldova
MOLDOVA EUROPEANĂ

Autoritate contractantă: Casa Națională de Asigurări Sociale

Contents

1. Glosar 8
2. Sinteză tehnică și ghid de verificare 9
2.1 Scopul acestei sinteze 9
2.2 Ce se propune 9
2.3 Cum se comportă soluția în practică 9
2.4 Arhitectura propusă și principiul de control tehnic 10
2.5 Migrare, phase-in și continuitate operațională 11
2.6 Livrare, acceptanță și handover 11
2.7 Utilizarea documentului și trasee de verificare 11
3. Înțelegerea obiectului și contextului CNAS 14
3.1 Obiectul proiectului: platformă instituțională, nu aplicație de evidență 14
3.2 Anexele funcționale ca descriere operațională a sistemului 14
3.3 Domenii operaționale principale 15
3.4 Problemele reale pe care sistemul trebuie să le rezolve 18
3.5 Principii de soluție, rol CNAS și rezultat urmărit 18
4. Model funcțional, UC-uri și anexe funcționale 20
4.1 Relația dintre UC-urile ToR și modelul funcțional propus 20
4.2 Gruparea funcțională a UC-urilor 23
4.3 Procese utilizator, cereri și lucru operațional 24
4.4 Registre, date, integrare și configurări 26
4.5 Rapoarte, documente, proceduri automate și audit 27
4.6 Lanțurile operaționale end-to-end 28
4.7 Ce trebuie demonstrat la acceptanță 32
4.8 Concluzie funcțională 32
5. UX/UI, MUD, accesibilitate și bilingvism/multilingvism 34
5.1 Rolul interfeței în SI „Protecția Socială” 34
5.2 Acoperirea cerințelor UI din caietul de sarcini 34
5.3 Aplicarea Modelului Unitar de Design 35
5.4 Arhitectura informațională și navigarea 35
5.5 Spațiul de lucru pe roluri și dashboardurile operaționale 35
5.6 Formulare, validări și lucrul cu date sensibile 36
5.7 Căutare, filtre, liste și registre 36
5.8 Limbile interfeței, traduceri și conținut 36
5.9 Accesibilitate și utilizare asistată 36
6. Configurabilitate, workflow și administrare operațională 38
6.1 Poziționarea ofertată: configurare cu efect operațional controlat 38
6.2 Acoperirea UC-urilor în stratul de configurabilitate și administrare 39

6.3 Acoperirea UC15-UC23 în administrarea sistemului 40
6.4 Operarea configurărilor, evidențe și rezultat 43
7. Interoperabilitate, MConnect și web-servicii 46
7.1 Rolul interoperabilității în SI „Protecția Socială” 46
7.2 Cerințele de interoperabilitate și aria acoperită 46
7.3 Integration Gateway / WSAdapter ca limită controlată de integrare 47
7.4 Integrarea cu ecosistemul e-guvernare 47
7.5 Servicii expuse de SI „Protecția Socială” 47
7.6 Servicii consumate și date externe 48
7.7 Integrarea cu Sistemul informațional financiar al CNAS (FMS) 48
7.8 Evenimente, mesagerie și procese asincrone 48
7.9 Semantica datelor, catalogul de integrare și modelul canonic 49
7.10 Securitate, audit și protecția datelor în schimbul de date 49
7.11 Reziliență, indisponibilitate externă și reconciliere 49
7.12 Monitorizare operațională și suport pentru integrări 50
7.13 Catalogul de integrare și pachetul de evidențe 50
7.14 Rezultatul urmărit pentru CNAS 50
8. Raportare, documente, șabloane și BI 52
8.1 Poziționarea capitolului: raportarea ca ieșire oficială a sistemului, nu ca anexă tehnică 52
8.2 Ancorarea în UC-uri și în Functional Backbone 52
8.3 Modelul de raportare propus 53
8.4 Date pregătite pentru raportare 53
8.4.1 Industrializarea raportării 54
8.4.2 Straturile tehnice și funcționale ale sursei de raportare 54
8.4.3 Scenariu descriptiv 55
8.4.4 Reguli de actualizare 56
8.4.5 Procesul de închidere lunară și raportarea pe perioade controlate 57
8.4.6 Instrumente și opțiuni tehnologice pentru fabrica de date de raportare 57
8.4.7 Catalogul de indicatori și guvernanța produselor de date 58
8.4.8 Reguli de proiectare care protejează oferta și implementarea 59
8.5 Raportare la scară: până la 150 de rapoarte și execuție în fundal 60
8.6 JasperReports ca mecanism controlat de raportare și documente 60
8.7 Documente, șabloane, exporturi și dashboarduri 61
8.8 Validarea rapoartelor, documentelor și șabloanelor 62
8.9 Evidențe și rezultat pentru raportare 63
9. Arhitectura soluției, stiva tehnologică, deployment și operabilitate 65
9.1 Sumar executiv al capitolului 65
9.2 Poziționarea arhitecturii: tehnologie ca mecanism de control 68

9.3 Principiul arhitectural: separare, control, reutilizare și operabilitate 68
9.4 Stack pe straturi: mecanisme asumate ale soluției 68
9.5 Application & API Layer 71
9.6 Identity, autentificare și autorizare: MPass nu înlocuiește controlul intern al accesului 71
9.7 Functional Backbone & Shared Services: mecanismul care ține sistemul unitar 72
9.8 Messaging, evenimente și asincronie 72
9.9 Batch, workers și orchestration 73
9.10 Data Persistence Layer 74
9.11 Reporting Data Factory: strat de raportare industrializat 74
9.12 Cache, căutare și fișiere: reducerea presiunii pe baza operațională 75
9.13 Observabilitate și operabilitate: sistemul explică ce se întâmplă 75
9.14 Platformă de deployment: containere, Kubernetes, Helm și MCloud ca strat de execuție 76
9.15 CI/CD, release control și trasabilitate deployment 78
9.16 Securitate arhitecturală și privacy by design 79
9.17 Continuitate operațională, backup, restore 80
9.18 Livrabile și evidențe de acceptanță pentru arhitectură și stack 83
9.19 Rezultatul arhitectural livrat către CNAS 84
10. Securitate informațională, audit și protecția datelor personale 88
10.1 Poziționarea securității 88
10.2 Ancora în cerințele ToR, UC-uri și standarde 89
10.3 Identitate, autentificare și autorizare granulară 90
10.4 Clasificarea datelor, marcaje de securitate și reguli de afișare 92
10.5 Protecția datelor personale pe ciclul de viață 92
10.6 Securitatea interfețelor, API-urilor și integrărilor externe 93
10.7 Securitate aplicație, validare și protecție OWASP 94
10.8 Secrete, criptare, caching și protecția datelor confidențiale 94
10.9 Audit business, jurnalizare centralizată și trasabilitate 94
10.10 Integritatea datelor și prevenirea manipulării 95
10.11 DevSecOps, testare de securitate și readiness 96
10.12 Monitorizare, incidente de securitate și răspuns operațional 96
10.13 Separarea mediilor și protecția datelor în testare, instruire și suport 96
10.14 Evidențe de acceptanță pentru securitate și protecția datelor 97
10.15 Rezultatul livrat pentru CNAS 101
11. Migrare, phase-in, punere în producție și stabilizare 102
11.1 Rolul capitolului si legatura cu metodologia generala 102
11.2 Obiective operationale si cerinte acoperite 103
11.3 Migration factory 103
11.4 Domenii de date migrate si reguli de prioritate 104

11.5 Data cleansing, sandbox de migrare si decizii asupra datelor murdare 105
11.6 Reconciliere, cockpit de calitate si acceptanta migrarii 106
11.7 Strategia de phase-in si co-existenta controlata 106
11.8 Sursa oficiala, freeze, delta si cutover pe date 107
11.9 Production rehearsal si go-live readiness 108
11.10 Plan de punere in productie, cutover, rollback si forward-fix 110
11.11 Stabilizare operațională si command center post-go-live 110
11.12 Defecte, incidente si criterii de acceptanta in stabilizare 112
11.13 Pachetul de evidenta pentru migrare, go-live si acceptanta finala 113
11.14 Rolul CNAS in migrare, phase-in si acceptanta 113
11.15 Rezultatul livrat catre CNAS 113
12. Testare, UAT și acceptanță pe evidențe 115
12.1 Rolul secțiunii 115
12.2 Ancorarea testării în UC-uri, cerințe ToR și livrabile 115
12.3 Strategie de testare bazată pe trasabilitate 117
12.4 Execuție, date de test și medii 117
12.5 UAT, defecte și testarea zonelor critice 118
12.6 Pachet de acceptanță și acoperirea testării 119
13. Instruire, documentație, cod sursă și handover operațional 120
13.1 Rolul secțiunii 120
13.2 Ancorarea instruirii și documentației în UC-uri și cerințe 120
13.3 Instruire pe roluri și scenarii reale 121
13.4 Materiale de instruire și suport post-training 121
13.5 Documentația funcțională, tehnică și operațională 121
13.6 Predare tehnică, handover operațional și criterii de finalizare 122
13.7 Handover operațional și shadowing tehnic 122
14. Suport, garanție, mentenanță și service management 124
14.1 Poziționarea serviciilor de suport 124
14.2 Obiectivul perioadei de garanție și suport 124
14.3 Model service desk, registru solicitări și SLA 125
14.4 Hypercare, garanție și mentenanță controlată 128
14.5 Raportarea serviciilor de suport 130
15. Proprietate, licențiere, transferabilitate și evitarea dependenței de furnizor 133
15.1 Rolul secțiunii 133
15.2 Ancorarea transferabilității în cerințe, UC-uri și livrabile 133
15.3 Proprietate, licențiere și controlul componentelor terțe 134
15.4 Proprietate, licențiere, transferabilitate și evitarea dependenței de Furnizor 135
15.5 Transfer artefacte, portabilitatea datelor și continuitate 135

16. Managementul implementării, metodologie și plan de execuție 137
16.1 Sumar metodologic și principiu de livrare 137
16.2 Guvernanță, rol CNAS, RACI și mecanisme de decizie 141
16.3 Delivery Assurance: cerințe, trasabilitate, incrementuri și Model Office 144
16.4 Execuție pe fluxuri: Functional Backbone, Shared Services, migrare, integrare, testare 147
16.5 Calitate, securitate, integrare, performanță și testare 155
16.6 Readiness gates, phase-in, BCDR și acceptanță pe evidențe 158
16.7 Raportare, riscuri, schimbări și control operațional 160
16.8 Instruire, handover, service transition și reducerea dependenței de Furnizor 163
17. Corespondență cu anexele suport și documentele de lucru ale ofertei 167

1. Glosar

Glosarul stabilește sensul termenilor metodologici și tehnici folosiți în document. Textul original al ofertei este păstrat; glosarul are rol de referință unică pentru citire consecventă.

Termen	Utilizare în ofertă
SI „Protecția Socială” / SI PS	Sistemul informațional nou propus pentru procesele CNAS de evidență, contribuții, cont individual, cereri, decizii, plăți, raportare, interoperabilitate, audit și suport operațional.
Functional Backbone	Modelul funcțional comun care leagă obiectele recurente ale sistemului: cerere, dosar, workflow, decizie, document, drept, plată, raportare, integrare și audit.
Shared Services / Shared Artefacts	Servicii și artefacte reutilizabile în mai multe domenii: notificări, documente, șabloane, registre, audit, raportare, integrare, workflow, administrare și configurări.
Readiness Gate	Punct formal de control înainte de trecerea într-o etapă sau acceptarea unui livrabil major; verifică existența dovezilor, nu doar finalizarea declarativă a activităților.
Delivery Assurance	Ansamblu de controale de livrare: planificare, demo, testare, registru decizii, registru riscuri, release package, pachet de evidențe și acceptanță pe livrabile.
Model Office	Mecanism de validare practică a fluxurilor cu utilizatori reprezentativi CNAS, scenarii reale și observații documentate înainte de extinderea soluției.
Integration Gateway / WSAdapter	Strat de integrare care controlează schimbul de date cu sisteme externe: contracte, transformări, jurnalizare, retry, erori, monitorizare și audit.
Migration Factory	Mecanism repetabil de migrare: profilare surse, mapping, staging, transformare, validare, încărcare, reconciliere, gestiune excepții și rerun controlat.
Reporting Data Factory	Mecanism de pregătire a datelor pentru rapoarte: structuri agregate, snapshot-uri, indicatori guvernați, audit de generare și verificări de control.
Release Package	Pachetul livrat la un release: versiune cod, build, scripturi DB, configurări, release notes, rezultate teste, instrucțiuni de instalare și rollback/forward-fix dacă scenariul tehnic o cere.
Evidence Package	Pachetul de dovezi pentru acceptanță: livrabil, versiuni, teste, rezultate, defecte, decizii, documente justificative și confirmări relevante.
Design Authority	Mecanism de control tehnic și funcțional al deciziilor de arhitectură, integrare, date, securitate, configurări și impact transversal.
SRS	Software Requirements Specification / document de cerințe funcționale și nefuncționale, rezultat al analizei și validării cerințelor.
SDD	Software Design Document / document de proiectare tehnică: arhitectură, model date, componente, API, securitate, deployment, operare și integrare.
UAT	User Acceptance Testing / testarea de acceptanță cu Beneficiarul, pe scenarii, date, rezultate și defecte documentate.
SLA	Service Level Agreement / niveluri de serviciu pentru suport, incidente, timpi de reacție/remediere, raportare și escaladare.
MCloud	Platforma tehnologică guvernamentală unde soluția trebuie să fie pregătită pentru desfășurare conform cerințelor autorităților competente.
MUD	Modelul Unitar de Design utilizat ca reper pentru coerență vizuală, accesibilitate și experiență de utilizare în sistemele guvernamentale.

2. Sinteză tehnică și ghid de verificare

2.1 Scopul acestei sinteze

Această secțiune are rolul de a orienta evaluatorul înainte de parcurgerea detaliată a ofertei tehnice. Ea explică ce sistem este propus, cum trebuie înțeles proiectul CNAS, cum se comportă soluția în procesele reale de lucru, cum va fi livrată și acceptată implementarea și unde se găsesc răspunsurile detaliate în restul documentației.

Sinteza nu înlocuiește matricea de conformitate, anexele tehnice, planul de implementare sau documentele de livrabile. Ea este harta de lectură a ofertei. Corpul principal explică soluția într-o formă narativă, ușor de urmărit de evaluatorii funcționali, tehnici și de achiziții, iar anexele vor demonstra acoperirea cerințelor, livrabilele, calendarul, arhitectura, migrarea, testarea, instruirea, suportul și alocarea echipei.

Propunerea este construită astfel încât întrebările principale — ce se livrează, cum funcționează, cum se controlează riscurile, cum se demonstrează acceptanța și cum rămâne sistemul operabil după lansare — primesc răspuns în documentul principal, iar detaliile verificabile sunt susținute prin anexe și evidențe.

2.2 Ce se propune

Se propune elaborarea și implementarea noului SI „Protecția Socială” ca platformă operațională integrată pentru activitatea CNAS. Sistemul nu este tratat ca o aplicație izolată pentru o singură categorie de prestații și nici ca o simplă înlocuire tehnologică a unor componente vechi. El este propus ca mecanism instituțional care leagă, într-un flux coerent și trasabil, plătitorii, contribuțiile, persoanele asigurate, contul individual, cererile, dosarele, deciziile, pensiile și prestațiile, plățile, raportarea, interoperabilitatea, auditul și suportul operațional.

Această poziționare este importantă deoarece proiectul CNAS are o natură diferită de un proiect software obișnuit. Sistemul va susține procese publice critice, volume mari de date, reguli cu impact legal și financiar, date personale sensibile, raportări instituționale, integrări cu alte sisteme guvernamentale și activități care trebuie să continue în timpul modernizării. Prin urmare, abordarea ofertată nu se limitează la construirea unor ecrane noi; ea organizează proiectarea într-o platformă controlabilă, verificabilă, auditată și transferabilă.

Valoarea soluției propuse este capacitatea de control. CNAS trebuie să poată urmări de unde provine o dată, ce regulă a fost aplicată, ce calcul a fost efectuat, ce decizie a rezultat, ce utilizator a intervenit, ce document a fost generat, ce plată a fost inițiată și ce informație a fost transmisă sau primită prin interoperabilitate. Acest control trebuie să existe atât în utilizarea zilnică a sistemului, cât și în audit, raportare, suport, remediere și dezvoltare ulterioară.

Sistemul existent va fi utilizat ca sursă de analiză, mapping, migrare și verificare a continuității operaționale. El nu va fi copiat ca model arhitectural. Logica validă va fi analizată, documentată și reimplementată în componente moderne, testabile și auditate, iar datele istorice și curente vor fi migrate prin mecanisme repetabile, cu validare și reconciliere.

2.3 Cum se comportă soluția în practică

Soluția este descrisă prin lanțuri operaționale, nu prin module izolate. Activitatea CNAS nu se oprește la limita unui ecran sau a unei baze de date: o contribuție poate influența contul individual, contul individual poate susține stabilirea unui drept, dreptul poate genera decizie, decizia poate genera plată, iar plata poate

fi recalculată, suspendată, reluată, raportată sau verificată ulterior. Oferta tratează aceste legături ca parte centrală a sistemului.

În zona plătitorilor și contribuțiilor, sistemul va susține evidența obligațiilor, achitărilor, restanțelor, soldurilor, istoricului și corelării cu persoanele asigurate. În zona persoanei asigurate, sistemul va consolida datele relevante pentru contul individual, stagiu, perioade, contribuții și drepturi. În zona cererilor, dosarelor și deciziilor, sistemul va susține depunerea, verificarea, completarea, calculul, aprobarea, emiterea documentelor și urmărirea statutului. În zona plăților, soluția va controla drepturile acordate, modificările, recalculările, suspendările, restabilirile, reținerile, restituirile și comenzile de plată. În zona raportării, soluția va produce rapoarte operaționale, statistice și analitice din date controlate, nu din prelucrări direct pe fluxurile tranzacționale critice.

Workflow-ul este tratat ca mecanism de control. Obiectele importante — cererea, dosarul, decizia, dreptul, plata, documentul, raportul, integrarea și solicitarea de suport — vor avea stări, responsabilități, acțiuni permise, termene, istoric și audit. Interfața va ghida utilizatorul, dar backend-ul va rămâne limita finală de validare și autorizare. O acțiune nepermisă nu trebuie să fie imposibilă doar pentru că butonul nu apare în ecran; ea trebuie să fie blocată și la nivel de serviciu.

Configurabilitatea este propusă acolo unde este sigură și utilă: nomenclatoare, șabloane, fluxuri operaționale, notificări, parametri administrativi, rapoarte și proceduri automate. Regulile critice care produc efecte juridice, financiare sau de securitate vor fi implementate controlat, testate și versionate. Această separare evită două extreme la fel de riscante: un sistem rigid, care cere dezvoltare pentru orice ajustare, și un sistem excesiv configurabil, în care reguli sensibile ajung să fie modificate informal în producție.

2.4 Arhitectura propusă și principiul de control tehnic

Arhitectura soluției este construită pe separarea responsabilităților. Interfața utilizatorului, serviciile de business, integrarea, procesările batch, raportarea, baza de date, auditul, observabilitatea și suportul operațional au roluri distincte. Această separare nu este o preferință tehnică abstractă, ci un răspuns la riscurile reale ale proiectului: volum mare de date, fluxuri critice, raportare grea, migrare complexă, dependențe de sisteme externe, cerințe stricte de securitate și necesitatea de operare pe termen lung.

Backend-ul va concentra regulile de business, validările, tranzacțiile, autorizarea, orchestrarea proceselor și auditul. Baza de date relațională va susține datele operaționale, istoricul, configurările, auditul și structurile pregătite pentru raportare. Procesările grele — migrare, importuri, recalculări, agregări, exporturi masive și rapoarte complexe — vor fi separate de fluxurile interactive, pentru ca activitatea utilizatorilor să nu fie blocată de operațiuni de durată. Stratul de integrare va controla contractele, transformările, timeouts, retry, jurnalizarea și monitorizarea schimburilor de date cu sisteme externe.

Soluția va fi pregătită pentru deployment controlat în medii separate, cu versionare, release notes, scripturi de bază de date, configurări externalizate, evidențe de testare și posibilitate de diagnostic. Un release nu va fi tratat ca simplă instalare, ci ca pachet verificabil care leagă codul sursă, build-ul, configurația, testele, documentația și artefactele de deployment.

Această abordare permite izolarea problemelor. Dacă o integrare este indisponibilă, sistemul trebuie să păstreze starea operațională clară. Dacă un raport rulează greu, fluxurile tranzacționale nu trebuie afectate necontrolat. Dacă un job batch eșuează, trebuie să existe stare, log, posibilitate de reluare și evidență. Dacă o acțiune este executată de un utilizator, trebuie să existe urmă auditabilă.

2.5 Migrare, phase-in și continuitate operațională

Migrarea nu este tratată ca import tehnic unic executat la final. Pentru SI „Protecția Socială”, migrarea este o activitate de inginerie a datelor și de pregătire operațională. Datele sursă vor fi profilate, mapate, transformate, validate, încărcate, reconciliate și acceptate pe evidențe. Migrarea finală trebuie să fie execuția controlată a unui mecanism deja testat prin rulări repetate, loturi pilot, rapoarte de calitate și corectarea excepțiilor.

Strategia de punere în producție propusă este phase-in controlat, nu big-bang nejustificat. Aceasta nu înseamnă exploatarea nedefinită a două sisteme concurente, ci trecerea etapizată către noul sistem, cu reguli clare privind sursa de adevăr, domeniile migrate, ferestrele de sincronizare, verificările comparative, instruirea utilizatorilor și pregătirea suportului. Acolo unde anumite componente trebuie lansate împreună pentru a evita inconsistența datelor, gruparea va fi documentată și justificată.

Niciun domeniu critic nu trebuie introdus în producție doar pentru că dezvoltarea software este finalizată. Lansarea trebuie să fie precedată de date migrate și reconciliate, integrări verificate, rapoarte validate, utilizatori instruiți, scenarii UAT executate, suport pregătit și decizie formală de readiness. Pentru un sistem CNAS, go-live-ul este o tranziție instituțională, nu o simplă operațiune de deployment.

2.6 Livrare, acceptanță și handover

Finalizarea proiectului nu va fi demonstrată doar prin prezentarea aplicației. Fiecare etapă importantă trebuie să lase evidențe: cerințe aprobate, design, model de date, model de securitate, contracte de integrare, plan de migrare, rapoarte de testare, scenarii UAT, defecte închise, rapoarte de performanță, documentație de instalare și operare, materiale de instruire, release notes, cod sursă și pachet de handover.

Oferta introduce o logică de readiness gates: design readiness, development readiness, migration readiness, UAT readiness, go-live readiness, support readiness și final acceptance readiness. Rolul acestor porți nu este birocratic. Ele previn trecerea formală într-o etapă pentru care sistemul, datele, utilizatorii, mediile, integrările sau suportul nu sunt pregătite demonstrabil.

La final, CNAS trebuie să primească un sistem operațional, nu doar aplicații instalate. Pachetul de predare trebuie să includă cod sursă, configurări, scripturi, documentație tehnică, ghiduri de utilizare, ghid de instalare și configurare, ghid de mentenanță, ghid de dezvoltator, ghid pentru arhivare și restabilire, runbook operațional, evidențe de testare, materiale de instruire și registru de schimbări. Transferul de cunoștințe va include explicații tehnice și operaționale privind arhitectura, datele, integrările, auditul, raportarea, migrarea, deployment-ul și suportul.

Suportul post-implementare este tratat ca serviciu organizat, nu ca disponibilitate informală a echipei de dezvoltare. Modelul propus include service desk, registru unic al solicitărilor, clasificare, SLA, trasabilitatea incidentelor, remedieri controlate, raportare periodică și actualizarea documentației atunci când sunt livrate schimbări sau remedieri.

2.7 Utilizarea documentului și trasee de verificare

Întrebarea	Răspunsul principal	Evidență / document suport
Ce sistem este propus?	Capitolul privind înțelegerea obiectului și modelul funcțional explică SI „Protecția Socială” ca platformă integrată CNAS.	Matricea de conformitate, descrierea funcțională, modelul operațional.

Întrebarea	Răspunsul principal	Evidență / document suport
Cum sunt acoperite procesele reale CNAS?	Capitolul funcțional descrie lanțurile operaționale: plătitori, contribuții, cont individual, cereri, dosare, decizii, plăți și raportare.	Matrice cerință-cu-cerință, scenarii funcționale, fluxuri aprobate în SRS/SDD.
Cum este controlată flexibilitatea sistemului?	Capitolul privind configurabilitatea și workflow-ul explică ce se configurează, ce rămâne logică implementată și cum se auditează schimbările.	Catalog configurări, workflow-uri, matrice roluri, evidență versiuni.
Cum va funcționa raportarea?	Capitolul privind raportarea explică separarea dintre date tranzacționale, structuri pregătite pentru raportare, șabloane și exporturi controlate.	Catalog rapoarte, șabloane, seturi de date, teste de performanță.
Cum este construită arhitectura?	Capitolul de arhitectură descrie componentele, separarea responsabilităților, backend-ul, baza de date, batch-ul, integrarea, deployment-ul și observabilitatea.	Diagramă arhitecturală, SDD, contracte API, documentație deployment.
Cum sunt gestionate integrările?	Capitolul de interoperabilitate descrie stratul de integrare, contractele, monitorizarea, jurnalizarea, retry și tratarea erorilor.	Catalog integrare, contracte API/SOAP/REST, teste de integrare.
Cum sunt protejate datele și acțiunile?	Capitolul de securitate descrie modelul rolurilor, permisiunilor, auditului, protecției datelor personale și controlului exporturilor.	Model securitate, matrice roluri, jurnal audit, teste de securitate.
Cum se face migrarea?	Capitolul de migrare și phase-in descrie migration factory, staging, validare, reconciliere, rerun și criterii de acceptanță.	Plan de migrare, mapping, rapoarte de reconciliere, error bucket.
Cum se lansează sistemul în producție?	Capitolul de go-live explică production rehearsal, readiness gates, pilotare, cutover și stabilizare.	Plan de punere în producție, checklist readiness, raport de stabilizare.
Cum se demonstrează acceptanța?	Capitolul de testare și UAT explică testele, scenariile, criteriile de acceptanță, defectele și evidențele.	Raport testare, UAT sign-off, defect log, protocol de acceptanță.
Cum se face instruirea și predarea?	Capitolul de instruire și handover descrie materialele pe roluri, ghidurile, codul sursă, runbook-ul și transferul tehnic.	Ghiduri, materiale training, cod sursă, repository, documentație tehnică.
Cum este asigurat suportul după lansare?	Capitolul de suport descrie service desk, SLA, registru solicitări, mentenanță, raportare și tranziția către exploatare.	SLA, registru suport, rapoarte lunare, proceduri service management.
Cum se controlează implementarea?	Capitolul de management descrie guvernanța, milestone-urile, riscurile, dependențele, deciziile și raportarea progresului.	Plan implementare, Gantt, registru riscuri, minute, rapoarte de progres.

Căi recomandate de lectură

Evaluatorul funcțional poate începe cu această sinteză, apoi cu modelul funcțional și operațional, configurabilitatea, workflow-ul, raportarea, migrarea și UAT. Acest traseu arată cum se transformă procesele CNAS în fluxuri, obiecte, stări, validări, decizii, plăți, rapoarte și audit.

Evaluatorul tehnic poate începe cu arhitectura, interoperabilitatea, securitatea, performanța, deployment-ul, migrarea și documentația tehnică. Acest traseu permite verificarea separării componentelor, a modului de integrare, a controlului datelor, a mecanismelor de audit, a operabilității și a transferabilității.

Evaluatorul responsabil de implementare și acceptanță poate urmări capitolele privind planul de implementare, testarea, UAT, readiness gates, go-live, stabilizarea, livrabilele și suportul. Acest traseu arată cum se trece de la analiză la sistem acceptat, fără a concentra riscul la final.

Evaluatorul de achiziții și conformitate poate folosi matricea de conformitate, matricea de livrabile, planul de implementare, secțiunea de proprietate/licențiere și capitolul de suport. Acest traseu permite verificarea faptului că propunerea este completă, non-comercială în corpul tehnic, verificabilă și aliniată cerințelor formale.

Orientare finală

Oferta trebuie citită ca propunere de implementare bazată pe evidențe. Ea nu se limitează la confirmarea cerințelor și nu tratează modernizarea CNAS ca exercițiu de rescriere tehnologică. Documentul arată cum cerințele devin produs operațional: fluxuri controlate, date reconciliate, decizii auditabile, plăți verificabile, raportare pregătită, integrări monitorizate, securitate aplicată în backend, utilizatori instruiți, cod și documentație predate, suport activat și acceptanță demonstrată.

Prin această abordare, Furnizorul se poziționează ca partener de implementare pentru un sistem critic de stat. Angajamentul principal este livrarea unei platforme CNAS funcționale, trasabile, operabile și transferabile, nu doar a unui set de componente software. Diferența trebuie să fie vizibilă în fiecare parte a ofertei: cerința este legată de soluție, soluția este legată de livrabil, livrabilul este legat de testare, iar acceptanța este legată de evidențe verificabile.

3. Înțelegerea obiectului și contextului CNAS

Capitolul integrează anexele funcționale, UC-urile, lanțurile operaționale și mecanismele de livrare asumate în capitolele ulterioare.

Acest capitol fixează interpretarea de bază a obiectului contractului. SI „Protecția Socială” nu este o aplicație izolată, un portal nou sau o simplă înlocuire tehnologică a unor sisteme istorice. Este platforma operațională prin care CNAS va administra date, procese, decizii, drepturi, plăți, documente, raportare, interoperabilitate și suport pentru domenii cu efect instituțional, financiar și social direct.

Înțelegerea obiectului pornește de la două niveluri complementare ale Caietului de sarcini. Primul nivel este reprezentat de cazurile de utilizare UC01–UC23, care definesc funcționalități formale ale sistemului. Al doilea nivel este reprezentat de anexele funcționale, care descriu procesele reale: plătitori și contribuții, persoane asigurate, cont individual, servicii publice pe evenimente, evidența plăților, registre, web-servicii, rapoarte și modele de documente. Oferta tratează ambele niveluri ca obligatorii.

Anexele funcționale nu sunt transformate în liste paralele de ecrane, iar UC-urile nu sunt reduse la o bifare formală. Ele vor fi unite printr-un model funcțional comun: obiecte operaționale, workflow-uri, sarcini, decizii, documente, notificări, plăți, raportare și audit. Această interpretare conduce restul ofertei: modelul funcțional, arhitectura, raportarea, securitatea, migrarea, testarea, instruirea și suportul sunt construite pentru a demonstra că procesele CNAS devin sistem operabil și verificabil.

3.1 Obiectul proiectului: platformă instituțională, nu aplicație de evidență

Obiectul proiectului este implementarea unui sistem integrat pentru procesele CNAS în care partea de venituri și contribuții, partea de persoane asigurate și cont individual, partea de cereri/dosare/decizii, partea de plăți și partea de raportare nu sunt tratate ca lumi separate. Evidența plătitorilor și contribuțiilor fundamentează datele contributive. Datele contributive și istoricul persoanei fundamentează contul individual. Contul individual, împreună cu alte date și verificări, fundamentează stabilirea drepturilor. Drepturile produc decizii, documente, plăți, modificări, rapoarte și audit.

Într-o aplicație administrativă simplă, un modul poate fi analizat relativ separat. În SI „Protecția Socială”, separarea mecanică pe module ar ascunde partea critică: legătura dintre datele de intrare, regulile aplicate, decizia emisă, plata efectuată și raportarea ulterioară. Din acest motiv, soluția este proiectată în jurul obiectelor operaționale și al ciclurilor lor de viață, nu în jurul unor meniuri independente.

Această poziționare este relevantă deoarece arată că Furnizorul nu tratează sistemul ca o colecție de funcții, ci ca infrastructură informațională instituțională. Un plătitor, o contribuție, o persoană asigurată, o cerere, o decizie, un drept sau o plată sunt obiecte cu surse, istoric, reguli, stări, documente, verificări și audit. Implementarea trebuie să le trateze ca atare.

3.2 Anexele funcționale ca descriere operațională a sistemului

Cerințele din anexele funcționale nu vor fi tratate ca material auxiliar sau ca detaliu care se descoperă doar după contractare. Ele reprezintă descrierea operațională detaliată a sistemului: domenii, procese, registre, evenimente, servicii publice, plăți, web-servicii, rapoarte și modele documentare. De aceea, anexele vor fi utilizate ca input direct pentru SRS, SDD, modelul de date, workflow-uri, catalogul de integrare, catalogul de rapoarte, catalogul de șabloane, scenariile de testare și UAT pack-ul.

Cazurile de utilizare UC01–UC23 rămân unitățile formale de verificare funcțională. Anexele arată însă unde și cum se activează aceste UC-uri în procese reale. De exemplu, UC-urile pentru cereri, formulare, examinare,

aprobare/respingere, notificare și jurnalizare nu sunt doar funcții generale; ele se regăsesc în servicii publice distincte, cu reguli și documente diferite. În același mod, UC-urile pentru registre, schimb de date, rapoarte și administrare trebuie citite prin procesele de plătitori, persoane asigurate, plăți, rapoarte și web-servicii.

Oferta principală va păstra descrierea lizibilă la nivel de domenii operaționale și lanțuri funcționale. Acoperirea detaliată a anexelor va fi susținută printr-o anexă separată de conformitate funcțională și scenarii operaționale, în format tabelar, în care fiecare proces/scenariu va fi mapat către UC-uri, obiecte informaționale, componente ale soluției, livrabile SRS/SDD, scenarii UAT și evidențe de acceptanță.

Grup funcțional din anexele ToR	Ce definește pentru SI „Protecția Socială”	Tratament în ofertă / mecanism propus
Plătitori și contribuții	Registrul plătitorilor, declarații, contribuții calculate și achitate, plăți, solduri, restituiri, penalități și insolvabili.	Domeniu operațional pentru venituri BASS, cu obiecte trasabile, istoric, validări, raportare, reconciliere și integrare cu surse externe.
Persoane asigurate și cont individual	Evidența persoanelor, contribuții individuale, perioade de activitate, inclusiv perioade realizate până la 01.01.1999, istoric de asigurare și extras de cont.	Obiect comun folosit în calculul drepturilor, pensii/prestații, verificări, migrare, raportare și audit.
Servicii publice pe evenimente	Naștere, securitate socială, dizabilitate, sănătate, deces, servicii conexe și alte procese de prestare a serviciilor publice.	Fluxuri cerere–dosar–verificare–calcul–decizie–document–notificare–plată/audit, cu reguli specifice pe domeniu și obiecte comune reutilizate.
Evidența plăților	Sume calculate și achitate, conturi de plată, comenzi, rețineri, restituiri, suspendări, recalculări și registre aferente.	Domeniu propriu de control operațional, integrat cu deciziile, batch processing, reporting layer, audit și reconciliere.
Registre instituționale	Registrul documentelor executorii, registrul deciziilor, registrul conturilor de plată, registrul comenzilor și alte structuri operaționale.	Modele de date și ecrane/reguli de lucru cu istoric, stare, drepturi de acces, export controlat, audit și testare UAT pe registre.
Web-servicii expuse și consumate	Schimb de date cu sisteme externe și instituții publice, prin servicii expuse/consumate, payload-uri, erori și răspunsuri.	Integration Gateway, contracte API, timeout/retry, circuit breaker, snapshot de răspuns, audit și scenarii negative de testare.
Rapoarte	Listă preliminară de rapoarte operaționale, statistice, analitice și exporturi.	Reporting layer, data marts, snapshot-uri, catalog indicatori, guvernanța șabloanelor, audit de generare și teste pe valori de control.
Modele de cereri, decizii și documente	Formulare, decizii, rapoarte și documente oficiale care trebuie generate, păstrate și urmărite.	Șabloane versionate, document service, metadate, generare, semnare pentru documentele sau procesele care o solicită, notificare, arhivare și audit.

3.3 Domenii operaționale principale

Procesele privind plătitorii și contribuțiile nu vor fi tratate ca un registru simplu de entități. Ele controlează relația dintre plătitor, declarație, obligație, contribuție calculată, contribuție achitată, sold, restanță, penalitate, restituire și stare specială, inclusiv insolvabilitate. Aceste obiecte trebuie să fie trasabile, istorice

și verificabile, deoarece ele influențează atât raportarea BASS, cât și datele utilizate ulterior pentru persoane asigurate și drepturi.

Modelul de date și fluxurile operaționale păstrează legătura dintre datele de intrare, sursa lor, perioada de referință, modificările ulterioare și efectul asupra evidenței. O contribuție nu va fi doar o sumă într-un tabel; va fi un obiect legat de plătitor, perioadă, tip, sursă, stare, eventuale corecții și reconciliere. Acest model permite verificarea ulterioară a modului în care un sold, o datorie, o plată sau o informație contributivă a fost produsă.

Pentru implementare, domeniul contribuțiilor va fi legat de modelul de date, procesele batch, integrările, raportarea, migrarea și scenariile de testare. În UAT nu va fi suficientă afișarea unui registru; trebuie validate fluxuri complete: înregistrare/actualizare plătitor, preluare/validare declarație, calcul/achitare, corecție, reconciliere, raportare și audit.

Persoana asigurată și contul individual: obiect comun pentru drepturi, verificări și istoric

Domeniul persoanelor asigurate este unul dintre punctele de legătură dintre evidența contribuțiilor și stabilirea drepturilor. Persoana asigurată, contul individual, contribuțiile pe persoană, perioadele de activitate și istoricul de asigurare nu sunt date auxiliare. Ele formează baza pentru verificări, calcul, decizii, rapoarte și explicații ulterioare ale sistemului.

Oferta tratează contul individual ca obiect comun, nu ca ecran izolat. Acesta trebuie să poată agrega date din surse istorice și curente, să păstreze perioade, să explice sursa și să fie utilizat controlat în fluxurile de pensii, prestații, verificări, rapoarte și migrare. Perioadele istorice, inclusiv cele realizate înainte de 01.01.1999, trebuie tratate cu reguli clare de mapping, validare și păstrare a provenienței.

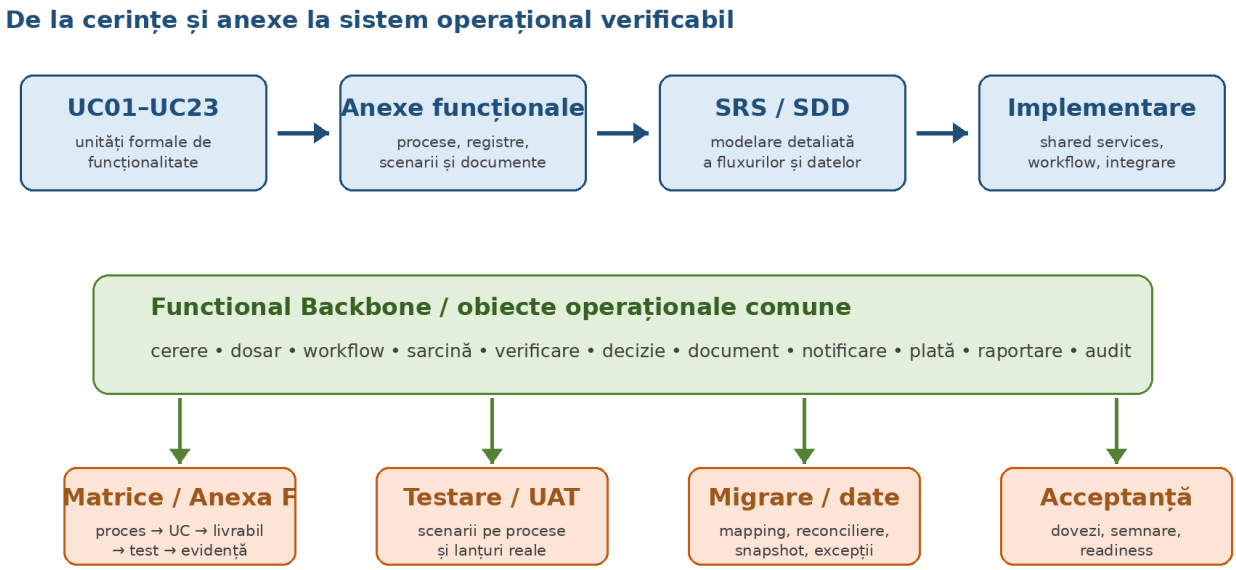
Această abordare protejează proiectul de un risc major: calculul drepturilor pe date insuficient explicabile. Pentru CNAS, nu este suficient ca sistemul să arate un rezultat; trebuie să poată indica datele și perioadele pe care s-a sprijinit rezultatul. De aceea, modelul de persoană asigurată și cont individual va fi conectat la migrare, data quality, audit, raportare și UAT.

Serviciile publice pe evenimente: de la formular la decizie și efect operațional

Anexele privind serviciile publice confirmă că sistemul trebuie să susțină familii de procese, nu doar formulare electronice. Evenimentele Naștere, Securitate socială, Dizabilitate, Sănătate, Deces, Servicii conexe și Evidența plăților descriu situații operaționale diferite, dar toate folosesc un set comun de obiecte instituționale: solicitant, cerere, dosar, documente, verificări, sarcini, calcule, decizii, drepturi, notificări, plăți și audit.

Functional Backbone-ul comun este utilizat pentru aceste obiecte, fără a forța toate serviciile într-un flux artificial unic. Fiecare domeniu va păstra reguli, documente, condiții de eligibilitate, verificări și decizii specifice. Mecanismele comune — cerere, dosar, workflow, sarcină, decizie, document, notificare, audit — vor asigura coerență, reutilizare și administrare unitară.

Această separare este importantă pentru exploatare. Utilizatorul trebuie să lucreze cu fluxuri adaptate procesului real, nu cu un generic greu de utilizat. În același timp, CNAS trebuie să evite trei implementări diferite pentru aceleași concepte: o cerere în pensii, o cerere în beneficii și o cerere în alt serviciu nu trebuie să aibă modele incompatibile de audit, documente, stări sau notificări.



Evidența plăților și registrele

Plata nu va fi tratată ca simplu rezultat final al unei decizii. Anexele arată că evidența plăților are propriile procese, registre și efecte: sume calculate și achitate, conturi de plată, comenzi, restituiri, suspendări, rețineri, corecții, reconciliere și raportare. Din acest motiv, plata este tratată ca domeniu operațional propriu, legat de drepturi și decizii, dar controlat prin mecanisme dedicate.

Registrele de documente executorii, decizii, conturi de plată și comenzi vor fi tratate ca structuri instituționale cu stare, drepturi de acces, istoric, audit și raportare. Ele nu vor fi simple tabele de afișare. Fiecare registru trebuie să fie conectat la procesul care îl alimentează, la documentele aferente, la efectele asupra plăților și la evidențele necesare pentru suport, audit și acceptanță.

Această abordare reduce riscul de necorelare între decizie, drept, plată și raportare. Sistemul trebuie să poată explica de ce o sumă a fost calculată, ce decizie a stat la bază, ce comandă sau cont de plată a fost afectat, ce modificări au intervenit și ce raport a reflectat situația.

Interoperabilitate, rapoarte și documente: ieșiri oficiale din procese controlate

Web-serviciile expuse și consumate nu vor fi tratate ca simple conexiuni tehnice. Ele sunt parte a proceselor CNAS. Un apel extern poate valida o cerere, poate completa un profil, poate confirma o stare, poate bloca sau permite o acțiune, poate alimenta un raport sau poate susține o decizie. De aceea, schimbul de date este controlat prin Integration Gateway, contracte, tratarea erorilor, timeout/retry, circuit breaker, snapshot de răspuns și audit de schimb de date.

Rapoartele și documentele sunt ieșiri oficiale ale sistemului, nu exporturi ad-hoc. Rapoartele vor fi legate de surse de date controlate, data marts, snapshot-uri, indicatori, valori de control și audit de generare. Documentele și deciziile vor fi legate de șabloane versionate, metadate, limbă, semnare pentru documentele sau procesele care o solicită, notificare, arhivare și acces controlat.

Această poziționare este esențială pentru sistemele publice. Un raport sau o decizie trebuie să poată fi explicată ulterior: din ce date s-a generat, ce versiune de șablon a folosit, ce reguli au fost aplicate, cine a generat-o, ce parametri au fost utilizați și dacă ulterior a existat o rectificare sau o versiune nouă.

3.4 Problemele reale pe care sistemul trebuie să le rezolve

Modernizarea CNAS nu poate fi redusă la implementarea unor ecrane moderne peste date vechi. Problemele reale sunt mai adânci: fragmentarea logicii, lipsa trasabilității complete, dependența de operațiuni manuale, raportarea nereproductibilă, intervențiile directe în date, dificultatea de a reconstitui o decizie, migrarea istorică, plățile și corecțiile ulterioare, integrările lente sau indisponibile și necesitatea de suport după go-live.

Răspunsul tehnic la aceste probleme se bazează pe mecanisme asumate în capitolele următoare: Functional Backbone pentru obiecte comune, Shared Services pentru reutilizare, Reporting Data Factory pentru rapoarte și indicatori, Integration Gateway pentru schimb de date, Migration Factory pentru date istorice, Delivery Assurance pentru progres pe evidențe, observabilitate pentru operare și securitate multi-layer pentru date personale și acțiuni sensibile.

Această abordare protejează atât CNAS, cât și Furnizorul. CNAS primește un sistem care poate fi explicat și verificat. Furnizorul livrează pe criterii controlabile, nu pe interpretări informale. Acceptanța nu se sprijină doar pe demonstrații vizuale, ci pe cerințe, procese, date, teste, documentație și evidențe.

Risc de interpretare sau implementare	Cum îl controlează oferta
Anexele sunt tratate ca material secundar	Anexele devin input pentru SRS/SDD, model de date, workflow, catalog de rapoarte, catalog API, testare.
UC-urile sunt livrate ca funcții izolate	UC-urile sunt mapate la lanțuri operaționale și obiecte comune: cerere, dosar, decizie, document, plată, raportare și audit.
Procesele de plată sunt văzute doar ca rezultat final	Plățile, conturile, comenzile și reconcilierea sunt tratate ca domeniu operațional propriu, cu batch, audit și raportare.
Raportarea rămâne SQL manual sau export punctual	Rapoartele se bazează pe reporting layer, data marts, snapshot-uri, indicatori guvernați și audit de generare.
Migrarea este tratată ca import tehnic	Migrarea devine migration factory: profilare, mapping, staging, validare, error bucket, reconciliere, dress rehearsal și sign-off.
CNAS validează prea târziu sensul proceselor	Incrementuri lunare, Model Office, review SRS/SDD, decision log și UAT pe procese/anexe reduc riscul de interpretare greșită.

3.5 Principii de soluție, rol CNAS și rezultat urmărit

În baza acestei interpretări, oferta asumă câteva principii de soluție care vor rămâne constante pe tot parcursul proiectului.

Functional Backbone comun: Cererile, dosarele, deciziile, documentele, notificările, plățile, rapoartele și auditul se construiesc pe mecanisme comune, cu reguli specifice pe domeniu.

Shared Services și Shared Artefacts: Obiectele și serviciile recurente nu vor fi reinventate separat în contribuții, pensii și beneficii; ele vor fi livrate, versionate și reutilizate controlat.

Date explicabile și raportare reproductibilă: Datele operaționale, istoricul, snapshot-urile, data marts și indicatorii guvernați vor permite reconstituirea rapoartelor și deciziilor.

Integrare controlată: Schimbul de date se va realiza prin contracte, gateway, snapshot, audit, tratarea erorilor și scenarii negative, nu prin apeluri izolate în fiecare modul.

Migrare repetabilă: Datele istorice vor fi mutate prin profilare, mapping, staging, transformare, reconciliere și rulări repetate, nu prin import unic la final.

Acceptanță pe evidențe: Procesele, UC-urile, anexele, datele, rapoartele, securitatea și operabilitatea vor fi confirmate prin teste, documentație, demo-uri și pachete de evidențe.

Corpul ofertei

Oferta principală nu va relua integral anexele caietului de sarcini. Aceasta ar face documentul greu de citit și ar ascunde mesajul de soluție. În corpul ofertei, anexele sunt reflectate prin domenii operaționale, lanțuri funcționale, shared services, arhitectură, migrare, raportare, securitate, testare și acceptanță.

Acoperirea detaliată va fi prezentată într-o anexă separată — Matrice de conformitate funcțională și scenarii operaționale. Această anexă va permite filtrarea pe anexă ToR, proces, eveniment, obiect informațional, UC asociat, componentă de soluție, livrabil, test/UAT și evidență de acceptanță.

Această separare este intenționată. Documentul principal arată cum Furnizorul înțelege sistemul și ce mecanism propune. Anexa va arăta punctual cum fiecare proces și scenariu descris în caiet este urmărit de la cerință până la implementare, testare și acceptanță.

Rolul CNAS în confirmarea proceselor și datelor

CNAS nu va fi tratată ca observator pasiv al implementării. Procesele, datele, prioritățile, excepțiile și acceptanța aparțin autorității contractante. Furnizorul va pregăti analiza, variantele de implementare, impactul tehnic, documentația, testele și evidențele; CNAS va valida sensul funcțional, interpretările, prioritățile, excepțiile de date și readiness-ul etapelor.

Acest rol este deosebit de important pentru anexele funcționale. Unele reguli pot fi explicite în caiet, altele pot necesita clarificare în SRS/SDD, iar unele excepții vor apărea doar prin profilarea datelor sau testarea fluxurilor. Furnizorul nu va presupune unilateral reguli instituționale acolo unde este necesară decizia CNAS. Deciziile vor fi înregistrate, legate de cerințe și utilizate în implementare, testare și acceptanță.

Prin această metodă, clarificările nu rămân în discuții informale. Ele intră în decision log, în SRS/SDD, în backlog, în test cases și în pachetul de acceptanță.

Rezultatul urmărit pentru CNAS

Rezultatul proiectului trebuie să fie un sistem în care CNAS poate lucra, verifica și explica. Poate lucra, pentru că fluxurile, rolurile, sarcinile, documentele și registrele sunt organizate. Poate verifica, pentru că datele, calculele, rapoartele, integrările și migrările au evidențe. Poate explica, pentru că fiecare decizie, plată, modificare, raport sau export relevant este legat de surse, reguli, acțiuni și audit.

Aceasta este diferența dintre o implementare formală și o modernizare reușită. O implementare formală livrează funcționalități. O modernizare reușită livrează control instituțional: asupra datelor, asupra fluxurilor, asupra deciziilor, asupra plăților, asupra raportării, asupra securității și asupra operării post-lansare.

Capitolul 2 fixează această interpretare. Capitolele următoare arată cum ea este transformată în model funcțional, configurabilitate, raportare, arhitectură, securitate, migrare, testare, instruire, suport și transferabilitate. Anexele asigură nivelul detaliat de conformitate pe procese și scenarii. În acest mod, oferta rămâne clară pentru citire și verificabilă pentru acceptanță.

4. Model funcțional, UC-uri și anexe funcționale

Acest capitol este secțiunea funcțională principală a ofertei. El arată ce cumpără CNAS din punct de vedere funcțional, cum sunt acoperite cazurile de utilizare din caietul de sarcini și cum aceste funcționalități lucrează împreună într-un sistem operațional coerent. Capitolul nu înlocuiește matricea de conformitate cerință-cu-cerință, dar fixează răspunsul funcțional al ofertei: UC01-UC23 sunt acoperite ca funcții contractuale, iar lanțurile operaționale explică modul în care ele devin produs utilizabil în activitatea reală CNAS.

Ideea centrală este simplă: CNAS nu primește doar 23 de ecrane sau 23 de funcții separate. CNAS primește o platformă în care accesul public, dashboardurile, sarcinile, cererile, formularele, registrele, schimbul de date, rapoartele, configurarea, notificarea și jurnalizarea lucrează împreună. Fiecare UC are valoare proprie, dar valoarea sistemului apare atunci când UC-urile sunt legate corect: o cerere ajunge în sarcină, sarcina produce examinare, examinarea poate cere date externe, decizia generează document și notificare, iar toate acțiunile rămân jurnalizate.

4.1 Relația dintre UC-urile ToR și modelul funcțional propus

Caietul de sarcini definește 23 de cazuri de utilizare. Acestea sunt unitățile funcționale contractuale ale sistemului: ele indică ce trebuie să poată face utilizatorii, administratorii, sistemele externe și procesele automate. Oferta răspunde explicit la această structură și tratează UC01-UC23 ca bază pentru proiectare, implementare, testare și acceptanță.

Lanțurile operaționale nu înlocuiesc UC-urile. Ele explică de ce UC-urile nu trebuie livrate ca insule. În exploatarea CNAS, un utilizator nu „consumă” UC-uri izolate; el pornește din dashboard, primește o sarcină, accesează o cerere sau un registru, verifică documente, aprobă sau respinge, generează documente, primește notificări și lasă urme de audit. Prin urmare, UC-urile sunt unitățile verificabile ale cerinței, iar lanțurile sunt unitățile de funcționare ale produsului.

Această abordare protejează oferta de două riscuri: pe de o parte, riscul de a transforma capitolul funcțional într-o listă mecanică de cerințe; pe de altă parte, riscul de a rămâne la un nivel prea conceptual. În documentul principal, UC-urile sunt grupate pe capabilități și fluxuri, iar în matricea de conformitate fiecare CF aferent va fi mapat către răspuns, livrabil și criteriu de acceptanță.

Caz de utilizare ToR	Funcționalitate contractată	Rol în modelul operațional propus
UC01 - Explorez conținut interfață publică	Interfață publică accesibilă utilizatorilor Internet și utilizatorilor autentificați, cu date publice, date depersonalizate, informații despre servicii și documente, rapoarte statistice și indicatori.	Asigură stratul de transparență și informare publică, separat de zona operațională internă și alimentat din date aprobate, organizate și controlate.
UC02 - Accesez servicii informative	Acces la servicii informative CNAS, explicații, criterii, rezultate consultative sau informații disponibile fără inițierea unui flux complet de cerere.	Transformă portalul public din pagină statică în punct de intrare pentru beneficiari, reducând solicitările repetitive și orientând utilizatorul spre serviciul potrivit.
UC03 - Caut/vizualizez date	Căutare, filtrare, sortare și vizualizare date conform metadatelor și drepturilor de acces.	Este mecanismul de consultare controlată utilizat în portal, registre, dashboarduri și fluxurile interne, cu reguli de vizibilitate pe rol și context.
UC04 - Utilizez dashboard	Dashboarduri pe roluri, indicatori, notificări, sarcini, obiecte în lucru și navigare către acțiuni relevante.	Este intrarea operațională a utilizatorului autorizat; sistemul nu obligă utilizatorul să caute manual munca, ci îi prezintă coada de lucru și prioritățile.

Caz de utilizare ToR	Funcționalitate contractată	Rol în modelul operațional propus
UC05 - Execut sarcini	Preluare, executare, finalizare, repartizare sau urmărire sarcini generate de fluxuri de lucru.	Leagă workflow-ul de activitatea zilnică: fiecare cerere, document sau aprobare se transformă în sarcină responsabilizată și auditabilă.
UC06 - Depunere cerere	Depunerea cererilor prin canale disponibile, cu identificare solicitant, date necesare, documente atașate și inițiere de flux.	Deschide lanțul de prestare a serviciului public: cererea devine obiect operațional, nu doar formular salvat.
UC07 - Înregistrare formular	Înregistrarea formularului electronic sau intern, completarea metadatelor, validări inițiale și atașarea la proces.	Asigură intrarea controlată a datelor în sistem și reduce riscul ca formularul să circule ca document fără stare, proprietar și reguli.
UC08 - Examinare document	Verificarea documentelor, completitudinii, validității, coerenței și legăturii cu cererea/formularul.	Transformă verificarea documentară într-o etapă urmărită, cu rezultat, observații, solicitări de completare și audit.
UC09 - Extrag rapoarte	Extracție rapoarte, indicatori și date pentru utilizatorii autorizați, conform rolurilor și parametrilor disponibili.	Oferă vizibilitate operațională fără acces brut la baza de date; rapoartele sunt produse controlate.
UC10 - Aprob/resping	Aprobarea sau respingerea documentelor, formularelor, cererilor sau altor obiecte de flux conform rolului și stării.	Este punctul de decizie din flux: acțiunea trebuie să fie permisă de rol, stare, reguli și context, apoi păstrată în istoric.
UC11 - Descarc document	Descărcare documente generate sau disponibile: certificate, extrase, rapoarte, decizii, formulare, rezultate publice sau interne.	Închide multe fluxuri prin livrarea rezultatului către solicitant, utilizator intern sau public, cu audit pentru documente sensibile.
UC12 - Explorez registru	Consultarea registrelor gestionate de sistem, inclusiv plătitori, persoane asigurate, solicitări, documente sau alte obiecte informaționale.	Oferă acces controlat la baza operațională a CNAS; registrul devine instrument de lucru, nu doar depozit de date.
UC13 - Gestionez profilul solicitantului	Crearea, actualizarea și consultarea profilului solicitantului, cu date de identificare, contacte, istoric și legături cu cereri/documente.	Leagă persoana de interacțiunile sale cu CNAS și permite reutilizarea controlată a datelor în servicii succesive.
UC14 - Schimb date cu sisteme externe	Schimb de date și documente cu sisteme externe prin servicii guvernamentale și integrări dedicate.	Introduce date oficiale în fluxuri fără copiere informală; fiecare schimb are contract, stare, rezultat, eroare, metadate și audit.
UC15 - Configurez serviciu electronic	Configurarea serviciilor electronice: formulare, câmpuri, documente, reguli, canale, vizibilitate, parametri și activare.	Permite extinderea portofoliului de servicii CNAS fără intervenții necontrolate în cod sau bază de date.
UC16 - Configurez flux de lucru	Configurarea fluxurilor: stări, tranziții, roluri, acțiuni, termene, notificări și reguli operaționale unde este sigur.	Transformă workflow-ul în mecanism de guvernanță: obiectele avansează doar prin pași autorizați și explicați.
UC17 - Gestionez metadate și șabloane de documente	Administrarea metadatelor, nomenclatoarelor, clasificatoarelor, șabloanelor de documente și parametrilor asociați.	Asigură consistența datelor, documentelor și rapoartelor prin versiuni, proprietar, aprobare și istoric.
UC18 - Administrez utilizatori și controlul accesului	Administrarea utilizatorilor, rolurilor, grupurilor, permisiunilor și accesului la funcții/date.	Aplică principiul privilegiului minim și face diferența dintre autentificare, rol operațional, acțiune permisă și acces la date.

Caz de utilizare ToR	Funcționalitate contractată	Rol în modelul operațional propus
UC19 - Generez rapoarte și documente	Generarea documentelor și rapoartelor oficiale din șabloane și date controlate.	Produce ieșirile oficiale ale sistemului: decizii, extrase, certificate, rapoarte și documente verificabile.
UC20 - Execut proceduri automate	Execuția procedurilor automate: importuri, sincronizări, agregări, notificări, procesări recurente, recalculări sau alte joburi.	Mută procesele repetitive și de volum în execuții controlate, cu stare, rezultat, reluare și raport de excepții.
UC21 - Procesare cerere/formular	Procesarea cererilor și formularelor după depunere/înregistrare: validări, completări, repartizare, examinare, calcul, decizie.	Este nucleul prestării serviciului public; aici cererea devine dosar operațional și produce rezultat instituțional.
UC22 - Notific utilizatori	Notificarea utilizatorilor interni și externi prin dashboard, email/MNotify și alte canale disponibile, în funcție de evenimente.	Leagă sistemul de utilizator în timp real: sarcini, termene, rezultate, aprobări, probleme și acțiuni necesare nu rămân invizibile.
UC23 - Jurnalizez evenimente	Jurnalizarea evenimentelor de business: autentificare, accesare/modificare date, cereri, examinări, sarcini, documente, aprobări, configurări, integrări, rapoarte și interogări.	Este memoria verificabilă a sistemului. Fără UC23, fluxurile există doar operațional; cu UC23, ele devin auditabile și explicabile.

Pe lângă UC01–UC23, Furnizorul va trata anexele funcționale ale Caietului de sarcini ca sursă obligatorie pentru proiectarea, implementarea, testarea și acceptanța SI „Protecția Socială”. Procesele aferente plătitorilor de contribuții, contribuțiilor calculate și achitate, persoanelor asigurate, contului individual, serviciilor publice prestate pe evenimente, evidenței plăților, registrelor, web-serviciilor, rapoartelor și modelelor de documente vor fi transformate în cerințe detaliate, scenarii de implementare, reguli de date, workflow-uri, teste și criterii de acceptanță.

Oferta principală descrie aceste procese la nivel de domenii operaționale și lanțuri funcționale, pentru a păstra documentul lizibil și orientat spre soluție. Acoperirea detaliată va fi prezentată într-o anexă separată de conformitate funcțională și scenarii operaționale, în format tabelar, în care fiecare proces/scenariu va fi mapat către UC-uri, obiecte informaționale, componente ale soluției, livrabile SRS/SDD, scenarii UAT și evidențe de acceptanță.

Această abordare permite păstrarea unei oferte principale clare, fără pierderea trasabilității. CNAS va putea verifica atât viziunea funcțională integrată a sistemului, cât și acoperirea punctuală a proceselor și scenariilor descrise în anexele caietului de sarcini. Furnizorul își asumă că anexele nu sunt tratate ca material informativ secundar, ci ca input funcțional obligatoriu pentru proiectarea detaliată și verificarea sistemului livrat.

Tabelul de mai jos marchează modul în care anexele funcționale sunt absorbite în modelul operațional al soluției. Scopul nu este reluarea anexelor în corpul ofertei, ci demonstrarea faptului că fiecare anexă are un loc clar în arhitectura funcțională, în modelul de date, în mecanismele de workflow, în integrări, în raportare și în scenariile de acceptanță.

În faza SRS/SDD, această hartă va fi detaliată prin registrul de procese și scenarii, astfel încât fiecare proces descris în caiet să fie urmărit de la cerință până la implementare și testare. În acest mod, funcționalitatea nu rămâne la nivel de afirmație generală, ci devine trasabilă prin obiecte, reguli, componente, teste și evidențe.

Anexă ToR	Domeniu operațional	Obiecte principale	UC-uri asociate	Evidență în ofertă / livrabile
Anexa 1	Plătitori, contribuții calculate și contribuții achitate	plătitor, declarație, obligație, contribuție, plată, sold, restanță, insolvabil	UC12–UC14, UC20, UC23	model date, fluxuri contribuții, reporting, reconciliere, UAT contribuții
Anexa 2	Persoane asigurate, cont individual, contribuții pe persoană și perioade istorice	persoană asigurată, cont individual, stagiu, contribuție persoană, perioadă istorică	UC12–UC14, UC19, UC23	registru persoane, cont individual, migrare istorică, teste date/stagiu
Anexa 3	Servicii publice pe evenimente: naștere, securitate socială, dizabilitate, sănătate, deces, servicii conexe și plăți	cerere, dosar, verificare, calcul, decizie, drept, plată, document, notificare	UC06–UC11, UC20–UC23	workflow, shared artefacts, scenarii UAT, documente/decizii
Anexa 4	Web-servicii expuse	API, serviciu public/instituțional, contract, payload, autentificare, audit	UC14, UC23	catalog API, contracte, teste integrare, audit schimb date
Anexa 5	Web-servicii consumate	sistem extern, verificare, răspuns, snapshot, timeout, retry, eroare controlată	UC14, UC20, UC23	Integration Gateway, scenarii negative, contract tests
Anexa 6	Rapoarte	raport, indicator, data mart, snapshot, export, parametri, audit generare	UC09, UC19, UC23	catalog rapoarte, data products, teste valori de control
Anexa 7	Modele de cereri, decizii și rapoarte	șablon, document, metadate, versiune, limbă, semnare, generare	UC17, UC19, UC21, UC22, UC23	guvernanță șabloane, catalog documente, teste generare

4.2 Gruparea funcțională a UC-urilor

Pentru a fi evaluabil, capitolul păstrează vizibilă lista UC. UC-urile sunt grupate în capabilități funcționale. Această grupare permite simultan acoperirea formală și logica sistemului. Fiecare grup are obiecte operaționale, actori, rezultate, controale și evidențe de acceptanță.

Grup funcțional	UC-uri incluse	Ce livrează sistemul	Evidență de acceptanță
Interfață publică și servicii informative	UC01, UC02, UC03, UC11	Acces public, servicii informative, căutare/vizualizare și descărcare documente/date permise.	Portal public, rezultate căutare, conținut public/depersonalizat, documente descărcabile, reguli de publicare.
Spațiu de lucru operațional	UC04, UC05, UC22	Dashboard, notificări, sarcini, termene, obiecte în lucru și navigare către acțiuni.	Dashboard pe rol, cozi de lucru, task history, notificări cu link către obiect.
Prestarea serviciilor publice	UC06, UC07, UC08, UC10, UC21, UC11, UC22, UC23	Depunere cerere, înregistrare formular, examinare documente, aprobare/respingere, procesare, documente, notificare și audit.	Flux cerere-formular-dosar-decizie, stări, tranziții, documente, notificări, jurnal business.
Registre și profil solicitant	UC03, UC12, UC13, UC14, UC23	Consultare registre, profil solicitant, legături cu surse externe și urmărire istoric.	Registre accesibile pe rol, profil solicitant, snapshoturi date externe, audit acces/modificare.

Grup funcțional	UC-uri incluse	Ce livrează sistemul	Evidență de acceptanță
Configurare și administrare	UC15, UC16, UC17, UC18, UC23	Configurare servicii, fluxuri, metadate, șabloane, utilizatori și drepturi.	Catalog configurări, versiuni, aprobări, matrice drepturi, jurnal configurări.
Raportare, documente și proceduri automate	UC09, UC19, UC20, UC22, UC23	Extragere rapoarte, generare documente, joburi automate, notificări și audit.	Catalog rapoarte/documente, șabloane, execuții batch, loguri, rezultate și rapoarte de excepții.

4.3 Procese utilizator, cereri și lucru operațional

UC01, UC02, UC03 și UC11 formează zona prin care sistemul comunică cu publicul și cu utilizatorii care au nevoie de informații fără a intra direct în procese interne. Această zonă nu este un simplu site de prezentare. Ea este stratul controlat prin care datele publice, datele depersonalizate, informațiile despre servicii, indicatorii și documentele permise devin accesibile într-o formă organizată, căutabilă și inteligibilă.

Pentru UC01, sistemul va furniza o interfață publică accesibilă utilizatorilor Internet și utilizatorilor autentificați. Conținutul public va fi structurat pe servicii, categorii de date, documente eliberate, rapoarte statistice și indicatori, cu separare clară față de datele operaționale interne. Publicarea nu va expune direct tabele sau obiecte tranzacționale, ci seturi de date și informații aprobate pentru diseminare.

Pentru UC02, serviciile informative vor ghida utilizatorul spre datele relevante și spre pașii necesari pentru accesarea serviciilor CNAS. În loc ca utilizatorul să caute în descrieri statice, sistemul va permite prezentarea serviciilor prin criterii, instrucțiuni, documente necesare, rezultate posibile și legături către cereri sau formulare acolo unde fluxul continuă către prestarea unui serviciu public.

Pentru UC03, căutarea și vizualizarea datelor vor funcționa pe criterii definite prin metadatele sistemului. Rezultatele vor fi filtrate și sortate conform criteriilor permise, iar vizualizarea va respecta diferența dintre utilizator anonim, solicitant autentificat, utilizator CNAS și rol administrativ. Același principiu se aplică și în registre: căutarea nu este acces liber la toate datele, ci mecanism controlat de consultare.

Pentru UC11, descărcarea documentelor va fi tratată ca acțiune de sistem, nu ca simplu link către fișier. Documentele publice pot fi descărcate fără autentificare acolo unde regimul lor permite. Documentele aferente cererilor, deciziilor, rapoartelor interne sau datelor sensibile vor fi disponibile numai în contextul și rolul autorizat. Accesarea și descărcarea documentelor relevante vor fi jurnalizate unde conținutul sau contextul o impune.

Dashboard, sarcini și lucru operațional zilnic

UC04 și UC05 sunt esențiale pentru ca sistemul să nu fie doar o arhivă de date cu formulare. Dashboardul și sarcinile transformă sistemul în spațiu de lucru. Utilizatorul CNAS, șeful direcției, șeful CNAS, administratorul sau alt rol autorizat trebuie să vadă ce are de făcut, ce este întârziat, ce necesită aprobare, ce a fost repartizat și ce rezultate au fost generate.

UC04 va fi implementat ca dashboard pe roluri și contexte, nu ca pagină universală identică pentru toți. Un utilizator care examinează documente trebuie să vadă cereri/documente de verificat. Un responsabil de aprobare trebuie să vadă obiecte pregătite pentru aprobare/respingere. Un manager trebuie să vadă indicatori de volum, termene, restanțe și progres. Administratorul trebuie să vadă starea configurărilor, joburilor sau incidentelor relevante. Aceeași aplicație are intrări diferite, dar reguli comune de securitate și audit.

UC05 va gestiona sarcina ca obiect operațional. O sarcină are sursă, tip, obiect aferent, responsabil, termen, stare, acțiuni disponibile, rezultat și istoric. Sarcinile pot proveni din depunerea unei cereri, înregistrarea unui formular, necesitatea examinării documentelor, aprobări, notificări, proceduri automate, erori de integrare sau activități administrative. Sistemul trebuie să arate nu doar că o sarcină există, ci cine o are, de când, ce poate face și ce rezultat a produs.

Această zonă este locul unde lanțurile devin vizibile pentru utilizator. Fără dashboard și sarcini, fluxurile rămân descrieri de proces. Cu UC04 și UC05 implementate corect, sistemul conduce utilizatorul către acțiunea potrivită și reduce riscul de dosare uitate, documente neexaminate, termene depășite sau aprobări blocate.

Cereri, formulare, documente, aprobări și procesare

UC06, UC07, UC08, UC10 și UC21 constituie nucleul funcțional al prestării serviciilor publice. Aici sistemul trebuie să arate că înțelege activitatea CNAS: o solicitare nu este doar un formular completat, ci începutul unui dosar operațional care are date, documente, verificări, sarcini, reguli, decizii, documente generate, notificări și audit.

UC06 va permite depunerea cererii prin canalele definite în proiectare, cu colectarea datelor necesare, atașarea documentelor, validări inițiale și crearea obiectului de proces. Cererea va primi stare, identificator, solicitant, context, documente, canal, moment de depunere și legături către verificările ulterioare. Astfel, cererea intră în sistem ca obiect urmărit, nu ca fișier sau înregistrare izolată.

UC07 va acoperi înregistrarea formularului. Formularul poate proveni din interfața electronică, din preluare internă sau dintr-un flux asistat de utilizator CNAS. În toate cazurile, datele formularului vor fi validate, asociate cu solicitantul și procesul corect, iar eventualele lipsuri vor fi transformate în mesaje, sarcini sau solicitări de completare. Înregistrarea formularului trebuie să fie suficient de strictă pentru date oficiale și suficient de clară pentru utilizator.

UC08 va permite examinarea documentelor. Sistemul va susține verificarea completitudinii, valabilității și coerenței documentelor atașate sau generate. Examinarea trebuie să producă rezultat operațional: document acceptat, document respins, document care necesită completare, observație, sarcină de remediere sau continuare a procesului. Acest rezultat se păstrează în istoricul dosarului și influențează tranzițiile următoare.

UC10 va trata aprobarea și respingerea ca acțiuni guvernate de rol, stare și reguli. Aprobarea nu este un buton generic. Ea trebuie să fie disponibilă numai pentru obiecte ajunse în starea corespunzătoare și pentru utilizatori care au rolul necesar. Respingerea trebuie să păstreze motiv, dată, utilizator, document sau obiect afectat și efectul asupra fluxului. Pentru obiectele sensibile, aprobarea/respingerea este act operațional care trebuie reconstruit ulterior.

UC21 acoperă procesarea cererii sau formularului după depunere și examinare. Această procesare poate include validări automate, verificări cu sisteme externe, completări, repartizare, calcul, determinarea rezultatului, generarea documentelor și trecerea către aprobare sau notificare. UC21 este locul unde se vede dacă sistemul este cu adevărat operațional: datele colectate trebuie să producă efect, nu doar să fie stocate.

Lanțul complet este următorul: depunere cerere -> înregistrare formular -> examinare documente -> procesare -> aprobare/respingere -> generare document -> notificare -> jurnalizare. Fiecare pas are actor, stare, date, reguli, documente, acțiuni permise și evidență. Acesta este motivul pentru care oferta păstrează lanțurile operaționale: ele arată cum UC-urile lucrează împreună.

4.4 Registre, date, integrare și configurări

UC12 și UC13 sunt legătura dintre procesele de servicii publice și baza informațională a CNAS. Sistemul nu poate funcționa doar pe cereri izolate. El trebuie să ofere registre consultabile, profiluri de solicitant, legături cu istoricul cererilor, documentelor, deciziilor și, pentru procesele care le folosesc, informații despre plătitori, persoane asigurate, cont individual și alte obiecte operaționale.

UC12 va permite explorarea registrelor conform rolurilor și drepturilor de acces. Registrele nu vor fi tratate ca tabele administrative brute. Ele vor oferi căutare, filtrare, vizualizare, istoric relevant, legături către obiecte asociate și acțiuni permise. Pentru plătitori și persoane asigurate, registrul devine punct de intrare în istoricul contribuțiilor, documentelor, perioadelor, soldurilor, obligațiilor sau interacțiunilor relevante.

UC13 va permite gestionarea profilului solicitantului. Profilul solicitantului nu este doar fișa de contact. El concentrează date de identificare, date de comunicare, cereri depuse, documente, rezultate, notificări, istoric și eventuale legături cu date obținute din sisteme externe. Profilul trebuie să reducă duplicarea datelor, să păstreze controlul asupra modificărilor și să faciliteze prestarea serviciilor următoare.

În acest grup funcțional, riscul principal este accesul prea larg sau prea opac la date. Oferta răspunde prin roluri, metadate, filtrare, audit și separarea între vizualizare, editare, export și administrare. Un utilizator poate avea dreptul să consulte anumite date fără să poată modifica, exporta sau vedea toate detaliile sensibile.

Schimbul de date cu sisteme externe

UC14 este unul dintre cazurile de utilizare care schimbă natura sistemului. SI „Protecția Socială” nu funcționează în izolare. El va primi și va transmite date prin servicii externe, platforme guvernamentale și integrări instituționale. Aceste schimburi trebuie tratate ca parte a procesului de business, nu ca detaliu tehnic ascuns.

Sistemul propus va gestiona schimbul de date printr-un strat controlat de integrare. Fiecare integrare va avea contract, scop, actor tehnic, tip de date, reguli de securitate, jurnalizare, tratare erori, timeout, retry unde este permis, mecanism de monitorizare și legătură cu obiectul operațional afectat. Un răspuns extern utilizat într-o decizie, verificare sau calcul trebuie să poată fi explicat ulterior: ce serviciu a fost apelat, când, pentru ce obiect, ce rezultat a întors și ce efect a produs.

Pentru datele externe relevante în decizii, sistemul va păstra metadate și, unde este necesar, snapshot operațional. Aceasta previne situația în care o decizie luată astăzi devine inexplicabilă mâine deoarece datele din sursa externă s-au modificat. Integrarea este astfel legată de trasabilitate, nu doar de schimb de mesaje.

Configurarea serviciilor, fluxurilor, metadatelor și accesului

UC15, UC16, UC17 și UC18 formează zona prin care sistemul rămâne administrabil după go-live. Aceasta este o piesă funcțională centrală, nu o anexă tehnică. CNAS trebuie să poată ajusta servicii, fluxuri, metadate, șabloane, utilizatori și drepturi în mod controlat, fără intervenții directe în baza de date și fără modificări informale în producție.

UC15 va permite configurarea serviciilor electronice. Aici se definesc elementele care descriu un serviciu: formular, câmpuri, documente necesare, reguli de validare configurabile, canale, mesaje, vizibilitate, parametri și condiții de activare. Configurarea serviciului va avea versiune, stare, autor, dată, motiv și, unde este necesar, aprobare înainte de publicare.

UC16 va permite configurarea fluxurilor de lucru. Fluxul nu este desen decorativ, ci set de stări, tranziții, roluri, acțiuni, termene, notificări și reguli operaționale. Acolo unde ToR permite configurare, CNAS va putea ajusta trasee operaționale fără dezvoltare software disproporționată. Totuși, regulile critice de calcul, securitate, integrare sau efect legal vor rămâne implementate, testate și versionate prin procesul de dezvoltare.

UC17 va gestiona metadatele și șabloanele de documente. Nomenclatoarele, clasificatoarele, metadatele și șabloanele nu vor fi valori dispersate. Ele vor fi administrate prin interfețe, cu istoric, versiune, stare activ/inactiv și audit. Pentru documente oficiale, șablonul trebuie să fie legat de sursa datelor, parametri, versiune și condițiile de generare.

UC18 va administra utilizatorii și controlul accesului. Sistemul va separa identitatea autentificată de rolul operațional și de permisiunile concrete. Accesul va fi controlat la nivel de rol, acțiune, obiect, stare și context. Interfața poate ascunde sau afișa acțiuni, dar decizia finală de autorizare aparține backend-ului. Aceasta protejează sistemul de execuții neautorizate prin apeluri directe sau ocolirea interfeței.

4.5 Rapoarte, documente, proceduri automate și audit

UC09 și UC19 acoperă una dintre cele mai vizibile zone pentru CNAS: rapoartele și documentele. Sistemul nu este complet dacă poate procesa cereri, dar nu poate produce rapoarte, extrase, decizii, certificate, indicatori și documente oficiale într-o formă controlată. Raportarea și documentele sunt produsele prin care datele sistemului devin evidență instituțională.

UC09 va permite extragerea rapoartelor de către utilizatori autorizați. Rapoartele vor avea parametri, sursă de date, reguli de acces, format și criterii de performanță. Pentru rapoarte simple, execuția poate fi interactivă. Pentru rapoarte grele sau statistice, sistemul va utiliza structuri pregătite pentru citire, agregări sau execuții asincrone, astfel încât raportarea să nu degradeze fluxurile tranzacționale.

UC19 va permite generarea documentelor și rapoartelor oficiale din șabloane și date controlate. Documentul generat trebuie să poată fi legat de obiectul sursă: cerere, formular, decizie, registru, raport, solicitant sau alt obiect relevant. Generarea documentului va păstra versiunea șablonului, datele folosite, momentul, utilizatorul sau procesul automat și acțiunea ulterioară: descărcare, transmitere, notificare sau arhivare.

Această zonă trebuie proiectată împreună cu guvernanța șabloanelor. Dacă șabloanele sunt modificate informal, documentele oficiale devin greu de explicat. Dacă rapoartele rulează direct pe tabele tranzacționale grele, sistemul devine lent. Dacă exporturile nu sunt auditate, datele personale pot circula necontrolat. Oferta răspunde prin surse de date pregătite, șabloane versionate, audit și reguli de acces.

Proceduri automate, notificări și jurnalizare

UC20, UC22 și UC23 sunt funcționalități transversale. Ele nu aparțin unui singur modul, ci susțin întregul sistem. Procedurile automate reduc munca repetitivă și permit procesări de volum. Notificările fac sistemul activ și orientat spre acțiune. Jurnalizarea transformă utilizarea sistemului în evidență verificabilă.

UC20 va executa proceduri automate cu stare, programare, rezultat, jurnal de erori și posibilitate de reluare unde procesul permite. Exemplele relevante includ importuri, sincronizări, agregări, notificări automate, verificări periodice, pregătire rapoarte, recalculări sau alte joburi definite în proiectare. O procedură automată nu trebuie să fie o cutie neagră. CNAS trebuie să vadă când a rulat, ce a procesat, ce a eșuat și ce acțiune este necesară.

UC22 va notifica utilizatorii interni și externi despre evenimente relevante: asignarea unei sarcini, depășirea unui termen, necesitatea implicării într-un flux, rezultat al unei acțiuni, acceptare, înregistrare document, aprobare, respingere, probleme de performanță sau alte evenimente configurate. Notificarea din dashboard va conduce direct către cererea, documentul sau formularul relevant, iar integrarea cu MNotify va permite canale externe acolo unde sunt agreate și disponibile.

UC23 va asigura jurnalizarea evenimentelor de business. Vor fi jurnalizate cel puțin evenimentele de autentificare/deconectare, accesare/modificare/suprimare înregistrări, recepționare cereri, examinare cereri, executare sarcini, eliberare documente, aprobare/respingere formulare sau documente, configurări de servicii, modificări de nomenclatoare/metadate, activare/dezactivare utilizatori, atribuire roluri, schimburi de date cu sisteme externe, generare/accesare rapoarte sau documente și alte evenimente specifice activității CNAS. Fiecare eveniment va păstra identificator, utilizator, categorie, moment, componentă, obiect afectat, detalii ale acțiunii și referință către obiectul operațional, în funcție de natura evenimentului.

UC23 este mecanismul prin care oferta devine demonstrabilă. Fără jurnalizare, sistemul poate funcționa, dar nu poate explica suficient de bine ce s-a întâmplat. Cu jurnalizare de business, fiecare flux critic poate fi reconstruit: cine a depus, cine a examinat, ce document a fost accesat, ce integrare a fost apelată, cine a aprobat, ce raport a fost generat și ce configurare a fost modificată.

4.6 Lanțurile operaționale end-to-end

După maparea UC-urilor, modelul funcțional trebuie privit prin lanțuri end-to-end. Acestea sunt scenariile reale prin care se înțelege produsul. Fiecare lanț activează mai multe UC-uri și produce un rezultat operațional verificabil. În SRS, SDD, matricea de conformitate și planul de testare, aceste lanțuri vor fi transformate în scenarii, reguli, stări, date, ecrane, servicii și criterii de acceptanță.

Această secțiune completează explicit stratul UC. UC-urile răspund la întrebarea „ce funcții trebuie să existe?”. Lanțurile răspund la întrebarea „cum funcționează sistemul CNAS când aceste funcții sunt folosite împreună?”. Ambele niveluri sunt necesare: fără UC-uri, oferta pare conceptuală; fără lanțuri, sistemul riscă să fie perceput ca o colecție de ecrane fără comportament instituțional.

Lanțul plătitor - contribuții - cont individual - drept

Primul lanț funcțional critic leagă plătitorii, obligațiile, declarațiile, achitările și contribuțiile de contul individual al persoanei asigurate. Acest lanț nu este doar zonă de evidență financiară. El este una dintre bazele pe care CNAS poate stabili, verifica sau explica ulterior anumite drepturi. De aceea, funcțiile de registru, căutare, profil, schimb de date, raportare și audit trebuie să lucreze împreună.

În termeni UC, lanțul activează UC03 pentru căutare și vizualizare, UC12 pentru explorarea registrelor, UC13 pentru legătura cu profilul persoanei/solicitantului, UC14 pentru date preluate sau verificate prin sisteme externe, UC09 și UC19 pentru rapoarte și documente, UC20 pentru proceduri automate de import/agregare și UC23 pentru jurnalizarea evenimentelor. Dacă acest lanț este tratat doar ca registru static, sistemul poate afișa date, dar nu poate demonstra suficient cum aceste date au devenit bază operațională pentru drepturi.

Plătitorul trebuie să fie obiect operațional cu istoric, nu doar valoare într-un nomenclator. Pentru fiecare plătitor, sistemul trebuie să poată lega datele de identificare, obligațiile, declarațiile, achitările, soldurile, restanțele, corecțiile, eventualele documente și rapoartele relevante. Contribuția individuală trebuie să poată fi asociată persoanei, perioadei, sursei, plătitorului și istoricului de modificare. Această logică permite acceptanță practică: se poate urmări un caz de la înregistrarea/plasarea datelor până la consultarea în cont individual și utilizarea în fluxuri ulterioare.

Rezultatul verificabil al lanțului nu este doar existența unui ecran de registru. Rezultatul este capacitatea sistemului de a explica relația dintre plătitor, contribuție, perioadă, persoană asigurată și efectul operațional. În testare, acest lucru se demonstrează prin scenarii cu date inițiale, modificări/corecții, consultare, raportare și audit.

Lanțul persoană asigurată - istoric - cont individual

Persoana asigurată este nodul în jurul căruia se întâlnesc date de identificare, contribuții, perioade, stagiu, documente, cereri, decizii, drepturi și plăți. Din acest motiv, modelul funcțional nu trebuie să trateze persoana ca simplă fișă de date. Profilul trebuie să fie locul în care utilizatorul autorizat vede relațiile relevante, sursele, istoricul, acțiunile posibile și limitele de acces.

Acest lanț folosește UC03 pentru căutare, UC12 pentru registre, UC13 pentru profil, UC14 pentru verificări externe, UC08 pentru documente asociate, UC09/UC19 pentru rapoarte sau extrase și UC23 pentru audit. În funcție de serviciul public procesat, lanțul poate continua spre UC06-UC21, atunci când persoana devine solicitant într-un flux de cerere sau beneficiar al unui rezultat.

Contul individual trebuie să fie utilizabil atât ca instrument de lucru, cât și ca mecanism de explicare. Utilizatorul autorizat trebuie să poată înțelege ce perioade sunt luate în considerare, care este sursa datelor, ce corecții au existat, ce date lipsesc sau sunt neclare și ce efect poate avea această informație într-un proces de stabilire sau verificare a drepturilor. Pentru date migrate, sistemul trebuie să poată marca originea și calitatea datelor, astfel încât istoricul să fie explicabil, nu doar transferat.

Acceptanța acestui lanț trebuie să demonstreze că profilul persoanei, contul individual, registrele și istoricul nu sunt ecrane separate fără legătură. Scenariul trebuie să poată porni de la persoană, să urmărească datele relevante, să vadă sursele, să deschidă obiecte asociate și să identifice evenimentele jurnalizate.

Lanțul cerere - formular - dosar - verificare - calcul - decizie

Acesta este lanțul care arată cel mai clar diferența dintre implementarea unor UC-uri și livrarea unui sistem funcțional. UC06 permite depunerea cererii, UC07 înregistrarea formularului, UC08 examinarea documentelor, UC21 procesarea, UC10 aprobarea/respingerea, UC19 generarea documentului, UC22 notificarea și UC23 jurnalizarea. Separat, fiecare UC este necesar. Împreună, ele formează ciclul de prestare a serviciului public.

Cererea trebuie să intre în sistem ca obiect cu identitate, solicitant, canal, date, documente, stare și istoric. Formularul trebuie să fie asociat procesului corect și validat conform regulilor aplicabile. Documentele trebuie examinate cu rezultat clar, nu doar atașate. Procesarea trebuie să execute verificări, completări, calcule, repartizări sau decizii intermediare. Aprobarea sau respingerea trebuie să fie disponibilă numai în starea corectă, pentru rolul corect și cu motiv/document/rezultat păstrat.

Calculul, acolo când scenariul o cere, nu trebuie să fie rezultat opac. Sistemul trebuie să păstreze datele folosite, parametrii, sursele, versiunea regulilor sau configurațiilor relevante și legătura cu decizia generată. Dacă apare o contestație, o verificare internă sau o solicitare de audit, CNAS trebuie să poată reconstrui traseul: cine a depus, ce date au fost verificate, ce documente au fost acceptate sau respinse, ce calcul a fost executat, cine a aprobat și ce document a rezultat.

În testare, acest lanț trebuie probat cap-coadă, nu doar prin bifarea ecranelor. Se pornește de la solicitant și cerere, se trece prin formular, documente, sarcini, verificări externe, procesare, decizie, document generat, notificare și audit. Aici se vede dacă sistemul este o platformă operațională sau doar un set de funcții.

Lanțul drept - plată - modificare

După emiterea unei decizii sau stabilirea unui rezultat cu impact financiar, sistemul intră într-un alt lanț critic: dreptul trebuie transformat în plată și gestionat pe durata lui de viață. Dreptul nu este o valoare statică. El poate fi indexat, recalculat, suspendat, reluat, modificat, corectat sau încetat. Plata nu este doar transfer de sumă; ea este efectul unui drept, al unei perioade, al unei decizii și al unor reguli aplicate.

În structura UC, acest lanț se leagă de UC21 pentru procesare, UC10 pentru aprobare/respingere acolo unde este necesar, UC19 pentru documente/rapoarte, UC20 pentru proceduri automate de volum, UC14 pentru date externe care pot influența statutul sau plata, UC22 pentru notificări și UC23 pentru jurnalizare. Chiar dacă unele detalii de pensii/prestații/plăți vor fi dezvoltate în capitolele funcționale specializate sau în SRS/SDD, Capitolul 3 trebuie să arate principiul: dreptul, plata și modificarea trebuie să rămână legate și explicabile.

Separarea dintre drept și plata efectivă este importantă. Dreptul explică de ce o persoană are de primit o sumă pentru o perioadă. Plata explică dacă suma a fost inclusă într-o comandă, transmisă, achitată, respinsă, returnată, reținută sau modificată. Dacă aceste două niveluri se amestecă, sistemul devine greu de auditat și greu de reconciliat. Dacă se separă fără legătură, utilizatorul nu mai poate explica traseul.

Rezultatul verificabil este capacitatea sistemului de a răspunde la întrebarea practică a CNAS: de ce o persoană a primit sau nu a primit o sumă, ce eveniment a schimbat plata, ce regulă s-a aplicat, ce proces automat a intervenit și cine a autorizat acțiunea. Acesta este tipul de scenariu care trebuie să apară în UAT, nu doar în documentație.

Lanțul integrare - validare - snapshot - efect operațional

Integrarea cu sisteme externe nu este anexă tehnică la funcțional. În procesele CNAS, datele externe pot confirma identitatea, statutul, eligibilitatea, perioadele, plățile, comunicările sau alte elemente care influențează decizia și raportarea. Din acest motiv, UC14 trebuie citit împreună cu UC06-UC21, UC20, UC22 și UC23, nu izolat.

Lanțul funcțional corect este: sistemul are nevoie de date externe, inițiază schimbul prin contract controlat, primește răspuns, validează răspunsul, tratează eroarea sau indisponibilitatea, păstrează metadate și, unde este necesar, snapshot operațional, apoi folosește rezultatul în flux. Astfel, datele externe devin parte explicabilă a dosarului, deciziei, raportului sau notificării.

Snapshotul nu este o copie inutilă. El este necesar atunci când decizia de astăzi trebuie explicată mâine, chiar dacă sursa externă și-a modificat ulterior datele. Sistemul trebuie să poată arăta ce s-a verificat, când, cu ce parametri, ce răspuns a venit, ce eroare a apărut sau ce fallback operațional a fost aplicat. Fără această urmă, integrarea poate funcționa tehnic, dar nu susține suficient auditul business.

Acceptanța acestui lanț trebuie să includă scenarii cu răspuns pozitiv, răspuns negativ, lipsă de date, eroare temporară, timeout și reluare. Pentru fiecare scenariu, sistemul trebuie să păstreze starea fluxului și să nu lase utilizatorul într-o situație ambiguă.

Lanțul raportare - document - date controlate

Raportarea și documentele sunt ieșirile vizibile ale sistemului. UC09 permite extragerea rapoartelor, UC19 generarea rapoartelor și documentelor, UC11 descărcarea, UC20 pregătirea automată a datelor sau execuțiilor de volum, iar UC23 auditul. Aceste UC-uri trebuie legate de date controlate, nu de interogări pe tabele operaționale.

Lanțul corect pornește din date operaționale validate, trece prin reguli de acces, surse pregătite pentru raportare, parametri, șabloane versionate, generare, export sau descărcare și jurnalizare. Pentru rapoarte simple, execuția poate fi interactivă. Pentru rapoarte grele, statistice sau recurente, sistemul trebuie să poată utiliza agregări, read models, materialized views sau joburi automate, astfel încât raportarea să nu blocheze fluxurile tranzacționale.

Documentul generat trebuie să fie legat de obiectul sursă: cerere, decizie, formular, registru, solicitant, drept, plată sau raport. Trebuie păstrată versiunea șablonului, momentul generării, utilizatorul sau procedura automată, parametrii și acțiunea ulterioară. Astfel, un document nu este doar fișier descărcat, ci rezultat oficial al unui proces verificabil.

Acceptanța trebuie să demonstreze rapoarte generate cu parametri, documente generate din șabloane, exporturi controlate, reguli de acces și jurnalizarea descărcărilor sau accesărilor sensibile.

Lanțul administrare - configurare - audit

Un sistem CNAS nu rămâne util doar pentru că a fost livrat corect la go-live. El trebuie să poată fi administrat: servicii electronice, fluxuri, metadate, șabloane, utilizatori, roluri, notificări, proceduri automate și reguli configurabile trebuie gestionate prin mecanisme autorizate. De aceea UC15-UC18 sunt funcționalități centrale, nu anexe administrative.

Lanțul începe cu o schimbare operațională: un serviciu nou, un șablon modificat, o tranziție de flux, un nomenclator, un rol sau o permisiune. Schimbarea trebuie introdusă de rol autorizat, versionată, verificată, aprobată unde impactul o cere, activată la momentul potrivit și jurnalizată. UC23 este obligatoriu în acest lanț, deoarece configurarea fără audit devine risc operațional.

În același timp, oferta nu promite configurabilitate nelimitată. Regulile de calcul, validările cu efect legal/financiar, controalele de securitate și integrările oficiale trebuie dezvoltate, testate și acceptate prin proces controlat. Configurabilitatea este folosită acolo unde reduce dependența de dezvoltare fără a compromite corectitudinea sistemului.

Acceptanța trebuie să arate că administratorul poate configura servicii, fluxuri, șabloane, metadate, utilizatori și drepturi fără intervenții informale în baza de date, iar sistemul păstrează istoricul și efectele acestor configurări. Acesta este unul dintre semnele că CNAS primește o platformă operabilă, nu doar o aplicație finalizată într-o anumită zi.

Lanț operațional	UC-uri activate	Descriere	Rezultat verificabil
Acces public la informație	UC01, UC02, UC03, UC11, UC23	Utilizatorul accesează portalul, explorează conținut public, caută date permise, vizualizează rezultate și descarcă documente publice sau autorizate.	Informație publică/depersonalizată disponibilă, căutabilă, descărcabilă și jurnalizată unde este cazul.
Inițiere serviciu public	UC02, UC03, UC06, UC07, UC13, UC22, UC23	Solicitantul identifică serviciul, depune cererea, completează formularul, actualizează profilul și primește confirmare/notificare.	Cerere/formular creat, date validate inițial, solicitant identificat, proces inițiat și notificat.
Examinare și decizie	UC04, UC05, UC08, UC10, UC14, UC21, UC19, UC22, UC23	Utilizatorul CNAS primește sarcină, examinează documente, solicită/verifică date externe, procesează cererea, aprobă/respinge și generează document.	Dosar procesat, decizie/document generat, rezultat notificat și istoric complet al acțiunilor.

Lanț operațional	UC-uri activate	Descriere	Rezultat verificabil
Registre și profil operațional	UC03, UC12, UC13, UC14, UC23	Utilizatorul autorizat caută în registre, consultă profilul solicitantului sau obiecte asociate, verifică date externe și urmărește istoricul.	Date operaționale coerente, consultabile conform rolului, cu acces și modificări auditate.
Raportare și documente	UC09, UC11, UC19, UC20, UC23	Sistemul generează rapoarte sau documente, eventual prin joburi automate, le pune la dispoziție pentru vizualizare, export sau descărcare.	Rapoarte/documente generate din surse controlate, cu parametri, versiune șablon, audit și criterii de performanță.
Configurare și administrare	UC15, UC16, UC17, UC18, UC20, UC23	Administratorul configurează serviciu, flux, șablon, metadate, utilizatori sau proceduri automate, cu activare controlată și audit.	Sistem administrabil fără intervenții informale în DB, cu istoric și control al schimbărilor.
Monitorizare operațională	UC04, UC05, UC09, UC20, UC22, UC23	Managerii și utilizatorii autorizați urmăresc sarcini, termene, volume, excepții, proceduri automate și notificări.	Vizibilitate asupra funcționării sistemului și asupra blocajelor operaționale.

4.7 Ce trebuie demonstrat la acceptanță

Pentru acest capitol, acceptanța nu se poate baza doar pe afirmația că toate UC-urile au fost implementate. Fiecare grup funcțional trebuie demonstrat prin scenarii executate, date, capturi, rezultate, loguri, documente și rapoarte. În mod practic, capitolul funcțional produce baza pentru SRS, SDD, matricea de conformitate, matricea de test coverage și scenariile UAT.

- Pentru UC01-UC03 și UC11: interfață publică funcțională, conținut organizat, căutări și sortări executate, documente descărcate, reguli de vizibilitate validate.
- Pentru UC04-UC05: dashboarduri pe rol, sarcini generate din fluxuri reale, acțiuni disponibile conform stării și istoricul execuției sarcinilor.
- Pentru UC06-UC08, UC10 și UC21: cereri/formulare depuse, documente examinate, procesări executate, aprobări/respingări efectuate, decizii/documente generate și notificări transmise.
- Pentru UC12-UC13: registre consultabile, profil solicitant gestionat, legături cu cereri/documente și audit al accesului sau modificărilor.
- Pentru UC14: servicii externe apelate în scenarii relevante, răspunsuri gestionate, erori tratate, metadate și snapshoturi păstrate unde este necesar.
- Pentru UC15-UC18: servicii, fluxuri, șabloane, metadate, utilizatori și permisiuni administrate prin interfețe, cu versiune, istoric și audit.
- Pentru UC09 și UC19: rapoarte și documente generate din date controlate, cu parametri, șabloane, exporturi și reguli de acces validate.
- Pentru UC20-UC23: proceduri automate executate cu stare și rezultat, notificări generate în dashboard/MNotify când scenariul o cere, evenimente de business jurnalizate și regăsibile.

Această evidență va confirma că sistemul nu este doar prezentat ca lanțuri operaționale, ci livrează funcțiile cerute prin UC01-UC23. Lanțurile rămân diferențiatorul de maturitate: ele arată că funcțiile nu au fost implementate ca bucăți independente, ci ca mecanisme operaționale care pot susține activitatea reală CNAS.

4.8 Concluzie funcțională

Modelul funcțional propus răspunde direct la structura ToR: UC01-UC23 sunt acoperite ca funcționalități contractuale, iar gruparea lor în capabilități și lanțuri arată modul în care sistemul va funcționa în practică.

CNAS cumpără un sistem, nu o prezentare despre procese; de aceea capitolul face vizibile funcțiile concrete. În același timp, CNAS are nevoie de un sistem care să nu se rupă în 23 de piese. De aceea, oferta explică și lanțurile care leagă UC-urile în fluxuri reale: acces public, dashboard, sarcini, cerere, formular, examinare, aprobare, procesare, document, notificare, raportare, integrare, configurare și audit.

Prin această abordare, Capitolul 3 devine baza funcțională a ofertei. Matricea de conformitate va demonstra acoperirea fiecărei cerințe CF. SRS și SDD vor detalia regulile, stările, datele, ecranele, serviciile și contractele. Scenariile UAT vor demonstra executarea cap-coadă. Iar jurnalizarea, raportarea și documentele generate vor permite CNAS să verifice nu doar că sistemul există, ci că sistemul explică ceea ce face.

5. UX/UI, MUD, accesibilitate și bilingvism/multilingvism

5.1 Rolul interfeței în SI „Protecția Socială”

Interfața SI „Protecția Socială” nu este tratată ca strat grafic aplicat peste funcționalități. Pentru CNAS, interfața este spațiul operațional în care utilizatorii lucrează cu cereri, dosare, registre, decizii, documente, plăți, rapoarte, notificări și sarcini. De aceea, proiectarea UX/UI se va lega direct de fluxurile funcționale, de roluri, de stări, de acțiuni permise și de evidențele care trebuie păstrate pentru audit și acceptanță.

Abordarea propusă pornește de la faptul că sistemul va fi utilizat de categorii diferite de utilizatori: utilizatori publici, solicitanți autentificați, operatori CNAS, specialiști de examinare, aprobatori, manageri, administratori de sistem, administratori de configurări și echipa de suport. Fiecare categorie trebuie să vadă informațiile, sarcinile și acțiunile necesare rolului său, fără expunere excesivă de date și fără obligarea utilizatorului să navigheze prin module care nu sunt relevante pentru activitatea curentă.

Prin urmare, interfața va fi proiectată pe spații de lucru, lanțuri operaționale și obiecte de proces. Un utilizator nu va lucra cu „ecrane” izolate, ci cu cereri, dosare, persoane, plătitori, contribuții, decizii, documente, plăți, rapoarte și notificări. Fiecare obiect important va avea stare, istoric, acțiuni disponibile, documente asociate, verificări externe, mesaje de validare și legătură cu jurnalul de evenimente.

5.2 Acoperirea cerințelor UI din caietul de sarcini

Cerințele UI001-UI016 sunt tratate ca cerințe operaționale, nu ca listă de proprietăți vizuale. Ele definesc modul în care sistemul trebuie să poată fi folosit în activitatea zilnică: toate funcționalitățile accesibile prin interfață, interfață intuitivă pentru roluri administrative și non-administrative, suport lingvistic, conformitate WCAG 2.1, optimizare pentru rezoluția minimă indicată, responsive design, traduceri centralizate, salvare intermediară, căutare globală și QBE, filtrare, exporturi, atașamente cu metadate, ajutor contextual și utilizarea Modelului Unitar de Design.

Cerință UI	Tratament propus în soluție	Evidență verificabilă
UI001-UI002	Funcționalitățile accesibile utilizatorilor vor fi disponibile prin interfață, organizate pe roluri, sarcini și obiecte operaționale. Interfața administrativă și cea operațională vor avea structuri separate, dar coerente.	Hartă ecrane/roluri, prototipuri, matrice funcționalitate-rol, scenarii UAT pe rol.
UI003, UI007	Interfața va fi administrată prin mecanism centralizat de texte și traduceri pentru română, rusă și engleză, cu preferință lingvistică asociată contului utilizatorului.	Catalog texte UI, chei de traducere, verificare limbi, capturi ecran pe limbi.
UI004	Componentele UI, formularele, navigarea, focusul, mesajele de eroare, contrastul și compatibilitatea cu tehnologii asistive vor fi verificate față de WCAG 2.1.	Raport verificare accesibilitate, test keyboard navigation, listă remedieri.
UI005-UI006	Interfața va fi optimizată pentru PC/notebook la rezoluția 1360x768 și va avea comportament responsive pentru funcționalitățile cheie pe desktop, tabletă și smartphone.	Test responsive, capturi la rezoluții, scenarii pe dispozitive.
UI008	Formularele critice vor avea salvare intermediară, protecție împotriva pierderii datelor introduse și reluarea controlată a operațiunilor inițiate.	Test autosave/draft, istoric versiune formular, scenariu reluare.
UI009-UI012	Căutarea va combina principii unitare: căutare globală, QBE, filtrare în rezultate, filtre pe nomenclatoare, criterii exacte/logice și măști de căutare.	Demo căutare, teste filtre, seturi de date cu valori controlate.
UI013	Gridurile și rezultatele permise vor permite export în PDF, XLS/XLSX și CSV, cu respectarea rolurilor, a restricțiilor de acces și a auditului exporturilor.	Exporturi generate, log export, verificare drepturi.
UI014	Atașamentele și referințele URL vor fi asociate obiectelor informaționale cu metadate: tip, dimensiune, creator, dată creare/modificare și legătura cu obiectul procesat.	Atașamente test, metadate, reguli acces, log acces/modificare.

UI015	Ajutorul contextual va fi disponibil în interfață pentru funcționalitățile principale, cu explicații legate de acțiunea curentă și de statutul obiectului.	Mostre ajutor contextual, scenarii instruire, capturi interfață.
UI016	Modelul Unitar de Design va ghida proiectarea și implementarea interfeței prin tokens, componente, layout-uri și pattern-uri conforme.	Prototipuri MUD, component mapping, verificare UI/UX.

5.3 Aplicarea Modelului Unitar de Design

Modelul Unitar de Design va fi folosit ca bază de proiectare pentru interfață, nu doar ca inspirație vizuală. Aplicarea lui în SI „Protecția Socială” presupune utilizarea fundamentelor, componentelor și șabloanelor acceptate pentru serviciile digitale guvernamentale, cu adaptarea controlată la procesele CNAS. Aceasta permite ca sistemul să fie coerent cu alte platforme ale statului, dar și suficient de specializat pentru activitatea complexă de pensii, prestații, contribuții, plăți și rapoarte.

Implementarea MUD va fi controlată prin trei niveluri. Primul nivel este nivelul vizual: culori, tipografie, spațiere, iconografie, stări vizuale și componente standard. Al doilea nivel este nivelul de interacțiune: formulare, validări, mesaje, tabele, filtre, taburi, panouri de detaliu, pași de proces și navigare. Al treilea nivel este nivelul operațional: ecrane de lucru construite pe fluxuri CNAS, cu sarcini, stări, acțiuni, documente, verificări și audit.

Pentru frontend-ul React propus în ofertă, aplicarea MUD se va realiza prin preluarea design tokens și a structurii componentelor în biblioteca frontend a proiectului. Componentele React vor encapsula regulile vizuale și comportamentale necesare: input-uri, butoane, mesaje de eroare, tabele, filtre, paginare, carduri, modale, taburi, panouri de status, breadcrumbs și layout-uri responsive. Această abordare evită copierea manuală și neuniformă a stilurilor în fiecare ecran.

5.4 Arhitectura informațională și navigarea

Arhitectura informațională va separa clar zona publică, zona de lucru operațională, zona de administrare, zona de raportare și zona de suport. Utilizatorul public trebuie să găsească informații, servicii și documente fără a fi expus la logica internă a CNAS. Utilizatorul CNAS trebuie să ajungă rapid la sarcina, cererea, dosarul, registrul sau raportul relevant. Administratorul trebuie să gestioneze configurări și drepturi fără a interveni direct în baza de date.

Navigarea va fi construită în jurul obiectelor și acțiunilor. Pentru cereri și dosare, utilizatorul va vedea starea curentă, pașii parcurși, documentele atașate, verificările efectuate, acțiunile disponibile și restricțiile. Pentru registre, utilizatorul va putea căuta, filtra, sorta, exporta și intra în detaliu, cu vizibilitate limitată la drepturile sale. Pentru raportare, utilizatorul va porni de la catalogul de rapoarte, parametri, perioade și formatul de ieșire.

Pentru procesele cu durată sau cu multe interacțiuni, interfața va utiliza indicatori vizuali de stare, timeline de proces, liste de sarcini, notificări și linkuri directe către obiectul afectat. Aceasta reduce riscul ca utilizatorii să lucreze pe informații vechi sau să execute acțiuni în afara fluxului aprobat.

5.5 Spațiul de lucru pe roluri și dashboardurile operaționale

Dashboardul nu va fi tratat ca panou decorativ de indicatori. Pentru SI „Protecția Socială”, dashboardul este mecanismul prin care utilizatorii autorizați văd sarcinile, termenele, blocajele, notificările, volumele de lucru și acțiunile care necesită intervenție. Dashboardurile vor fi diferențiate pe roluri: operator, specialist, aprobator, manager, administrator și suport.

Pentru utilizatorul operațional, dashboardul va pune în față sarcini, cereri în lucru, dosare cu termen, notificări și excepții. Pentru manager, dashboardul va oferi volume, întârzieri, încărcare pe echipe, procese blocate și indicatori operaționali. Pentru administrator, dashboardul va arăta starea joburilor, erori tehnice, configurări relevante și alerte de mentenanță. Pentru suport, dashboardul va lega solicitările de obiectele operaționale afectate.

Acest model reduce dependența de căutări manuale și de liste generale. Utilizatorul pornește din spațiul său de lucru și ajunge direct la obiectul de proces, cu acțiunile permise pentru rolul și starea curentă.

5.6 Formulare, validări și lucrul cu date sensibile

Formularele electronice vor fi proiectate pentru procese reale, nu ca simple colecții de câmpuri. Pentru fiecare formular se vor defini secțiuni, câmpuri obligatorii, validări, mesaje de eroare, reguli de salvare intermediară, atașamente, precompletări din surse autorizate și acțiuni disponibile. Validările vizuale din client vor ajuta utilizatorul, dar validarea finală va rămâne în backend.

Pentru datele sensibile, interfața va aplica principiul vizibilității minime necesare. Câmpurile cu IDNP, date financiare, date medicale, informații despre dizabilitate sau alte date cu regim special vor fi afișate doar utilizatorilor autorizați și doar în contextul funcțional justificat. Listele și exporturile vor respecta aceleași reguli de acces ca ecranele de detaliu.

Mesajele de eroare și avertizare vor fi formulate astfel încât să fie utile utilizatorului, dar să nu expună detalii tehnice sau date nepermise. Interfața va diferenția erorile de completare, avertizările de business, indisponibilitatea unui serviciu extern, blocările de acces și erorile tehnice care trebuie tratate de suport.

5.7 Căutare, filtre, liste și registre

Căutarea este una dintre funcțiile centrale ale sistemului, deoarece CNAS lucrează cu volume mari de persoane, plătitori, contribuții, cereri, dosare, decizii, plăți și documente. Interfața va oferi principii unitare de căutare: căutare globală acolo unde este utilă, căutări specializate pe registre, QBE pentru filtrare precisă, filtre în liste, sortare, paginare și criterii pe nomenclatoare sau intervale.

Listele nu vor fi doar tabele. Ele vor afișa informații suficiente pentru identificarea rapidă a obiectului, statusul, ultimele acțiuni, alertele și acțiunile rapide permise. Pentru obiectele critice se va putea naviga către detaliu, istoric, documente, verificări externe și jurnal de evenimente. Exportul din grid va fi controlat prin roluri și jurnalizare, pentru a evita extragerile necontrolate de date.

Pentru registrele operaționale, interfața va combina eficiența de lucru cu protecția datelor. Utilizatorul va putea filtra și identifica rapid înregistrările, dar nu va putea accesa sau exporta informații dincolo de drepturile acordate.

5.8 Limbile interfeței, traduceri și conținut

Suportul lingvistic al interfeței va fi tratat ca funcție de platformă. Textele interfeței, mesajele, etichetele, titlurile, alertele și explicațiile vor fi gestionate centralizat prin chei de traducere, nu hardcodate în ecrane. Utilizatorul va putea selecta limba interfeței și va putea păstra preferința lingvistică în setările contului.

În practică, această abordare permite actualizarea textelor fără intervenții directe în codul fiecărui ecran și reduce riscul apariției unor traduceri neuniforme. Pentru formulare, șabloane de documente și rapoarte, mecanismul de limbă va fi corelat cu guvernanța șabloanelor și metadatelor, astfel încât limba interfeței și limba documentului generat să fie controlate separat acolo unde procesul o cere.

Traducerile vor fi verificate nu doar prin existența textelor, ci și prin afișare corectă în interfață: lungime, aliniere, diacritice, alfabet chirilic, mesaje de eroare, exporturi și documente generate. Această verificare este importantă deoarece diferențele de lungime între română, rusă și engleză pot afecta layout-ul, mai ales în tabele, butoane, meniuri și validări.

5.9 Accesibilitate și utilizare asistată

Accesibilitatea va fi abordată ca parte a proiectării și testării interfeței. Interfața va urmări navigarea cu tastatura, focus vizibil, contrast suficient, etichete clare pentru câmpuri, texte alternative pentru elementele relevante, mesaje de eroare asociate câmpurilor, structură logică a paginii și compatibilitate cu instrumente de accesibilitate.

Pentru formulare și tabele, accesibilitatea are impact direct asupra utilizării. Utilizatorul trebuie să poată înțelege ce câmp completează, ce eroare trebuie corectată, ce rând este selectat, ce filtru este activ și ce acțiune urmează să execute. Pentru procesele publice, accesibilitatea reduce barierele pentru cetățeni; pentru back-office, reduce erorile și oboseala în utilizare intensivă.

Verificarea accesibilității va combina instrumente automate cu verificări manuale pe fluxuri reprezentative: autentificare, căutare, completare formular, examinare documente, aprobare/respingere, generare document, raportare și administrare. Rezultatele vor fi incluse în evidențele de testare și remediere.

Calitatea interfeței nu se confirmă doar prin faptul că ecranele sunt implementate. Acceptanța UX/UI trebuie să demonstreze că utilizatorii pot executa fluxurile principale fără pași inutili, fără confuzie privind starea procesului și fără acces la date sau acțiuni nepermise. De aceea, validarea va include prototipuri, review cu utilizatori CNAS, scenarii de utilizare și verificări pe roluri.

Pentru fiecare grup de ecrane se vor păstra evidențe: prototip sau mockup aprobat, mapare la UC/proces, listă de componente MUD utilizate, diferențe justificate față de componenta standard, verificare responsive, verificare lingvistică, verificare accesibilitate și scenarii de acceptanță. Aceste evidențe reduc riscul ca designul să fie evaluat doar subiectiv.

Rezultatul urmărit este o interfață care susține activitatea CNAS: utilizatorul vede ce are de făcut, înțelege starea obiectului, primește mesaje clare, accesează rapid documentele și verificările relevante, iar sistemul păstrează auditul acțiunilor efectuate.

Domeniu UI/UX	**Ce se livrează în proiect**	**Cum se verifică**
MUD și componente	Bibliotecă frontend bazată pe tokens/componente MUD, React, exemple de utilizare.	Component mapping, prototipuri, capturi, review UI.
Fluxuri operaționale	Ecrane pentru dashboard, cereri, dosare, registre, documente, plăți, rapoarte, administrare.	Scenarii end-to-end pe roluri și procese.
Accesibilitate	Aplicarea standardelor WCAG la nivel de componente și fluxuri principale.	Raport verificare accesibilitate și remediere.
Limbi	Interfață română/rusă/engleză, traduceri centralizate, preferință de limbă.	Matrice texte, verificare afișare, capturi pe limbi.
Căutare și exporturi	Căutare globală/QBE, filtre, exporturi controlate.	Teste căutare, export, audit acces/export.
Ajutor contextual	Explicații în interfață pentru acțiuni și zone funcționale principale.	Mostre ajutor, scenarii instruire și UAT.

6. Configurabilitate, workflow și administrare operațională

Pentru CNAS, stratul funcțional de configurare, workflow și administrare operațională face controlabile după go-live serviciile electronice, fluxurile, formularele, metadatele, șabloanele, rolurile, notificările, procedurile automate și jurnalizarea. Acest strat nu este tratat ca zonă tehnică secundară, ci ca mecanism prin care sistemul rămâne exploatabil, ajustabil și verificabil pe parcursul utilizării sale reale.

UC-urile și lanțurile operaționale sunt susținute de mecanisme administrabile. O cerere poate fi procesată controlat doar atunci când serviciul este definit, formularul este activ, documentele obligatorii sunt cunoscute, fluxul are stări și tranziții, utilizatorii au drepturi potrivite, sarcinile ajung în dashboard, notificările se emit la evenimentele corecte, iar acțiunile rămân jurnalizate. Configurabilitatea devine astfel infrastructura funcțională prin care produsul va putea fi exploatat de CNAS în mod disciplinat.

UC15-UC18 formează nucleul funcțional al administrării: configurarea serviciilor electronice, configurarea fluxurilor de lucru, gestionarea metadatelor și șabloanelor, administrarea utilizatorilor și controlului accesului. Aceste mecanisme sunt proiectate împreună cu UC04-UC05, UC20, UC22 și UC23, astfel încât fiecare configurare validă să producă efect vizibil în dashboarduri, sarcini, proceduri automate, notificări și jurnalul de evenimente. CNAS va primi astfel nu doar funcții de administrare, ci un model operațional în care administrarea schimbă controlat comportamentul sistemului.

Oferta propune o regulă de guvernanță practică: se configurează ceea ce poate fi schimbat sigur prin versiune, aprobare, testare și audit; se implementează în cod ceea ce produce efect juridic, financiar, de securitate sau integrare critică. Această separare permite flexibilitate fără pierderea controlului. Sistemul nu va obliga CNAS să apeleze la intervenții în baza de date pentru ajustări operaționale uzuale și nu va transforma regulile sensibile în parametri liberi care pot afecta drepturi, plăți sau acces la date.

6.1 Poziționarea ofertată: configurare cu efect operațional controlat

Configurarea este tratată ca acțiune de business cu efect în sistem, nu ca modificare izolată de setări. Un serviciu electronic configurat va controla ce informații sunt vizibile, ce formular se utilizează, ce documente se solicită, ce flux se activează, ce roluri pot interveni, ce notificări se emit, ce documente se generează și ce evenimente se păstrează în audit. Această abordare transformă UC15-UC18 într-un mecanism funcțional integrat, nu într-o zonă administrativă ruptă de exploatarea zilnică.

CNAS va putea administra elementele care se schimbă frecvent și pot fi guvernate sigur: servicii electronice, formulare, câmpuri, documente obligatorii, nomenclatoare, clasificatoare, metadate, șabloane, stări de flux, termene, notificări, reguli operaționale simple, planificări de joburi și drepturi de acces. Pentru fiecare zonă configurabilă vor fi prevăzute proprietăți de control: cod, denumire, descriere, versiune, stare, dată de activare, perioadă de valabilitate, autor, motiv, istoric, dependențe și, unde natura obiectului permite, mecanism de dezactivare sau revenire.

Regulile care pot modifica drepturi, cuantumuri, obligații, plăți, semnături, integrări oficiale sau acces la date sensibile vor fi livrate prin mecanismul normal de dezvoltare, testare, release și acceptanță. În acest mod, sistemul oferă flexibilitate pentru administrarea operațională, dar păstrează disciplina necesară pentru componentele care produc efecte juridice sau financiare.

Prin această poziționare, oferta evită două extreme: rigiditatea unui sistem în care orice ajustare cere modificare de cod și riscul unui sistem în care orice regulă poate fi schimbată direct în producție. Soluția va livra o zonă de administrare autorizată, auditată și verificabilă, iar modificările configurabile vor intra în fluxuri controlate de creare, verificare, activare, monitorizare și retragere.

6.2 Acoperirea UC-urilor în stratul de configurabilitate și administrare

UC15-UC18 sunt tratate ca nucleul configurabilității și administrării operaționale. Ele definesc modul în care CNAS va controla serviciile, fluxurile, datele descriptive, șabloanele, utilizatorii și drepturile de acces. Acest nucleu este conectat direct la UC04-UC05, UC20, UC22 și UC23, deoarece efectul unei configurări se vede în spațiul de lucru, în sarcini, în execuții automate, în notificări și în jurnalizare.

Această conexiune este esențială pentru un sistem CNAS real. Configurarea unui serviciu electronic produce valoare numai atunci când serviciul poate fi inițiat, repartizat, procesat, notificat, documentat și auditat. Configurarea unui flux produce valoare numai atunci când sarcinile apar la actorii corecți, tranzițiile sunt permise doar în condițiile aprobate, iar istoria acțiunilor rămâne disponibilă. Configurarea drepturilor produce valoare numai atunci când accesul este aplicat uniform în portal, dashboard, registre, documente, rapoarte, API-uri și proceduri automate.

Prin urmare, UC15-UC18 nu sunt livrate ca ecrane administrative separate, ci ca mecanisme care guvernează comportamentul UC-urilor operaționale. Tabelul de mai jos arată rolul fiecărui UC relevant în modelul propus.

UC relevant	Capacitate livrată în soluție	Efect operațional pentru CNAS
UC15 - Configurez serviciu electronic	Administrarea serviciilor electronice, formularelor, câmpurilor, documentelor obligatorii, canalelor, vizibilității, regulilor operaționale sigure și parametrilor de activare.	Serviciile CNAS pot fi publicate, activate, ajustate și retrase controlat; fiecare serviciu va conduce spre formular, flux, documente, notificări și audit.
UC16 - Configurez flux de lucru	Definirea stărilor, tranzițiilor, actorilor, responsabilităților, acțiunilor permise, termenelor, condițiilor operaționale și legăturilor cu notificări/sarcini.	Cererile, formularele, documentele, deciziile și procedurile nu circulă liber; ele avansează prin pași autorizați și explicabili.
UC17 - Gestionez metadate și șabloane de documente	Administrarea metadatelor, nomenclatoarelor, clasificatoarelor, câmpurilor, șabloanelor de documente, parametrilor de afișare și regulilor de utilizare.	Datele, documentele și rapoartele rămân coerente, versionate și reutilizabile; modificarea unui șablon sau clasificator nu devine intervenție informală în sistem.
UC18 - Administrez utilizatori și controlul accesului	Administrarea utilizatorilor, rolurilor, grupurilor, drepturilor, ariilor de competență, delegărilor și restricțiilor la funcții/date/documente.	Accesul se aplică după rol, scop și context operațional; utilizatorul vede și execută doar acțiunile permise.
UC04-UC05 - Dashboard și sarcini	Afișarea sarcinilor, cozilor de lucru, notificărilor, termenelor, obiectelor în lucru și acțiunilor disponibile în funcție de rol și flux.	Configurările de serviciu și workflow produc muncă reală în dashboard, nu rămân doar definiții administrative.
UC20 - Execut proceduri automate	Planificarea și execuția joburilor automate, sincronizărilor, importurilor, agregărilor, recalculărilor, notificărilor și altor procese repetitive.	Procesele de volum sunt executate controlat, cu stare, rezultat, erori, reluare și raport de excepții.
UC22 - Notific utilizatori	Definirea evenimentelor, șabloanelor, destinatarilor, canalelor și regulilor de emitere a notificărilor interne/externe.	Utilizatorii primesc informații la momentul potrivit: sarcini, termene, rezultate, excepții, aprobări și acțiuni necesare.
UC23 - Jurnalizez evenimente	Păstrarea evenimentelor de business și administrare: accesări, modificări, tranziții, aprobări, configurări, execuții automate și notificări.	Sistemul devine auditabil; CNAS poate reconstrui traseul unei configurări, al unei cereri, al unei decizii sau al unui document.

6.3 Acoperirea UC15-UC23 în administrarea sistemului

Soluția va furniza un mecanism de administrare a serviciilor electronice prin care CNAS va putea defini și controla portofoliul de servicii disponibile în sistem. Un serviciu electronic va fi tratat ca obiect funcțional complet: identitate, categorie, descriere, condiții de acces, canal, formular, documente obligatorii, reguli operaționale, vizibilitate, flux asociat, rezultate posibile, șabloane de documente, notificări și parametri de activare.

Configurarea serviciului va lega zona publică de zona operațională. Pentru serviciile care au componentă publică, datele descriptive și instrucțiunile vor putea fi afișate în portal. Pentru serviciile care pot fi inițiate de solicitant sau de utilizator CNAS, formularul și documentele obligatorii vor porni fluxul de procesare. Pentru serviciile interne sau specializate, vizibilitatea și accesul vor fi controlate prin roluri și arii de competență.

Fiecare serviciu va putea avea stare operațională: draft, în verificare, activ, suspendat, retras sau arhivat, conform modelului aprobat în SRS/SDD. Activarea unei versiuni de serviciu va produce efect numai după validarea elementelor obligatorii: formular asociat, flux de lucru, drepturi de acces, șabloane, notificări unde sunt aplicabile și reguli de jurnalizare. Astfel, un serviciu nu devine disponibil în exploatare într-o formă incompletă.

Pentru CNAS, acest mecanism va reduce dependența de modificări tehnice pentru ajustări operaționale controlabile. Adăugarea sau modificarea elementelor descriptive, a documentelor solicitate, a canalelor, a termenelor administrative sau a instrucțiunilor de serviciu va putea fi gestionată prin interfețe autorizate, cu istoric și audit. Modificările care afectează calculul drepturilor, validări juridice, integrarea oficială sau plățile vor intra în fluxul de schimbare software, cu analiză, implementare, testare și acceptanță.

În scenariile UAT, UC15 va fi demonstrat prin configurarea unui serviciu de la definire până la efect operațional: serviciul apare conform regulilor de vizibilitate, formularul asociat poate fi completat, cererea intră în fluxul configurat, sarcinile se generează pentru rolurile potrivite, notificările se emit la evenimentele aprobate, iar activarea și modificările rămân jurnalizate.

UC16 - Configurarea fluxurilor de lucru

Workflow-ul propus va controla ciclul de viață al obiectelor operaționale. Cererea, formularul, dosarul, documentul, decizia, dreptul, plata, raportul sau procedura automată vor avea stare, responsabil, acțiuni permise, condiții de tranziție, termene și evenimente de audit. Sistemul va preveni lucrul într-un spațiu liber de editare și va ghida utilizatorul prin acțiunile permise de rol, stare și context.

UC16 va permite configurarea fluxurilor acolo unde regulile pot fi administrate sigur. Stările, tranzițiile, actorii, coada de lucru, termenul, mesajele de validare, notificările și acțiunile operaționale vor fi definite într-un model controlat. Pentru regulile sensibile - de exemplu reguli de calcul, validări legale, verificări obligatorii cu sisteme externe sau efecte asupra plății - workflow-ul va apela servicii backend implementate, testate și versionate, nu reguli fragile introduse liber într-un ecran.

Legătura cu UC04 și UC05 va fi directă. O tranziție configurată în workflow va putea genera sarcini, va putea muta obiectul într-o coadă de lucru, va putea declanșa notificări și va putea actualiza dashboardul utilizatorului. Utilizatorii nu vor căuta manual obiectele care necesită acțiune; sistemul va livra munca în spațiul lor operațional, cu termene, prioritate, stare și acțiuni disponibile.

Fluxurile vor fi proiectate pentru scenarii pozitive și negative. Soluția va acoperi nu doar traseul ideal de aprobare, ci și completări, returnări, suspendări, respingeri, expirări de termen, erori de integrare, anulări,

retrageri și reluări unde procesul permite. Această disciplină este importantă pentru CNAS deoarece activitatea reală conține excepții, nu doar cazuri standard.

Pentru acceptanță, Furnizorul va livra exemple de fluxuri configurate, scenarii de tranziție, matrice rol-stare-acțiune, evidențe de task generation, loguri de tranziție și cazuri UAT în care aceeași cerere trece prin mai multe stări, actori, notificări și decizii. Rezultatul verificabil va fi un workflow care produce muncă, controlează acțiuni și păstrează istoric, nu doar o diagramă.

UC17 - Metadate, nomenclatoare, clasificatoare și șabloane

Soluția va furniza CNAS un mecanism administrabil pentru metadate, nomenclatoare, clasificatoare și șabloane de documente. Aceste elemente sunt părți funcționale ale sistemului, deoarece influențează formulare, validări, documente generate, rapoarte, căutări, filtre, traduceri, exporturi și interpretarea datelor. Ele nu vor fi tratate ca tabele tehnice ascunse, ci ca obiecte guvernate prin interfețe autorizate.

Metadatele vor descrie câmpurile, tipurile de date, etichetele, ordinea de afișare, obligativitatea, regulile de afișare, valorile permise și legătura cu serviciile sau formularele. Nomenclatoarele și clasificatoarele vor avea coduri stabile, denumiri, perioade de valabilitate, stare, sursă, limbă pentru elementele cu regim bilingv, istoric și reguli de utilizare. Această structură va permite sistemului să păstreze coerența între interfață, backend, documente și rapoarte.

Șabloanele de documente vor fi administrate ca versiuni controlate. Un șablon va avea denumire, tip document, serviciu sau flux asociat, limbă, stare, dată de activare, versiune, proprietar, sursă de date și istoric de modificări. Documentele generate vor putea fi legate de versiunea de șablon utilizată, astfel încât CNAS să poată explica ulterior de ce un document a avut un anumit conținut sau format la momentul emiterii.

Soluția va susține diferențierea dintre șablon, date și logică de business. Șablonul controlează structura documentului și prezentarea. Datele sunt preluate din obiectele operaționale aprobate. Regulile de calcul, eligibilitate sau decizie rămân în servicii backend. Această separare previne transformarea editorului de documente într-un loc unde se generează reguli de business în afara controlului tehnic.

Pentru CNAS, valoarea UC17 va fi vizibilă în utilizare: aceeași metadată va alimenta formularul, căutarea, documentul și raportul; același clasificator va fi aplicat uniform în mai multe fluxuri; un șablon actualizat va produce documente corecte fără modificare de cod acolo unde conținutul este configurabil; iar orice schimbare relevantă va avea istoric și audit.

UC18 - Utilizatori, roluri și controlul accesului

Soluția va livra un model de administrare a utilizatorilor și drepturilor care separă autentificarea de autorizarea operațională. Identitatea confirmă cine este utilizatorul; rolurile, drepturile, ariile de competență și contextul procesului determină ce poate vedea și ce poate executa. Această separare este critică pentru un sistem CNAS care gestionează date personale, documente oficiale, decizii și plăți.

Administrarea accesului va permite configurarea utilizatorilor, rolurilor, grupurilor, permisiunilor, ariilor organizaționale, delegărilor și restricțiilor. Modelul va acoperi diferențe între utilizatori CNAS centrali, utilizatori teritoriali, șefi de direcție, administratori, personal de suport și alți actori autorizați definiți în SRS. Un utilizator va primi acces la funcții și date în baza rolului și a contextului, nu doar în baza faptului că este autentificat.

Drepturile vor fi aplicate uniform în interfață, servicii backend, API-uri, rapoarte, documente și proceduri automate. Interfața va ascunde acțiunile nepermise pentru claritate, dar backend-ul va rămâne limita finală

de autorizare. Această abordare previne ocolirea regulilor prin apeluri directe, linkuri salvate, exporturi sau procese automate.

Sistemul va susține principiul privilegiului minim. Utilizatorul va primi doar drepturile necesare funcției sale. Pentru acțiuni sensibile, cum ar fi aprobări, modificări de configurare, acces la date personale, exporturi sau operațiuni administrative, soluția va păstra audit detaliat și va permite separarea responsabilităților. Dacă o acțiune necesită aprobare sau verificare suplimentară, aceasta va fi tratată prin flux, nu prin încredere informală.

Pentru acceptanță, Furnizorul va demonstra scenarii de acces pe roluri: același obiect vizibil diferit pentru roluri diferite, acțiuni permise sau blocate în funcție de stare, acces la documente și rapoarte conform drepturilor, jurnalizare a administrării utilizatorilor și aplicarea restricțiilor la nivel backend. CNAS va primi matricea rol-permisiune, scenarii de test și evidențe de verificare.

UC20 - Proceduri automate și execuții operaționale controlate

Administrarea și monitorizarea procedurilor automate se realizează prin mecanisme dedicate. UC20 acoperă procesele care se execută planificat, la cerere sau în urma unui eveniment: importuri, sincronizări, verificări periodice, agregări pentru raportare, notificări recurente, recalculări, exporturi, curățări operaționale, verificări de consistență și alte procese care vor fi detaliate în SRS/SDD.

Fiecare procedură automată relevantă va avea identitate, descriere, parametri, calendar, stare, responsabil, drepturi de pornire, istoric de execuție, volum procesat, rezultat, erori, durată, obiecte afectate și posibilitate de reluare unde procesul permite. Sistemul va evita execuțiile opace de tip „a rulat sau nu a rulat”. CNAS va vedea ce s-a procesat, ce a eșuat, ce a fost omis și ce necesită intervenție.

Pentru procesele care pot produce efect asupra drepturilor, plăților, documentelor sau raportării, soluția va aplica reguli de siguranță: idempotentă unde este posibil, blocare a execuțiilor paralele periculoase, jurnalizare, control al parametrilor, verificări înainte și după execuție, raport de excepții și separarea execuțiilor de test față de producție. Această disciplină permite automatizare fără pierderea controlului operațional.

UC20 se conectează direct la UC04-UC05, UC22 și UC23. O procedură automată poate genera sarcini pentru cazuri cu excepții, poate notifica utilizatorii responsabili, poate actualiza indicatori în dashboard și va lăsa evenimente de audit. Astfel, automatizarea nu rămâne ascunsă în infrastructură; ea produce rezultate vizibile și urmărite în exploatarea CNAS.

UC22 - Notificări ca mecanism de coordonare operațională

Soluția va livra notificările ca mecanism de coordonare între sistem, utilizatori și procese. Notificările nu vor fi tratate doar ca mesaje informative, ci ca reacții controlate la evenimente de business: cerere depusă, formular înregistrat, document de completat, sarcină atribuită, termen apropiat, aprobare, respingere, rezultat disponibil, execuție automată finalizată, eroare sau acțiune administrativă relevantă.

Administrarea notificărilor va permite definirea evenimentelor declanșatoare, destinatarilor, canalelor, șabloanelor, limbii, priorității, condițiilor de emitere și istoricului. Pentru notificările interne, dashboardul și coada de sarcini vor fi canalul principal de lucru. Pentru notificările externe sau instituționale, canalele concrete vor fi stabilite în SRS/SDD în funcție de cerințe, infrastructură disponibilă și integrarea cu servicii guvernamentale relevante.

Notificările vor fi legate de obiectul operațional care le-a generat. Utilizatorul va putea ajunge din notificare la cerere, dosar, document, sarcină, raport, procedură automată sau configurație, conform drepturilor sale. Această legătură transformă notificarea din mesaj pasiv în acțiune ghidată.

Pentru CNAS, valoarea UC22 va fi reducerea muncii pierdute în căutarea manuală a obiectelor și creșterea controlului asupra termenelor, excepțiilor și responsabilităților. Sistemul va ajuta utilizatorii să vadă ce au de făcut, ce s-a schimbat și unde se cere intervenția lor.

UC23 - Jurnalizare și audit al evenimentelor

Soluția va furniza jurnalizare de business și administrare pentru evenimentele relevante ale sistemului. UC23 este mecanismul prin care acțiunile utilizatorilor, schimbările de configurare, tranzițiile de workflow, accesul la date, generarea documentelor, notificările și execuțiile automate devin verificabile. Fără acest strat, sistemul ar putea funcționa operațional, dar nu ar putea explica suficient ce s-a întâmplat.

Jurnalizarea va păstra informații relevante pentru reconstrucția evenimentelor: utilizator sau proces, dată și oră, acțiune, obiect afectat, stare inițială și stare nouă când scenariul o cere, identificator de corelare, rezultat, eroare, motiv sau comentariu unde procesul îl solicită. Pentru datele personale, soluția va evita copierea necontrolată a payload-urilor sensibile în loguri tehnice și va utiliza identificatori, referințe și metadate potrivite pentru diagnostic și audit.

Auditul va acoperi și zona de configurare. Activarea unui serviciu, modificarea unui flux, schimbarea unui șablon, ajustarea unui rol sau pornirea unei proceduri automate vor fi evenimente jurnalizate. Astfel, CNAS va putea explica nu doar deciziile produse de sistem, ci și configurația care a determinat comportamentul sistemului la un moment dat.

Pentru acceptanță, Furnizorul va demonstra scenarii în care același obiect trece prin acțiuni succesive, iar sistemul permite urmărirea traseului: cine a accesat, cine a modificat, ce tranziție s-a executat, ce document s-a generat, ce notificare s-a emis și ce configurație era activă. Rezultatul pentru CNAS va fi o memorie verificabilă a proceselor, nu doar loguri tehnice dispersate.

6.4 Operarea configurărilor, evidențe și rezultat

Soluția va introduce un ciclu de viață pentru configurările relevante. Nu orice modificare va intra direct în exploatare. Pentru serviciile electronice, fluxurile, șabloanele, metadatele, rolurile și procedurile automate, modelul propus va permite pregătirea modificării, verificarea, activarea controlată și păstrarea istoricului. Detaliile finale ale stărilor și aprobărilor vor fi confirmate în SRS/SDD, dar oferta asumă principiul de bază: configurările cu efect operațional vor fi versionate și auditate.

Acest model permite CNAS să lucreze cu versiuni active și viitoare. De exemplu, un serviciu sau șablon poate fi pregătit înainte de intrarea în vigoare a unei modificări procedurale, activat la data stabilită și păstrat istoric pentru documentele emise anterior. Fluxurile pot fi actualizate fără pierderea istoricului cazurilor deja procesate. Nomenclatoarele pot avea perioade de valabilitate, iar rolurile pot fi ajustate cu audit.

În exploatare, această disciplină reduce riscul ca o schimbare administrativă să producă efecte neclare. Fiecare configurare importantă va avea identitate, versiune, stare, autor, motiv, dată, efect și istoric. CNAS va putea vedea ce configurație a fost activă la momentul unei decizii, unui document, unei sarcini sau unei notificări.

Etapă de configurare	Ce livrează soluția	Evidență pentru CNAS
Definire / Draft	Crearea sau modificarea serviciului, fluxului, șablonului, nomenclatorului, rolului, notificării sau	Versiune draft, autor, dată, motiv, obiect modificat și dependențe identificate.

Etapă de configurare	Ce livrează soluția	Evidență pentru CNAS
	procedurii automate într-o stare care nu afectează producția.	
Verificare funcțională	Validarea completitudinii, a dependențelor, a drepturilor, a șabloanelor, a notificărilor și a efectului în fluxurile asociate.	Checklist de verificare, scenariu de test, rezultat de validare și observații.
Aprobare / Activare	Trecerea configurării în stare activă de către rol autorizat, cu dată de aplicare și jurnalizare a acțiunii.	Eveniment audit, versiune activă, dată de intrare în vigoare și utilizator responsabil.
Utilizare în proces	Aplicarea configurării în cereri, formulare, sarcini, documente, notificări, joburi sau rapoarte.	Obiecte operaționale care referă configurația activă și istoric al efectelor produse.
Retragere / Înlocuire	Dezactivarea, arhivarea sau înlocuirea controlată a unei configurări fără pierderea istoricului cazurilor procesate anterior.	Versiune nouă sau stare retrasă, motiv, dată, istoric păstrat și impact documentat.

Administrarea operațională în exploatare

Interfețele administrative ale sistemului acoperă operarea zilnică a CNAS. Aceste interfețe vor acoperi administrarea serviciilor, fluxurilor, metadatelor, șabloanelor, utilizatorilor, rolurilor, procedurilor automate, notificărilor și parametrilor operaționali. Scopul este ca operațiunile autorizate să fie executate în aplicație, nu prin acces direct la baza de date sau prin intervenții informale ale echipei tehnice.

Administrarea operațională va fi separată de dezvoltarea software. Operatorii și administratorii CNAS vor putea gestiona elementele aprobate ca administrabile, în limitele rolurilor lor. Furnizorul va documenta aceste limite în SRS/SDD, ghidul administratorului și matricea de permisiuni. Elementele care ies din zona sigur configurabilă vor intra în managementul schimbărilor, cu analiză, implementare și release.

Interfețele administrative vor include controale de căutare, filtrare, stare, versiune, istoric și audit. Pentru obiectele cu impact transversal, sistemul va arăta dependențele: un serviciu folosește un formular, un formular folosește metadate, un flux folosește roluri, o notificare folosește șablon, iar un document folosește date și versiune de șablon. Această vizibilitate ajută CNAS să evite modificările cu efecte neanticipate.

Pentru zonele cu volum sau risc operațional, administrarea va include și monitorizare. Procedurile automate, notificările și unele fluxuri vor avea stare, ultimă execuție, rezultat, erori, acțiuni de reluare și legătură cu obiectele afectate. Administratorii și rolurile operaționale autorizate vor putea urmări nu doar configurația, ci și comportamentul rezultat din configurație.

Evidențe de livrare, testare și acceptanță

Furnizorul va demonstra configurabilitatea, workflow-ul și administrarea prin livrabile și scenarii executabile. CNAS va primi nu doar descrieri ale mecanismelor, ci exemple configurate, fluxuri funcționale, matrice de drepturi, șabloane versionate, proceduri automate rulate, notificări emise și evenimente de audit disponibile pentru verificare.

Pentru UC15, evidența va include servicii configurate și activate, cu formular, documente, flux, roluri și notificări asociate. Pentru UC16, evidența va include fluxuri cu stări, tranziții, sarcini, termene și acțiuni permise. Pentru UC17, evidența va include metadate, nomenclatoare, clasificatoare și șabloane versionate. Pentru UC18, evidența va include matrice de drepturi și scenarii de acces pe roluri. Pentru UC20, evidența va include execuții automate cu rezultat și excepții. Pentru UC22, evidența va include notificări generate pe evenimente. Pentru UC23, evidența va include jurnalizarea acțiunilor de business și administrare.

Scenariile UAT vor lega aceste UC-uri de procesele operaționale end-to-end. Un scenariu complet poate porni de la configurarea unui serviciu, continuă cu depunerea unei cereri, generarea sarcinilor în dashboard, examinare, decizie, document, notificare și audit. În acest mod, CNAS verifică nu doar că ecranele administrative există, ci că ele produc efectul funcțional promis în sistem.

Documentația livrată va include descrierea zonelor configurabile, limitele configurării, regulile de activare, rolurile autorizate, procedurile de administrare, scenariile de test, matricea de drepturi, catalogul de șabloane, catalogul notificărilor, descrierea joburilor automate și exemplele de jurnalizare relevante. Aceste livrabile vor susține atât acceptanța inițială, cât și exploatarea ulterioară.

Rezultatul pentru CNAS

Prin mecanismele descrise în acest capitol, CNAS va primi o platformă funcțională administrabilă, nu doar un sistem livrat într-o configurație inițială. Serviciile pot fi definite și activate controlat, fluxurile pot produce sarcini și decizii urmărite, șabloanele și metadatele pot guverna documente și date, accesul poate fi administrat pe rol și context, procedurile automate pot fi urmărite, notificările pot coordona utilizatorii, iar auditul poate reconstrui acțiunile relevante.

Această zonă este o piesă centrală a funcționalului deoarece susține viața sistemului după go-live. Un sistem CNAS nu rămâne valoros doar prin funcțiile existente la lansare, ci prin capacitatea de a fi operat, ajustat, controlat și explicat în timp. Această capacitate este construită prin UC15-UC18 și prin legătura lor directă cu dashboardurile, sarcinile, procedurile automate, notificările și jurnalizarea.

Rezultatul urmărit este o administrare sigură și verificabilă: modificările se fac în interfețe autorizate, efectele se propagă în fluxurile operaționale, drepturile se aplică uniform, notificările ajung la actorii potriviți, procedurile automate lasă rezultat, iar jurnalul păstrează memoria deciziilor și configurărilor. Astfel, CNAS obține flexibilitate operațională fără pierderea trasabilității.

7. Interoperabilitate, MConnect și web-servicii

7.1 Rolul interoperabilității în SI „Protecția Socială”

Interoperabilitatea este o componentă centrală a SI „Protecția Socială”, deoarece procesele CNAS nu pot fi executate corect doar pe baza datelor introduse manual în sistem. Stabilirea drepturilor, verificarea condițiilor, actualizarea registrelor, calculul, plata, notificarea, raportarea și auditul depind de schimburi controlate de date cu sisteme guvernamentale, sisteme externe și Sistemul informațional financiar al CNAS.

În ofertă, interoperabilitatea este tratată ca strat arhitectural distinct, nu ca set de apeluri punctuale implementate în fiecare modul. Această separare este necesară pentru a menține controlul asupra contractelor, securității, jurnalizării, time-out-urilor, retry-urilor, erorilor, răspunsurilor externe, versiunilor de API și evidențelor de acceptanță.

Principiul de bază este că orice schimb de date trebuie să fie explicabil ulterior: de ce s-a făcut, în baza cărui proces, pentru ce obiect intern, cu ce sistem, ce payload a fost transmis sau primit, ce răspuns a rezultat, cum a fost tratată eroarea și ce efect a avut asupra cererii, dosarului, deciziei, plății sau raportului.

7.2 Cerințele de interoperabilitate și aria acoperită

Cerințele INT001-INT005 stabilesc baza tehnică: API-uri și fluxuri de date bazate pe standarde deschise, interfețe capabile să funcționeze în timp real și offline, cuplare liberă bazată pe mesaje, capacitate de configurare a unor servicii web noi și documentare corespunzătoare a API-urilor. Aceste cerințe sunt completate de Anexa 4 privind web-serviciile expuse și Anexa 5 privind web-serviciile consumate.

În același timp, interoperabilitatea activează cerințe funcționale și nefuncționale din alte zone: UC14 pentru schimb de date cu sisteme externe, UC20 pentru proceduri automate, UC22 pentru notificări, UC23 pentru jurnalizare, cerințele de securitate pentru controlul accesului, cerințele de performanță pentru timp de răspuns și cerințele de raportare pentru trasabilitatea datelor.

Cerință / zonă	Interpretare în ofertă	Evidență de acceptanță
INT001	API-urile expuse și fluxurile externe vor utiliza standarde deschise, contracte documentate, formate stabile și versionare controlată.	Catalog API, OpenAPI/WSDL, scheme payload, contract tests.
INT002	Schimburile vor suporta scenarii în timp real și procese offline/asincroane pentru fluxuri de durată, indisponibilitate externă sau procesări batch.	Scenarii real-time/offline, job logs, retry logs, PV integrare.
INT003	Integrarea va folosi cuplare liberă, mesaje și contracte clare, evitând dependențe directe între modulele business și sistemele externe.	Integration Gateway, mesaje, correlation-id, logs.
INT004	Arhitectura va permite configurarea și implementarea controlată a unor servicii web noi, prin catalog API și guvernanță de integrare.	Proces adăugare API, template contract, evidențe configurare.
INT005	API-urile expuse vor fi documentate la nivel tehnic și funcțional.	Specificații API, descriere erori, exemple request/response, ghid testare.
Anexa 4	Serviciile expuse vor fi tratate ca obligații de catalog, securitate, audit, testare și monitorizare.	Catalog servicii expuse, teste externe, log acces.
Anexa 5	Serviciile consumate vor fi tratate ca dependențe controlate, cu snapshot, timeout, retry, erori și efect asupra procesului.	Catalog servicii consumate, scenarii negative, loguri integrare.
FMS	Schimbul de date cu Sistemul informațional financiar al CNAS va fi inclus în aceeași arhitectură de interoperabilitate și reconciliere.	Specificații integrare FMS, fluxuri, reconciliere, teste.

7.3 Integration Gateway / WSAdapter ca limită controlată de integrare

Integrarea va fi concentrată într-un strat dedicat - Integration Gateway / WSAdapter - care va separa logica de business a SI „Protecția Socială” de particularitățile fiecărui sistem extern. Modulele de pensii, contribuții, beneficii, plăți, documente sau rapoarte nu vor implementa direct protocoalele externe. Ele vor solicita date sau vor transmite evenimente prin servicii interne stabile, iar Gateway-ul va gestiona adaptarea către contractele externe.

Acest model are trei efecte importante. În primul rând, limitează impactul schimbărilor externe: dacă un serviciu își modifică payload-ul sau versiunea, modificarea se izolează în adaptor. În al doilea rând, centralizează securitatea și auditul: autentificarea tehnică, autorizarea, certificatele, logurile, correlation-id-urile și evidența răspunsurilor se aplică uniform. În al treilea rând, permite testare și monitorizare mai clară: contract tests, mock-uri, scenarii negative și indicatori de disponibilitate pot fi gestionate per integrare.

Gateway-ul va păstra pentru fiecare apel sau mesaj cel puțin: sistemul extern, serviciul, operațiunea, obiectul intern afectat, utilizatorul sau procesul care a inițiat schimbul, scopul funcțional, momentul, durata, rezultatul, codul de răspuns, eroarea dacă există și referința către snapshot-ul relevant al răspunsului, acolo unde acesta trebuie păstrat pentru trasabilitate.

7.4 Integrarea cu ecosistemul e-guvernare

Soluția va fi proiectată pentru integrare cu ecosistemul guvernamental relevant: MConnect pentru schimb de date, MConnect Events pentru scenarii de evenimente acolo unde fluxurile o cer, MPass pentru autentificare, MLog pentru jurnalizarea evenimentelor critice, MNotify pentru notificări, MPay pentru fluxurile de plată în care este implicată platforma de plăți, MDocs/MDelivery/MSign/MPower acolo unde procesele aprobate și contractele de integrare le cer.

MConnect este tratat ca mecanism principal de schimb de date între autorități atunci când datele sunt disponibile prin platforma de interoperabilitate sau când procedura de conectare stabilește acest traseu. Pentru fiecare set de date consumat, se va indica scopul, temeiul legal, furnizorul de date, sistemul sursă, structura de răspuns, frecvența, erorile posibile, tratamentul indisponibilității și responsabilitatea de business.

MConnect Events este relevant pentru scenarii în care SI „Protecția Socială” trebuie să consume sau să publice schimbări de stare aproape în timp real, fără cuplare strictă între sisteme. Pentru aceste fluxuri, arhitectura va utiliza principii de procesare idempotentă, confirmare consum, partiționare logică pe obiect și reluare controlată, astfel încât același eveniment să nu producă efecte duplicate sau inconsistente.

7.5 Servicii expuse de SI „Protecția Socială”

Serviciile expuse de SI „Protecția Socială” vor fi organizate într-un catalog API. Pentru fiecare serviciu se va defini consumatorul vizat, scopul funcțional, obiectul informațional afectat, datele expuse, restricțiile de acces, metoda de autentificare/autorizare, formatul request/response, codurile de eroare, limitele de utilizare, jurnalizarea și testele de contract.

Expunerea unui serviciu nu va însemna acces liber la datele operaționale. API-urile vor expune doar datele aprobate pentru scenariul respectiv, cu filtrare, mascarea datelor unde este necesar, reguli de autorizare și audit. Dacă același obiect intern este folosit în mai multe servicii, contractele externe vor fi definite separat, astfel încât fiecare consumator să primească doar structura necesară procesului său.

Pentru serviciile publice sau instituționale care au impact asupra drepturilor, plăților sau evidențelor oficiale, contractele API vor include reguli de versionare și compatibilitate. Modificările care pot afecta consumatorii vor fi gestionate prin versiuni, comunicare și testare, nu prin schimbări directe în producție.

7.6 Servicii consumate și date externe

Serviciile consumate de SI „Protecția Socială” vor fi tratate ca surse de date autorizate sau ca verificări externe, nu ca simple apeluri tehnice. Pentru fiecare serviciu consumat se va defini ce proces îl utilizează, când este apelat, dacă răspunsul este decisiv sau informativ, cât timp este valabil răspunsul, dacă se păstrează snapshot, ce se întâmplă când serviciul este indisponibil și ce mesaj primește utilizatorul.

În fluxurile de cerere/dosar/decizie, răspunsurile externe trebuie să fie legate de obiectul intern și de acțiunea pentru care au fost solicitate. Dacă o decizie se bazează pe date externe, sistemul trebuie să poată demonstra ulterior ce răspuns a fost utilizat, când a fost obținut și din ce sursă. Această evidență este importantă pentru audit, contestații, suport și explicația deciziilor.

Indisponibilitatea unui serviciu extern nu va fi tratată uniform pentru toate procesele. Pentru verificări decisive, procesul poate fi blocat controlat până la obținerea datelor. Pentru verificări informative, procesul poate continua cu marcaj explicit. Pentru procese asincrone, apelul poate fi reluat conform politicilor de retry și calendarului de joburi. Decizia de comportament va fi documentată în catalogul de integrare și în SRS/SDD.

7.7 Integrarea cu Sistemul informațional financiar al CNAS (FMS)

Integrarea cu Sistemul informațional financiar al CNAS (FMS) este inclusă explicit în aria de interoperabilitate a SI „Protecția Socială”. FMS nu este tratat ca sistem extern auxiliar, ci ca sistem cu impact direct asupra fluxurilor financiare, comenzilor, evidenței plăților, reconciliere și raportare.

În cadrul Sarcinii 3.3, schimbul de date cu FMS va fi analizat și specificat prin contracte tehnice clare: fluxuri de date, structuri transmise, identificatori comuni, perioade de referință, stări, mesaje de confirmare, erori, reguli de reluare și reconciliere. Livrabilul 3.1 va include specificațiile tehnice de integrare cu FMS alături de celelalte sisteme guvernamentale partajate și sisteme externe.

Pentru operațiunile cu impact financiar, integrarea cu FMS va include evidență de trasabilitate: obiectul intern care a generat schimbul, documentul sau comanda asociată, valoarea, perioada, statusul transmiterii, confirmarea primită, diferențele identificate și rezultatul reconcilierii. Această abordare reduce riscul ca decizia, dreptul, comanda și evidența financiară să evolueze separat.

7.8 Evenimente, mesagerie și procese asincrone

SI „Protecția Socială” va utiliza procese asincrone pentru operațiuni de durată, schimburi de date care nu trebuie să blocheze utilizatorul, notificări, joburi periodice, raportări mari, recalculări, migrare, reconciliere și integrare bazată pe evenimente. Mesageria nu este introdusă ca tehnologie decorativă, ci ca mecanism de control al volumelor, al indisponibilității externe și al decuplării între producerea unei schimbări și consumarea ei de către alte procese.

Pentru evenimentele interne, sistemul va păstra un model clar: eveniment produs, obiect afectat, stare anterioară și nouă, timp, sursă, consumatori, rezultat și erori. Pentru evenimentele externe, catalogul de integrare va indica dacă evenimentul este produs sau consumat, ce date conține, ce cheie de partitionare se utilizează, ce reguli de idempotency se aplică și ce efect produce în sistem.

Pentru procesele care nu trebuie să fie executate în timp real, joburile și coziile de procesare vor oferi stare, progres, reluare, raport de excepții și evidență de finalizare. Utilizatorul nu trebuie să ghicească dacă procesul a rulat; interfața și logurile vor indica rezultatul și acțiunea necesară.

7.9 Semantica datelor, catalogul de integrare și modelul canonic

Un risc major în interoperabilitate este folosirea aceloraşi termeni pentru date diferite sau folosirea unor structuri diferite pentru aceeași realitate operațională. Pentru SI „Protecția Socială”, catalogul de integrare va fi legat de modelul de date și de descrierea semantică a obiectelor: persoană, plătitor, contribuție, cerere, dosar, decizie, drept, plată, document, raport, eveniment și integrare.

Pentru fiecare schimb de date se va documenta semnificația câmpurilor, tipul de date, formatul, sursa, transformările, validările, nomenclatoarele utilizate, versiunea și relația cu obiectele interne. Acolo unde datele externe sunt transformate într-un obiect intern, se va păstra trasabilitatea transformării, astfel încât CNAS să poată explica proveniența informației și regulile aplicate.

Catalogul de integrare va fi folosit și în testare: datele de test, scenariile pozitive, scenariile negative, erorile de validare și testele de regresie vor fi legate de contractele definite, nu de interpretări informale.

7.10 Securitate, audit și protecția datelor în schimbul de date

Schimbul de date va fi securizat la nivel de canal, identitate tehnică, autorizare, scop, rol și audit. Interoperabilitatea nu va permite ocolirea modelului de securitate al aplicației. Datele primite sau transmise prin integrare vor fi tratate conform aceloraşi principii de acces minim, jurnalizare și trasabilitate ca datele introduse prin interfața utilizator.

Pentru fiecare integrare se va documenta mecanismul de autentificare tehnică, certificatele sau credențialele utilizate, mediile separate de test și producție, adresele permise, regulile de rotație sau expirare, configurațiile externalizate și pașii de verificare. Credențialele nu vor fi hardcodate, iar accesul la configurările sensibile va fi limitat.

Jurnalizarea schimburilor de date va păstra suficiente informații pentru audit fără a expune necontrolat payload-uri sensibile. Pentru evenimente critice, sistemul va integra jurnalizarea de business și, acolo unde este cerut, MLog. Logurile vor permite identificarea operațiunii, obiectului afectat, rezultatului, erorii și utilizatorului sau procesului care a inițiat schimbul.

7.11 Reziliență, indisponibilitate externă și reconciliere

Integrarea cu sisteme externe trebuie să rămână controlabilă chiar și atunci când un serviciu extern răspunde lent, este indisponibil, schimbă mesajele de eroare sau livrează date incomplete. Sistemul va aplica timeouts, retry controlat, circuit breaker, cozi de reluare, dead-letter pentru erori nerecuperabile și rapoarte de excepții pentru intervenție operațională.

Pentru procesele financiare și pentru datele care influențează decizii sau plăți, reconcilierea va fi parte a mecanismului de integrare. Reconcilierea nu se limitează la verificarea tehnică a transmiterii; ea compară obiectele, valorile, perioadele, stările și confirmările, astfel încât diferențele să fie identificate și tratate.

Comportamentul la indisponibilitate va fi vizibil pentru utilizator. În loc de erori tehnice generale, interfața va indica dacă verificarea este în așteptare, dacă trebuie reluată, dacă procesul este blocat până la disponibilitatea datelor sau dacă a fost creată o excepție pentru analiză.

7.12 Monitorizare operațională și suport pentru integrări

Fiecare integrare va avea indicatori de monitorizare: disponibilitate, timp mediu de răspuns, număr de apeluri, număr de erori, retry-uri, mesaje în așteptare, mesaje eșuate, fluxuri blocate și diferențe de reconciliere. Acești indicatori vor fi utilizați atât de echipa tehnică, cât și de suportul operațional.

Pentru echipa de suport, logurile de integrare trebuie să fie utile fără acces direct la cod sau bază de date. O solicitare de suport trebuie să poată fi analizată prin correlation-id, obiect intern, serviciu extern, moment, eroare și rezultat. Dacă o integrare a afectat o cerere sau o plată, legătura trebuie să fie vizibilă în istoricul obiectului.

Runbook-urile de integrare vor descrie pașii de diagnostic: verificare disponibilitate, verificare certificate/configurații, verificare cozi, verificare erori, reluare controlată, escaladare către proprietarul sistemului extern și documentarea rezultatului.

7.13 Catalogul de integrare și pachetul de evidențe

Catalogul de integrare este instrumentul principal de control pentru interoperabilitate. El va include atât serviciile expuse, cât și serviciile consumate, inclusiv integrarea cu FMS. Pentru fiecare integrare se vor indica: cod, denumire, direcție, sistem, proprietar, scop, temei, proces CNAS, UC/anexă asociată, protocol, endpoint, mediu, payload, autentificare, autorizare, frecvență, timeout, retry, erori, audit, testare și evidență de acceptanță.

Pachetul de evidențe pentru acceptanță va include specificații API, scheme de mesaje, exemple request/response, contract tests, scenarii negative, loguri de integrare, capturi de monitorizare, rapoarte de reconciliere și proces-verbal de acceptanță a mecanismului de interoperabilitate. Astfel, acceptanța nu se bazează pe afirmația că „integrarea funcționează”, ci pe dovezi tehnice și operaționale verificabile.

Catalogul va fi corelat cu Anexa - Matricea de acoperire a anexelor funcționale - astfel încât procesele, web-serviciile, rapoartele și modelele documentare din anexele caietului de sarcini să poată fi urmărite până la specificații, implementare, testare și acceptanță.

7.14 Rezultatul urmărit pentru CNAS

Rezultatul capitolului de interoperabilitate este un sistem care comunică în mod controlat cu ecosistemul extern, fără dependențe ascunse și fără apeluri dispersate în codul fiecărui modul. CNAS va primi un mecanism în care fiecare serviciu este documentat, securizat, monitorizat, testat și legat de procesul de business pe care îl susține.

Această abordare este esențială pentru un sistem de pensii și prestații: deciziile, plățile, rapoartele și notificările trebuie să poată fi explicate prin datele utilizate, sursele accesate, schimburile efectuate și rezultatele primite. Interoperabilitatea devine astfel parte din controlul instituțional al sistemului, nu doar din arhitectura tehnică.

Artefact	Conținut minim	Utilizare în acceptanță
Catalog integrare	Servicii expuse/consumate, FMS, MConnect/MConnect Events, proprietari, scop, contracte, securitate, SLA/timeout/retry.	Bază pentru verificarea acoperirii Anexelor 4-5 și a Sarcinii 3.3.
Specificații API	OpenAPI/WSDL, payload, erori, autentificare, exemple.	Contracte tehnice aprobate și testabile.
Contract tests	Teste pozitive/negative pe fiecare serviciu relevant.	Confirmare comportament la integrare.

Loguri și monitorizare	Correlation-id, stare, durată, rezultat, eroare, obiect afectat.	Trasabilitate și diagnostic.
Reconciliere	Comparare valori, perioade, stări, confirmări și diferențe.	Confirmare pentru fluxuri financiare și FMS.
PV interoperabilitate	Rezumat testare, deficiențe, remedieri, concluzie.	Acceptanța mecanismului de schimb de date.

8. Raportare, documente, șabloane și BI

8.1 Poziționarea capitolului: raportarea ca ieșire oficială a sistemului, nu ca anexă tehnică

Furnizorul va livra componenta de raportare, documente și guvernanță a șabloanelor ca mecanism oficial de transformare a datelor CNAS în informații verificabile, documente tipizate, rapoarte operaționale, rapoarte statistice, dashboarduri, exporturi și evidențe de audit. Această componentă nu va fi tratată ca simplu instrument de generare fișiere, ci ca parte a lanțurilor funcționale prin care contribuțiile, contul individual, cererile, dosarele, deciziile, drepturile, plățile, integrările și suportul operațional devin controlabile pentru CNAS.

Pentru un sistem de dimensiunea SI „Protecția Socială”, raportarea are rol dublu. În primul rând, susține activitatea zilnică: utilizatorii trebuie să vadă liste de lucru, stări, excepții, sarcini, registre, documente generate și rezultate ale procedurilor automate. În al doilea rând, susține controlul instituțional: CNAS trebuie să poată produce statistici, indicatori, situații oficiale, agregări de venituri și cheltuieli, rapoarte de plăți, rapoarte de contribuții, rapoarte de pensii/prestații, rapoarte de audit și ieșiri pentru management.

Oferta asumă că rapoartele și documentele vor fi construite pe date pregătite, surse controlate, șabloane versionate, drepturi de acces, audit și criterii de acceptanță. Rezultatul pentru CNAS nu este doar posibilitatea de a „scoate un raport”, ci capacitatea de a explica sursa datelor, regulile aplicate, versiunea șablonului, parametrii execuției, utilizatorul care a generat rezultatul, formatul produs și condițiile de acces la informație.

În acest capitol, „raportare” include rapoarte operaționale, statistice și analitice, dashboarduri, exporturi, documente generate și șabloane. Termenul nu se limitează la rapoarte tipărite; el acoperă toate ieșirile controlate ale sistemului.

8.2 Ancorarea în UC-uri și în Functional Backbone

Componenta de raportare și documente va fi ancorată direct în cazurile de utilizare ale sistemului și în Functional Backbone-ul descris în metodologia de implementare. UC09 și UC19 reprezintă nucleul raportării, extragerii și generării de rapoarte/documente, dar soluția va fi legată și de UC11 pentru descărcarea documentelor, UC17 pentru administrarea șabloanelor și metadatelor, UC20 pentru proceduri automate și execuții de durată, UC22 pentru notificarea rezultatului și UC23 pentru jurnalizarea evenimentelor.

Această ancorare este necesară deoarece documentele și rapoartele nu apar la finalul sistemului ca ieșiri izolate. Ele sunt produse de lanțuri funcționale: cererea produce dosar, dosarul produce verificare, verificarea produce calcul sau constatare, calculul produce decizie, decizia produce document și notificare, iar efectul operațional se reflectă în plăți, registre, rapoarte și audit. Prin urmare, raportarea va fi proiectată ca parte a comportamentului instituțional al sistemului, nu ca interogare separată peste baza de date.

UC / zonă funcțională	Rol în capitolul 5	Evidență urmărită
UC09 / UC19	Extragerea, generarea și consultarea rapoartelor, documentelor și situațiilor oficiale.	Catalog rapoarte, scenarii test, output validat, audit execuție.
UC11	Descărcarea documentelor, rapoartelor și exporturilor permise utilizatorului.	Reguli de acces, jurnal descărcare, control volum/date personale.
UC17	Administrarea șabloanelor, metadatelor, nomenclatoarelor și parametrilor utilizați la generare.	Catalog șabloane, versiuni, aprobări, istoric modificări.

UC / zonă funcțională	Rol în capitolul 5	Evidență urmărită
UC20	Execuția procedurilor automate, rapoartelor grele, agregărilor și exporturilor în fundal.	Job log, stare execuție, notificare, retry, rezultat descărcabil.
UC22	Notificarea utilizatorilor când rezultatul unui raport, document sau proces automat este disponibil.	Notificare livrată, legătură cu obiectul, jurnalizare.
UC23	Auditarea generării, modificării șabloanelor, exporturilor și accesului la rapoarte/documente.	Audit trail, eveniment business, utilizator, parametri, obiect afectat.

8.3 Modelul de raportare propus

Furnizorul va organiza raportarea în categorii clare, astfel încât fiecare tip de ieșire să aibă mecanism potrivit, criterii de performanță, drepturi de acces și mod de acceptanță. Rapoartele operaționale rapide nu vor fi tratate la fel ca rapoartele statistice grele; documentele oficiale nu vor fi tratate la fel ca exporturile de lucru; dashboardurile nu vor fi tratate ca pagini decorative, ci ca intrări în procese reale de verificare și decizie.

Modelul propus separă raportarea operațională, raportarea statistică/analitică, documentele tipizate, dashboardurile, exporturile și datele publice/depersonalizate. Această separare permite CNAS să primească atât instrumente rapide pentru activitatea curentă, cât și mecanisme robuste pentru indicatori, rapoarte oficiale, controale manageriale și raportare la scară.

Categorie	Ce livrează soluția	Control aplicat
Rapoarte operaționale	Liste, registre, sarcini, stări, excepții, rezultate ale procedurilor automate și indicatori pentru activitatea zilnică.	Filtrare la sursă, acces pe rol, performanță interactivă, legătură directă cu obiectul operațional.
Rapoarte statistice și analitice	Agregări, indicatori, situații BASS, pensii, prestații, plăți, contribuții, volume, evoluții și controale interne.	Read models, tabele agregate, materialized views, joburi asincrone, validare valori.
Documente tipizate	Cereri, decizii, extrase, notificări, confirmări, rapoarte oficiale și alte documente generate din șabloane.	Șabloane versionate, parametri, sursă de date, audit generare, criterii layout/conținut.
Dashboarduri operaționale	Vizualizări native în aplicație pentru stări, cozi de lucru, alerte, indicatori și navigare către obiecte.	Role-aware views, date actualizate controlat, navigare către dosare/cereri/rapoarte.
Exporturi	Fișiere descărcabile în formate uzuale, acolo unde exportul este permis de rol și scop.	Limitare volum, execuție asincronă, jurnalizare, mascare/agregare unde este cazul.
Date publice/depersonalizate	Informații agregate sau depersonalizate pentru publicare, conform drepturilor și regulilor aprobate.	Separare de date operaționale, anonimizare/depersonalizare, control publicare.

Date operaționale	Validare / reguli	Dataset controlat	Șablon / raport	Generare / export	Audit / notificare

Figura 5.1. Lanțul de transformare a datelor în rapoarte, documente și evidențe

8.4 Date pregătite pentru raportare

Furnizorul va proiecta raportarea pornind de la surse de date pregătite pentru citire și agregare. Rapoartele nu vor fi construite prin acces liber și necontrolat la tabelele tranzacționale critice. Pentru indicatorii frecvenți, rapoartele complexe, exporturile mari și analizele statistice se vor utiliza read models, vederi

controlate, tabele agregate, materialized views sau procese batch de pregătire a datelor, în funcție de volumul și natura informației.

Această abordare protejează fluxurile tranzacționale ale sistemului. Operațiunile de căutare, deschidere dosar, salvare formular, schimbare statut, generare decizie sau consultare cont individual trebuie să rămână rapide și stabile. Rapoartele grele, exporturile masive, agregările statistice și situațiile cu perioade mari de date vor fi separate de tranzacțiile curente și executate controlat.

Fiecare sursă de date pentru raportare va avea scop, domeniu, proprietar funcțional, frecvență de actualizare, reguli de calcul, criterii de validare și restricții de acces. Pentru rapoartele oficiale, acceptanța nu va verifica doar forma fișierului generat, ci și provenienta datelor, regulile de selecție, totalurile, filtrările, tratamentul datelor personale și concordanța cu scenariile aprobate.

8.4.1 Industrializarea raportării

Pentru rapoartele statistice, rapoartele operative, profilurile, contingentele, listele recurente și indicatorii manageriali, Furnizorul va separa calculul datelor de raportare de formatul final al raportului. Soluția nu va fi construită pe interogări SQL manuale, executate punctual asupra bazei operaționale, deoarece un asemenea model produce formule greu de urmărit, dependență de persoane, rezultate nereproductibile și risc de afectare a performanței operaționale.

Soluția va introduce o fabrică instituțională de date pentru raportare: captură controlată din sistemul operațional, staging, transformări versionate, teste de calitate, data marts pe domenii, snapshot-uri de perioadă, indicatori guvernați, joburi programate, audit de generare și mecanisme de rerun. Instrumentul de raportare va consuma aceste surse pregătite și nu va conține logica principală de selecție, curățare, agregare sau reconciliere.

SQL-ul va rămâne un instrument tehnic utilizat în transformări, vizualizări materializate și modele de date, dar nu va fi mecanismul operațional prin care CNAS produce manual rapoarte instituționale. Interogările și transformările vor fi păstrate în repository, versionate, testate, documentate și executate prin pipeline-uri controlate. Astfel, raportarea devine reproductibilă, verificabilă și independentă de intervenții individuale greu de auditat.

Prin „produs de date” se înțelege un set de date pregătit pentru un scop clar: raport statistic, dashboard, profil, contingent, export sau indicator managerial. El are surse, reguli, teste, proprietar funcțional și istoric, nu doar o interogare tehnică.

8.4.2 Straturile tehnice și funcționale ale sursei de raportare

Pentru a evita ambiguitatea între datele operaționale, datele curente, istoricul modificărilor și perioadele închise, Furnizorul va organiza sursa de raportare pe straturi clare. Fiecare strat are rol, moment de actualizare și tip de control propriu. Această separare permite raportare operativă aproape de ziua curentă, raportare statistică stabilă pe perioade închise și regenerare istorică fără rescriere tăcută a rezultatelor.

Modelul propus pornește de la Operational Core și coboară controlat spre Reporting Capture/Staging, Transformări versionate, Curated Data Marts, strat semantic/indicatori și, abia la final, instrumentele de prezentare: rapoarte oficiale, dashboarduri, exporturi sau documente. În acest model, instrumentul de raportare este doar canalul de prezentare; sursa adevărată a raportului este produsul de date guvernat.

Operational Core cereri, decizii, plăți, contribuții	Capture / Staging batch, evenimente, validări inițiale	Transformări versionate reguli, curățare, normalizare	Curated Data Marts contribuții, pensii, beneficii, plăți	Indicator Layer definiții oficiale, valori de control	Reporting Tools rapoarte, dashboarduri, exporturi

Figura 5.x. Fluxul datelor de raportare: de la sistemul operațional la produse de date și rapoarte

Strat	Ce conține	Ce face	Moment / mecanism
Operational Core	Cereri, dosare, decizii, drepturi, plăți, contribuții, cont individual, audit.	Păstrează adevărul operațional și tranzacțional al sistemului.	Actualizare în timp real prin funcționalitățile sistemului.
Capture / Staging	Copii controlate ale schimbărilor, loturi, evenimente, date brute extrase.	Primește datele fără a le declara încă oficiale pentru raportare.	Joburi nocturne, batch lunar, event log, CDC unde se justifică.
Transformări versionate	Modele intermediare, reguli de curățare, normalizare, deduplicare, agregare.	Transformă datele brute în structuri coerente și testabile.	Pipeline-uri versionate, transformări testabile, data quality checks, loguri, lineage logic și rerun controlat; instrumentele exacte se dimensionează în SDD, dar mecanismul este baseline.
Curated Data Marts	Mart contribuții, mart pensii, mart beneficii, mart plăți, mart decizii, mart contingente.	Furnizează sursa principală pentru rapoarte și dashboarduri.	Refresh programat, incremental sau lunar, în funcție de tipul raportării.
Snapshot-uri de perioadă	Situația lunii/perioadei la momentul închiderii.	Permite reproducerea raportului istoric și diferențierea rectificărilor.	Proces de închidere lunară, cu valori de control și sign-off.
Indicator Layer	Definiții oficiale: beneficiar activ, plată lunară, dosar în lucru, contingent etc.	Reduce riscul ca două rapoarte să calculeze diferit aceeași noțiune.	Catalog indicatori, ownership funcțional, versionare reguli.
Reporting Tools	Rapoarte oficiale, dashboarduri, exporturi, profiluri.	Prezintă și distribuie rezultatul, fără să concentreze logica grea.	Execuție interactivă sau asincronă, cu audit de generare.

8.4.3 Scenariu descriptiv

Pentru claritate, un flux tipic de raportare poate fi descris printr-un scenariu. Un operator aprobă o decizie sau un proces automat generează o modificare de drept. În Operational Core se actualizează obiectele de business: cerere, dosar, decizie, drept, plată, document și audit. Evenimentul relevant este înregistrat: decizie aprobată, drept creat, drept suspendat, plată generată, recalculare executată sau corecție aplicată.

La momentul programat, orchestratorul de pipeline preia schimbările. Datele intră în staging cu identificator de lot, sursă, timp de extracție, hash sau marcaj de modificare, perioadă de referință și tip de operațiune. În această etapă, datele sunt capturate, dar nu sunt încă declarate drept sursă oficială pentru raportare.

Transformările versionate aplică regulile agreate: ce înseamnă beneficiar activ, ce drept este inclus în perioada de raportare, ce plată se consideră achitată, ce decizie este inițială sau rectificativă, cum se tratează suspendările, anulările, recalculările și modificările ulterioare. Testele de calitate verifică obligatorii, duplicate, valori negative nepermise, coduri în afara nomenclatoarelor, plăți fără beneficiar, drepturi fără decizie sau diferențe față de valori de control.

După trecerea testelor, datele sunt publicate în data mart-ul relevant. Dashboardurile operative pot citi din structuri curente, iar rapoartele statistice oficiale se vor baza pe snapshot-uri de perioadă. Dacă testele nu trec, pipeline-ul nu publică rezultatul final, creează error bucket și notifică responsabilul; CNAS decide asupra excepțiilor funcționale care nu pot fi rezolvate tehnic de Furnizor.

Moment	Ce se întâmplă	Rezultat controlat
Eveniment operațional	Decizie aprobată, drept modificat, plată generată, cerere procesată.	Date operaționale și eveniment auditabil.
Captură / staging	Schimbarea este preluată în lot sau prin eveniment/CDC.	Rânduri brute cu batch_id, sursă, timp, tip operațiune.
Transformare	Se aplică reguli versionate și teste de calitate.	Modele curate, erori vizibile, reguli documentate.
Publicare data mart	Datele validate devin sursă pentru rapoarte și dashboarduri.	Produs de date guvernat și reproductibil.
Închidere perioadă	Se generează snapshot lunar și valori de control.	Raport statistic regenerabil istoric.
Corecție ulterioară	Se creează ajustare, rectificare sau versiune nouă, după decizia CNAS.	Istoric păstrat, fără rescriere tăcută.

8.4.4 Reguli de actualizare

Furnizorul va aplica reguli explicite pentru modul în care schimbările operaționale se reflectă în reporting. Nu toate modificările trebuie tratate la fel. Unele actualizează profilul curent, altele creează istoric versionat, altele produc efect doar în luna curentă, iar altele generează rectificări pentru perioade închise. Această diferențiere protejează CNAS de situația în care un raport istoric se schimbă tăcut din cauza unei corecții operate ulterior.

Modelul de raportare va distinge între date curente, istoric versionat și snapshot-uri de perioadă. Datele curente susțin dashboarduri și activitate operativă. Istoricul versionat arată evoluția obiectului în timp. Snapshot-ul păstrează situația la momentul închiderii perioadei. Corecțiile ulterioare vor fi tratate prin ajustări, rectificări sau versiuni noi de raportare, nu prin rescriere neauditată a trecutului.

Situație	Tratament în sistemul operațional	Tratament în reporting
Cerere nouă	INSERT obiect cerere/dosar.	INSERT în staging; apare în data mart dosare după transformare.
Decizie aprobată	INSERT decizie și schimbare statut dosar/drept.	Eveniment nou; current view actualizat; istoric versionat.
Drept suspendat/restabilit	Schimbare statut și decizie aferentă.	Se închide versiunea veche și se inserează versiune nouă în history.
Plată anulată/corectată	Status sau operațiune de anulare/corecție.	Nu se șterge tăcut; se marchează anulare/ajustare conform regulii de raportare.
Date persoană corectate	Profil operațional actualizat.	Current view actualizat; history păstrează perioada de valabilitate dacă este relevant.

Situație	Tratament în sistemul operațional	Tratament în reporting
Corecție după luna închisă	Decizie sau ajustare ulterioară.	Ajustare în luna curentă sau raport rectificativ pentru luna afectată, conform deciziei CNAS.
Regenerare raport	Nu modifică operaționalul.	Regenerare din același snapshot sau versiune nouă dacă se aprobă rectificare.
În reporting se evită ștergerea fizică a informației relevante. Se preferă anulare, versiune, rectificare, ajustare, valid_from/valid_to și audit, pentru ca istoricul instituțional să poată fi explicat ulterior.		

8.4.5 Procesul de închidere lunară și raportarea pe perioade controlate

Pentru rapoartele statistice lunare, Furnizorul va livra un proces controlat de închidere a perioadei. Acest proces nu va consta într-o copiere manuală de tabele, ci într-un pipeline reproductibil: confirmarea loturilor operaționale relevante, captură finală a schimbărilor, transformări versionate, teste de calitate, valori de control, reconciliere, generare de snapshot și marcarea perioadei ca pregătită pentru raportare.

Închiderea lunii va permite CNAS să diferențieze raportul inițial, raportul regenerat din același snapshot și raportul rectificativ. Dacă ulterior apar corecții pentru o perioadă închisă, sistemul nu va modifica fără urmă rezultatul inițial. Corecția va fi încadrată ca ajustare în perioada curentă sau ca rectificare a perioadei istorice, conform regulilor agreate cu CNAS.

Această abordare păstrează principiul operațional existent al pregătirii separate a datelor pentru raportare, dar îl transformă într-un mecanism automatizat, auditat și repetabil. CNAS va putea vedea ce date au intrat în snapshot, ce reguli au fost aplicate, ce teste au trecut, ce excepții au rămas și cine a confirmat rezultatul.

Pas în închiderea lunară	Ce verifică / produce	Evidență
Confirmare cut-off	Perioada și loturile relevante sunt stabilite.	Calendar închidere, listă loturi, decizie de pornire.
Extract final	Se preiau schimbările rămase pentru perioada raportată.	Batch log, număr înregistrări, surse.
Transformări	Se aplică regulile versionate pentru indicatori și data marts.	Versiuni modele, execution log.
Teste de calitate	Se verifică obligatorii, duplicate, valori, referințe, praguri de variație.	Data quality report, error bucket.
Reconciliere	Se compară sursă vs. rezultat: volume, sume, totaluri, diferențe.	Reconciliation report, valori de control.
Snapshot oficial	Se marchează setul de date al perioadei.	Snapshot_id, versiune, dată, utilizator/sistem.
Publicare raportare	Rapoartele oficiale pot fi generate din snapshot.	Audit generare, output validat, parametri.

8.4.6 Instrumente și opțiuni tehnologice pentru fabrica de date de raportare

Oferta asumă utilizarea unor mecanisme specializate pe roluri distincte, nu concentrarea întregii logici în instrumentul de raportare sau în baza tranzacțională. SRS/SDD și arhitectura tehnică vor detalia dimensionarea, configurația, integrarea cu infrastructura CNAS/MCloud, politicile de operare și combinația exactă de instrumente. Proprietățile obligatorii rămân însă asumate din ofertă: transformări versionate, pipeline-uri programate, teste de calitate, audit, reluare controlată și surse de raportare pregătite.

Reporting Data Factory nu se bazează pe ideea că PostgreSQL operațional „duce totul”. Arhitectura include scheme separate de staging și raportare, materialized views, data marts, snapshot-uri de perioadă, partitionare acolo unde profilul datelor o cere, joburi de refresh controlate și mecanisme dedicate de

orchestrare și calitate a datelor. Pentru pipeline-uri și transformări, oferta asumă controale de tip Airflow/dbt/Soda/Great Expectations sau mecanisme echivalente: dependențe explicite, transformări versionate, teste automate, loguri, retry, lineage logic și rerun controlat. SDD-ul va stabili combinația exactă și dimensionarea, dar nu va amâna existența acestor controale.

Dashboardurile interne, rapoartele de management și analizele statistice vor consuma data marts, snapshot-uri și indicatori guvernați din reporting layer/semantic layer.

Componentă / instrument	Rol în soluție	Poziționare în ofertă
PostgreSQL reporting layer	Scheme de raportare, staging, data marts, snapshot-uri, tabele agregate.	Bază principală pentru raportare controlată și reproductibilă.
Materialized views	Rezultate pre-calculate pentru agregări și interogări costisitoare.	Optimizare pentru rapoarte/dashboards frecvente.
Data marts	Produse de date pe domenii: contribuții, pensii, beneficii, plăți, decizii, contingente.	Sursa principală pentru rapoarte, profiluri și dashboarduri.
Orchestrator pipeline-uri	Planifică și monitorizează pipeline-uri, dependențe, retry, alertare și rerun.	Componentă baseline pentru migrare, reporting factory, închidere de perioadă și data quality; instrumentul exact se dimensionează în SDD.
Transformări versionate	Transformări versionate, modele, teste, documentare și lineage logic.	Mecanism baseline pentru eliminarea SQL-ului manual nereproductibil; instrumentele pot include dbt Core sau echivalent.
Data quality tests	Teste de valori, duplicate, referințe, totaluri, variații și reguli funcționale.	Baseline pentru migrare, raportare și calcul; instrumentele pot include Soda/Great Expectations sau mecanisme echivalente.
Dashboard BI / semantic layer	Vizualizare managerială și operativă pe date pregătite, indicatori guvernați și agregări.	Capabilitate baseline pentru management și analiză; acces exclusiv la data marts/snapshot-uri/indicatori controlați.
JasperReports engine	Layout, generare, export și programare rapoarte oficiale.	Strat asumat de prezentare pentru rapoarte/documente; nu deține logica principală de date.

8.4.7 Catalogul de indicatori și guvernanța produselor de date

Pentru a evita situația în care două rapoarte calculează diferit aceeași noțiune, Furnizorul va livra un catalog de indicatori și produse de date. Catalogul va defini, pentru fiecare indicator important, denumirea, descrierea, regula de calcul, sursa, perioada de referință, regulile de includere/excludere, data mart-ul utilizat, responsabilul funcțional, versiunea și rapoartele care îl consumă.

Indicatori precum beneficiar activ, dosar în lucru, drept suspendat, plată lunară, plată rectificativă, contingent, restanță, cerere depusă, decizie aprobată sau beneficiar pe teritoriu nu vor fi redefiniți separat în fiecare raport. Ei vor fi definiți central, validați cu CNAS și utilizați în rapoarte, dashboarduri și exporturi prin surse pregătite.

Catalogul de produse de date va include data mart-uri, snapshot-uri, materialized views și seturi de date utilizate de rapoarte. Pentru fiecare produs de date se vor indica sursele, pipeline-ul, frecvența de

actualizare, teste, valori de control, istoricul versiunilor și legătura cu rapoartele sau dashboardurile consumatoare.

Element catalogat	Conținut minim	De ce protejează CNAS
Indicator	Definiție, formulă, sursă, perioadă, owner, versiune.	Reduce interpretările diferite între rapoarte.
Data mart	Domeniu, surse, transformări, teste, frecvență, consumatori.	Clarifică de unde vin datele și cum se actualizează.
Snapshot	Perioadă, versiune, valori control, data închiderii, stare.	Permite regenerarea istorică și rectificarea controlată.
Raport / dashboard	Parametri, sursă, indicatori, drepturi, audit, output.	Leagă raportul de sursa declarată și de evidența de generare.
Pipeline	Pași, dependențe, retry, alertare, teste, owner tehnic.	Face vizibil ce se întâmplă înainte ca raportul să fie disponibil.

Anexele privind rapoartele și modelele de documente vor fi transformate în registre controlate: catalog de rapoarte, catalog de documente/șabloane și catalog de indicatori. Pentru fiecare raport sau model documentar se va defini sursa de date, proprietarul funcțional, parametrii, frecvența, regulile de includere/excludere, formatul de ieșire, drepturile de acces, auditul de generare și criteriile de validare.

Rapoartele din anexă nu vor fi tratate ca liste statice de fișiere de produs. Ele vor fi analizate ca rezultate ale unor produse de date și ale unor procese operaționale. Acolo unde raportul se bazează pe date voluminoase sau perioade închise, sursa lui va fi data mart-ul sau snapshot-ul aferent, nu interogarea directă a tabelelor operaționale. Acolo unde raportul are rol operativ, sursa poate fi un read model actualizat periodic sau o vizualizare materializată controlată.

Modelele de cereri, decizii și rapoarte vor fi gestionate prin guvernanța șabloanelor. O modificare de șablon nu va fi tratată ca editare informală de document, ci ca versiune controlată, cu proprietar, dată de activare, istoric, test de generare și audit. În acest mod, anexele documentare ale caietului sunt transformate în mecanism administrabil, nu în fișiere izolate dependente de intervenții manuale.

8.4.8 Reguli de proiectare care protejează oferta și implementarea

Pentru a evita diferențe de interpretare între CNAS și Furnizor, proiectarea raportării va porni de la reguli explicite. Fiecare raport statistic sau operativ important va avea sursă de date declarată, produs de date alimentator, indicatori utilizați, perioadă de referință, mecanism de actualizare, comportament la corecții, valori de control și audit de generare. Aceste elemente vor fi stabilite în SRS/SDD, catalogul de rapoarte și catalogul de indicatori.

Furnizorul nu va presupune unilateral regulile de includere/excludere, momentul de actualizare, modul de tratare a corecțiilor istorice sau condițiile de rectificare. Acolo unde regula este funcțională, CNAS va decide ca autoritate asupra procesului și datelor; Furnizorul va pregăti opțiuni, impact, recomandări și mecanismul tehnic de implementare.

Prin această disciplină, oferta protejează ambele părți. CNAS primește rapoarte explicabile, stabile și verificabile. Furnizorul poate implementa și testa raportarea pe reguli aprobate, fără ca fiecare raport să devină un caz separat de interpretare tehnică sau SQL manual.

Un „read model” este o structură pregătită pentru citire rapidă și raportare, diferită de tabelele tranzacționale folosite la salvarea operațiunilor. Scopul lui este performanța și stabilitatea raportării, fără a compromite integritatea datelor operaționale.

8.5 Raportare la scară: până la 150 de rapoarte și execuție în fundal

Furnizorul va integra/configura setul de rapoarte solicitat pentru SI „Protecția Socială”, inclusiv volumul de până la 150 de rapoarte prevăzut în documentația de achiziție. Acest volum va fi gestionat prin catalog de rapoarte, clasificare pe domenii, proprietari funcționali, surse de date, parametri, formate, drepturi de acces, criterii de acceptanță și reguli de performanță.

Rapoartele simple și necesare activității curente vor fi disponibile interactiv, cu filtrare și paginare la sursă. Rapoartele de durată sau cu volum mare vor fi executate asincron, prin joburi controlate. Utilizatorul va putea iniția raportul, va vedea starea execuției unde este relevant, va primi notificare la finalizare și va descărca rezultatul conform drepturilor sale. Execuția va păstra parametrii, utilizatorul, momentul, durata, rezultatul și eventualele erori.

Prin această separare, Furnizorul va îndeplini cerința de raportare la scară fără a transforma rapoartele în factor de degradare a sistemului. CNAS va primi rapoarte utilizabile, dar și control operațional asupra momentului, volumului, accesului, auditului și impactului asupra performanței.

Tip de raport / proces	Comportament propus	Evidență de acceptanță
Raport operațional scurt	Execuție interactivă, paginare, filtrare la sursă, rezultat imediat.	Scenariu de test, timp răspuns, acces pe rol.
Raport statistic/analitic greu	Job asincron, sursă agregată, notificare la finalizare, fișier descărcabil.	Job log, output validat, notificare, audit execuție.
Export masiv	Limitare/paginare sau execuție în fundal, cu reguli de acces și jurnalizare.	Registru export, parametri, volum, utilizator, rezultat.
Raport periodic	Planificare controlată, execuție monitorizată, istoric rezultate.	Calendar execuții, stare job, rezultate păstrate.
Raport oficial/managerial	Validare conținut, totaluri, agregări, sursă, versiune șablon și aprobare funcțională.	Raport acceptat, criterii valori/layout, sign-off CNAS.

8.6 JasperReports ca mecanism controlat de raportare și documente

JasperReports este motorul asumat pentru generarea rapoartelor și documentelor controlate, integrat în aplicație și alimentat din surse de date guvernate. JasperReports nu este locul în care se ascunde logica critică a sistemului: regulile decisive de calcul, validare, acces, eligibilitate, decizie și securitate rămân în backend, modelul de date și serviciile controlate ale aplicației.

Rolul platformei de raportare este să genereze, prezinte, exporte și tipărească rapoarte și documente pe baza datelor pregătite. Drepturile de vizualizare, configurare, modificare și publicare a șabloanelor vor fi atribuite strict rolurilor autorizate. Administratorii funcționali sau tehnici desemnați vor putea gestiona rapoartele în limitele aprobate, fără acces liber la structurile operaționale ale bazei de date și fără posibilitatea de a ocoli regulile backend.

În această arhitectură, JasperReports este strat de prezentare și execuție controlată a rapoartelor, nu motor principal de calcul statistic. Definițiile de indicatori, selecțiile complexe, curățarea datelor, agregările, regulile de perioadă și snapshot-urile sunt gestionate în reporting layer, data marts și transformări versionate. Această separare permite schimbarea formatului unui raport fără schimbarea formulei de calcul și verificarea formulei fără dependență de șablonul vizual.

Configurarea sau modificarea unui raport/șablon va fi tratată ca schimbare guvernată. Fiecare versiune va avea autor, motiv, data activării, criterii de verificare, istoric și, unde natura modificării permite, posibilitate

de revenire la versiunea precedentă. Această abordare oferă flexibilitate CNAS, dar păstrează controlul asupra conținutului, datelor, performanței și auditului.

8.7 Documente, șabloane, exporturi și dashboarduri

Furnizorul va trata documentele generate de sistem ca artefacte oficiale, nu ca fișiere auxiliare. Cererile, deciziile, notificările, extrasele, confirmările, rapoartele și alte documente tipizate vor fi generate din șabloane versionate, cu parametri expliciți și surse de date identificate. Pentru fiecare document trebuie să poată fi determinat ulterior ce șablon a fost utilizat, ce versiune era activă, cine a generat documentul, când a fost generat, pentru ce obiect operațional și cu ce date relevante.

Documentul generat poate susține comunicarea unei decizii, justificarea unei acțiuni, confirmarea unei situații, transmiterea unei informații către beneficiar sau evidența unui proces CNAS. Din acest motiv, acceptanța documentelor va verifica atât layout-ul și lizibilitatea, cât și datele incluse, condițiile de generare, limba, parametrii, metadatele, drepturile de acces și auditul generării.

Pentru decizii, documente aferente dosarelor, extrase și notificări, generarea va fi legată de starea obiectului și de drepturile utilizatorului. Un document oficial nu va fi generat arbitrar dintr-un ecran dacă obiectul nu se află într-o stare permisă sau dacă utilizatorul nu are drept de acțiune. Backend-ul va aplica aceste reguli indiferent de canalul de acces.

Guvernanța șabloanelor

Furnizorul va livra un model de guvernanță pentru șabloane, aplicabil rapoartelor, documentelor tipizate, notificărilor și exporturilor standardizate. Șabloanele vor fi gestionate într-un catalog centralizat, cu cod/nume, domeniu, scop, proprietar funcțional, sursă de date, parametri, format de ieșire, limbă, versiune, stare, dată de activare și criterii de acceptanță.

Ciclul de viață al unui șablon va include stări controlate: draft, în verificare, aprobat, activ, retras sau arhivat, după modelul final agreat cu CNAS în SRS/SDD. Activarea unei versiuni noi se va realiza numai după verificare funcțională și, pentru documentele sau rapoartele cu impact instituțional, după aprobarea rolurilor autorizate CNAS. Versiunile relevante vor fi păstrate pentru trasabilitate.

Această guvernanță permite CNAS să adapteze documentele și rapoartele la schimbări normative sau operaționale fără modificări informale în producție și fără pierderea trasabilității. Modificarea unui șablon nu este tratată ca simplă editare de text; ea poate afecta decizia comunicată, datele afișate, raportarea, drepturile utilizatorilor și auditul.

Element guvernat	Ce se controlează	Rezultat pentru CNAS
Catalog șabloane	Lista rapoartelor, documentelor, notificărilor și exporturilor standardizate.	Inventar clar al ieșirilor sistemului și al proprietarilor funcționali.
Versionare	Versiuni active, istorice, retrase, data activării și motivul modificării.	Posibilitate de explicare ulterioară a documentelor generate.
Parametrizare	Parametri disponibili, valori permise, validări și sursa datelor.	Generare controlată, fără introduceri arbitrare sau interpretări ascunse.
Aprobare	Review funcțional, testare, confirmare CNAS și activare.	Șabloane oficiale activate numai după verificare.
Audit	Autor, acțiune, dată, obiect afectat, parametri și rezultat.	Trasabilitate pentru modificare, generare, export și publicare.

Draft	Verificare	Aprobare CNAS	Activare	Utilizare	Retragere / arhivare

Figura 5.2. Ciclul de viață al unui șablon guvernat

Exporturi, date personale și control al difuzării

Furnizorul va implementa exporturile ca acțiuni controlate de rol, scop, obiect, volum și audit. Exportul nu va fi tratat ca funcție generică disponibilă automat oricărui utilizator care vede o listă în interfață. Datele cu caracter personal, datele cu impact financiar, datele privind drepturi/prestații, datele de plăți și datele agregate sensibile vor fi supuse regulilor de acces și jurnalizare.

Pentru liste generale, dashboarduri, exporturi și rapoarte statistice se vor aplica reguli de minimizare, mascare, agregare sau depersonalizare, în funcție de scop și de rol. IDNP și alte date personale vor fi afișate integral numai acolo unde rolul, contextul și scopul operațional justifică vizibilitatea. Pentru exporturile masive se vor putea aplica limitări, execuție asincronă, aprobare, împărțire pe loturi sau reguli de retenție a fișierului generat.

Fiecare export relevant va produce eveniment de audit: utilizator, rol/context, obiect sau raport, parametri, volum, moment, format și rezultat. Astfel, CNAS primește control asupra difuzării informațiilor, iar sistemul poate explica ulterior cine a extras date, în ce scop operațional și din ce sursă controlată.

Dashboarduri operaționale și legătura cu fluxurile de lucru

Dashboardurile vor fi livrate ca instrumente de lucru, nu ca simple vizualizări decorative. Ele vor afișa indicatori, sarcini, stări, excepții, alerte și rezultate relevante pentru rolul utilizatorului și vor permite navigarea către obiectul operațional: plătitor, persoană, cont individual, cerere, dosar, decizie, plată, raport, job sau integrare.

În acest model, dashboardul nu concurează cu raportarea statistică, ci o completează. Dashboardul susține activitatea curentă și controlul operațional; rapoartele statistice și analitice susțin analiza instituțională, managementul și raportarea oficială. Ambele vor utiliza surse de date controlate, reguli de acces și audit.

Furnizorul va proiecta dashboardurile împreună cu fluxurile de lucru. Indicatorii afișați trebuie să aibă sens operațional: număr de sarcini în așteptare, dosare cu termen depășit, rapoarte generate, joburi eșuate, integrări indisponibile, documente în așteptare, excepții de date sau volume relevante pentru management. Fiecare indicator important va avea definiție, sursă și criteriu de validare.

8.8 Validarea rapoartelor, documentelor și șabloanelor

Furnizorul va pregăti acceptanța raportării și documentelor prin scenarii de testare și criterii explicite. Pentru rapoarte, verificarea va acoperi sursa datelor, filtrele, parametrii, totalurile, agregările, tratamentul valorilor lipsă, drepturile de acces, performanța și formatul de export. Pentru documente, verificarea va acoperi șablonul, datele completate, condițiile de generare, limbajul, layout-ul, metadatele și auditul.

CNAS va participa ca autoritate funcțională la validarea rapoartelor și documentelor oficiale. Furnizorul va pregăti eșantioane, seturi de date controlate, comparații cu valori așteptate, cazuri pozitive și negative, precum și evidențe de execuție. Observațiile CNAS vor fi urmărite prin registru de feedback, defecte sau change control, după natura intervenției.

Pentru rapoartele de volum mare și exporturile masive, acceptanța va include și comportamentul operațional: execuție în fundal, notificare, descărcare, audit, durată, impact asupra sistemului și tratarea

erorilor. Astfel, un raport nu este acceptat doar pentru că se deschide, ci pentru că poate fi folosit în condiții reale fără a afecta procesele critice.

Obiect validat	Ce se verifică	Evidență transmisă CNAS
Raport operațional	Date, filtre, acces, navigare către obiect, timp de răspuns.	Scenariu test, output, timp execuție, observații.
Raport statistic/analitic	Agregări, totaluri, perioade, sursă, performanță, execuție fundal.	Set date, rezultat, job log, criterii acceptate.
Document tipizat	Șablon, date completate, condiții generare, layout, audit.	Exemple generate, versiune șablon, metadate, audit.
Șablon	Parametri, limbă, versiune, proprietar, stare, aprobare.	Catalog șabloane, istoric modificări, decizie activare.
Export	Rol, scop, volum, format, mascarea datelor, jurnalizare.	Registru export, parametri, rezultat, eveniment audit.

8.9 Evidențe și rezultat pentru raportare

Furnizorul va preda pentru această componentă un pachet de livrabile și evidențe care permite CNAS să administreze, verifice și opereze raportarea și documentele după go-live. Livrabilele nu vor acoperi doar fișierele de raport, ci întregul mecanism: catalog, surse de date, șabloane, reguli de acces, audit, scenarii de testare, ghiduri și criterii de acceptanță.

Livrabil / evidență	Conținut minim	Valoare pentru CNAS
Catalog rapoarte	Lista rapoartelor, domeniu, scop, proprietar, parametri, sursă, format, acces, performanță.	Control asupra portofoliului de raportare.
Catalog șabloane	Documente, decizii, notificări, rapoarte tipizate, versiuni, stări și proprietari.	Guvernanță documentară și trasabilitate.
Model date pentru raportare	Read models, vederi, tabele agregate, surse, frecvențe, reguli validare.	Raportare stabilă și performantă.
Matrice acces rapoarte/exporturi	Roluri, acțiuni, vizibilitate date, export permis, mascare/agregare.	Control asupra datelor personale și sensibile.
Pachet testare raportare/documente	Scenarii, date de test, rezultate, defecte, retestări și acceptanță.	Evidență pentru UAT și acceptanță.
Ghid administrare rapoarte/șabloane	Instrucțiuni pentru gestionare, versionare, activare, retragere și audit.	Exploatare independentă și controlată după go-live.
Rapoarte de performanță pentru ieșiri critice	Timp execuție, volum, joburi, impact, recomandări de operare.	Control asupra rapoartelor grele și exporturilor.

Rezultatul propus pentru CNAS

Prin această abordare, CNAS va primi o componentă de raportare și documente care poate fi exploatată, verificată și dezvoltată ulterior. Rapoartele vor avea surse de date controlate, documentele vor fi generate din șabloane versionate, exporturile vor fi guvernate prin drepturi și audit, iar rapoartele grele vor fi executate separat de fluxurile tranzacționale critice.

Capitolul 5 completează Functional Backbone-ul sistemului: datele care intră în fluxuri, deciziile produse, plățile inițiate, integrările apelate și acțiunile utilizatorilor devin vizibile prin rapoarte, documente, dashboarduri, exporturi și audit. Astfel, SI „Protecția Socială” nu livrează doar funcționalitate operațională,

ci și capacitatea CNAS de a controla, explica și raporta activitatea instituțională pe baza unor evidențe consistente.

Furnizorul va livra această componentă în aceeași logică de delivery assurance aplicată întregului proiect: cerințe legate de UC-uri, șabloane și rapoarte proiectate în SRS/SDD, implementare incrementală, testare pe scenarii, feedback CNAS, evidențe de acceptanță, documentație de administrare și transfer operațional. Rezultatul final va fi un mecanism de raportare și guvernanță documentară care susține activitatea zilnică, controlul managerial, auditul, comunicarea oficială și dezvoltarea ulterioară a sistemului.

Prin completarea reporting layer-ului cu staging, transformări versionate, data marts, snapshot-uri, indicatori guvernați și pipeline-uri controlate, componenta de raportare devine mecanism instituțional de producere a datelor, nu doar mecanism de afișare. CNAS va putea urmări ce date au alimentat fiecare raport, ce reguli au fost aplicate, ce perioadă a fost utilizată, ce versiune a fost generată și cum poate fi reprodus rezultatul ulterior.

Continuitatea față de modelul actual de rapoarte și diferența de abordare

În sistemele istorice bazate pe Oracle Forms / Oracle Reports, raportul este de regulă perceput de utilizator ca rezultat final: se selectează parametrii, se rulează raportul, se obține un document sau un export. Noul SI „Protecția Socială” va păstra această logică de utilizare acolo unde ea este firească pentru operatori și specialiști: utilizatorul va continua să lucreze cu rapoarte, parametri, documente generate, exporturi și rezultate verificabile.

Diferența propusă nu se află în gestul utilizatorului de a genera un raport, ci în mecanismul prin care raportul este alimentat. În modelul propus, raportul nu va fi locul principal în care se concentrează selecția complexă, curățarea datelor, agregarea statistică, tratarea corecțiilor, închiderea de perioadă și logica indicatorilor. Aceste responsabilități vor fi mutate într-un strat de date pregătite pentru raportare: staging, transformări versionate, data marts, snapshot-uri de perioadă, indicatori guvernați, valori de control și audit de generare.

Această schimbare permite păstrarea continuității pentru utilizatorul final, dar reduce dependența instituției de rapoarte construite ca interogări individuale greu de urmărit. Raportul devine forma de prezentare a unui produs de date controlat, nu locul unde se reinventează manual logica de calcul. Astfel, același indicator poate fi utilizat în raport statistic, dashboard managerial, export sau profil operațional fără ca formula lui să fie duplicată în fiecare ieșire.

Pentru CNAS, beneficiul principal este reproductibilitatea. Un raport generat pentru o perioadă închisă trebuie să poată fi explicat ulterior: din ce snapshot a fost generat, ce versiune de indicatori a folosit, ce transformări au fost aplicate, ce valori de control au fost obținute, cine l-a generat și dacă ulterior a existat o rectificare. În această abordare, instrumentul de raportare rămâne stratul de prezentare, iar adevărul statistic este administrat în reporting layer și în data marts.

Prin urmare, modernizarea nu elimină nevoia de rapoarte tipizate și exporturi oficiale. Dimpotrivă, le așază pe o bază mai sigură. Utilizatorii CNAS vor primi rapoarte într-o formă familiară, iar instituția va primi un mecanism mai controlabil pentru sursa datelor, formule, snapshot-uri, rectificări, audit și regenerare istorică.

9. Arhitectura soluției, stiva tehnologică, deployment și operabilitate

9.1 Sumar executiv al capitolului

Furnizorul va livra pentru SI „Protecția Socială” o arhitectură web enterprise în care stiva tehnologică, operabilitatea și continuitatea operațională sunt proiectate împreună. Soluția nu va fi prezentată ca enumerare de produse, limbaje și infrastructură, ci ca un ansamblu de straturi funcționale și tehnice care susțin procesele CNAS: acces utilizator, reguli de business, workflow, integrare, batch, date operaționale, raportare, audit, observabilitate, deployment și suport.

Decizii canonice privind stack-ul tehnologic enterprise

Tabelul de mai jos fixează interpretarea termenilor tehnici din ofertă. Pentru SI „Protecția Socială”, componentele critice de asincronie, caching, căutare, raportare analitică și calitate a datelor sunt asumate ca parte a baseline-ului enterprise al soluției și sunt tratate ca tehnologii open-source/fără licențe comerciale obligatorii în oferta tehnică. SDD-ul nu va decide existența lor, ci va detalia dimensionarea, configurația, politicile de operare, integrarea cu MCloud/STISC și limitele de exploatare. Această regulă elimină citirea ambiguă a tehnologiilor menționate în capitolele tehnice și reduce riscul de dispute comerciale după contractare.

Componentă / mecanism	Statut în ofertă	Regulă de utilizare / limită de interpretare
Java 25 LTS / Spring	Stack aplicativ asumat	Nucleul backend pentru reguli, tranzacții, API-uri, securitate aplicativă, workflow, batch și servicii comune. Unde documentul folosește „Java/Spring”, sensul este această linie de stack.
React+TypeScript	Stack frontend asumat	Pentru componenta frontend se propune **React + TypeScript**, ca tehnologie modernă și larg adoptată pentru aplicații web complexe, cu multe formulare, registre, dashboarduri și componente reutilizabile. Backend-ul Java/Spring Boot expune serviciile prin API-uri REST/OpenAPI, ceea ce asigură separarea clară între interfață, logica de business și integrarea cu sistemele externe.
UI styling	HTML5, CSS/SCSS, design system/MUD	Aliniere cu principiile Modelului Unitar de Design și cu cerințele de accesibilitate/usability
Contracte API	OpenAPI / REST	Separare clară între frontend și backend, testare contracte, versionare și documentare tehnică
PostgreSQL	Bază relațională asumată	Baza relațională principală pentru date operaționale, istoric, audit, configurări și structuri relaționale.
JasperReports	Motor de rapoarte/documente asumat	Motorul de generare pentru rapoarte oficiale și documente. Logica principală de selecție, curățare, agregare și indicatori rămâne în reporting layer/data marts, nu în șablonul de raport.
Containerizare, Kubernetes/Helm (MCloud)	Strat de deployment asumat	Soluția este proiectată pentru operare în MCloud prin artefacte containerizate, charturi/manifestări de deployment, configurări pe medii, health checks, rollout/rollback, secrets management și runbook. Dacă STISC/MCloud oferă servicii gestionate echivalente, acestea se integrează fără schimbarea arhitecturii aplicative și fără reducerea cerințelor de operare.

Componentă / mecanism	Statut în ofertă	Regulă de utilizare / limită de interpretare
Integration Gateway / WSAdapter	Mecanism arhitectural asumat	Responsabilitate centralizată pentru schimburi externe: contracte, autentificare tehnică, timeout/retry, audit, snapshot, monitorizare și tratarea erorilor.
Spring Batch / workers / scheduler	Mecanism asumat pentru procese de durată	Baza pentru joburi batch, importuri, recalculări, notificări programate, refresh reporting și procese asincrone coordonate.
Kafka / message broker / event streaming	Baseline enterprise pentru asincronie și decuplare	Oferta asumă existența unui strat de mesagerie/broker pentru evenimente, notificări, procese asincrone, retry și decuplare producer/consumer. Configurația exactă, topicurile/queue-urile, politicile de retenție, securitatea și dimensionarea se detaliază în SDD și sizing, dar prezența mecanismului este obligatorie, nu este opțională.
Redis / cache engine	Baseline asumat pentru cache și coordonare tehnică	Cache-ul distribuie citirile frecvente, reduce presiunea pe baza operațională, susține rate limiting/coordonare tehnică și păstrează date temporare reconstruibile. Nu este sursă de adevăr și nu stochează date juridice/financiare critice ca sistem de evidență.
Elasticsearch	Baseline asumat pentru căutare avansată	Oferta asumă un motor de căutare dedicat pentru dosare, persoane, plătitori, documente, autocomplete, audit/log și volume istorice. PostgreSQL rămâne sursa de adevăr; indexul de căutare este derivat, versionat și reconstruibil.
Airflow/dbt/Soda sau echivalent	Baseline asumat pentru pipeline-uri, transformări și data quality	Oferta asumă existența unui mecanism industrializat pentru orchestrare, transformări versionate, teste de calitate, lineage logic, loguri, retry și rerun. SDD-ul stabilește combinația exactă de instrumente și modul de operare, nu dacă aceste controale există.
Object storage compatibil S3 sau echivalent	Mecanism asumat de stocare documente	Conținutul fișierelor, atașamentelor, exporturilor mari și documentelor generate este păstrat în storage aprobat; PostgreSQL păstrează metadate, drepturi, checksum, stare și audit. Mențiunea S3 descrie compatibilitatea de interfață, nu impunerea unui produs anume.

Java 25 LTS / Spring, React și PostgreSQL formează nucleul aplicativ și de date asumat al soluției. Kubernetes, Helm, containerizarea și mecanismele de deployment formează stratul de execuție și operare. Între aceste două niveluri, Furnizorul va livra platforma aplicativă CNAS: servicii comune, mecanisme de workflow și taskuri, gateway de integrare, audit business, procesări de durată, documente, notificări, raportare industrializată, cache, căutare, versionarea bazei de date, observabilitate și controlul release-urilor.

Acest capitol fixează explicit unde se pune presiunea arhitecturală. Fiecare strat are rol, responsabilitate, mecanisme interne și evidență de acceptanță. Beneficiarul nu trebuie să deducă ulterior dacă o funcționalitate este „în aplicație”, „în infrastructură” sau „în raportare”. Oferta stabilește de acum structura logică a soluției, iar SRS/SDD vor detalia configurația finală, volumele, contractele, mediile și parametrii de operare.

Complexitatea arhitecturală este asumată împreună cu mecanismele de exploatare. Furnizorul nu va livra CNAS o „navă spațială” dificil de întreținut, ci o platformă enterprise însoțită de manualul de pilotaj: runbook operațional, proceduri de deployment, proceduri de incident, verificări de backup/restore, monitorizare,

instrucțiuni de reluare a joburilor, ghiduri pentru integrări și sesiuni de transfer tehnic. Astfel, beneficiarul primește nu doar componente moderne, ci și capacitatea documentată de a le opera și controla.

Strat	Ce livrează soluția	De ce este critic pentru CNAS
Frontend & experiență utilizator	React, UI shell, componente MUD, formulare, validări, navigare pe roluri, dashboarduri.	Operatorii lucrează pe fluxuri, nu pe ecrane izolate; interfața trebuie să reducă erorile și să ghideze acțiunile.
Application & API	Java 25 LTS / Spring, servicii de domeniu, API-uri, validări backend, tranzacții, OpenAPI.	Regulile cu efect juridic, financiar sau de securitate trebuie aplicate în backend, nu doar în interfață.
Shared Services / Functional Backbone	workflow, taskuri, documente, notificări, audit, clasificatoare, șabloane, configurări.	Cererile, dosarele, deciziile și documentele nu trebuie reinventate separat în pensii, beneficii și contribuții.
Integration & Async Processing	Integration Gateway, batch/workers, scheduler/orchestrare, broker de mesaje.	Sistemul trebuie să gestioneze procese lungi, servicii externe indisponibile, retry, erori și reluări controlate.
Data & Reporting	PostgreSQL operațional, istoric, data marts, snapshot-uri, materialized views, transformări versionate.	Rapoartele grele și închiderile de lună nu trebuie să afecteze lucrul operatorilor sau să devină SQL manual nereproductibil.
Operations & Continuity	CI/CD, observabilitate, logs/metrics/traces, backup/restore, config/secrets, MCloud/Kubernetes/Helm.	Sistemul trebuie instalat, monitorizat, diagnosticat, restaurat, actualizat și predat în mod controlat.

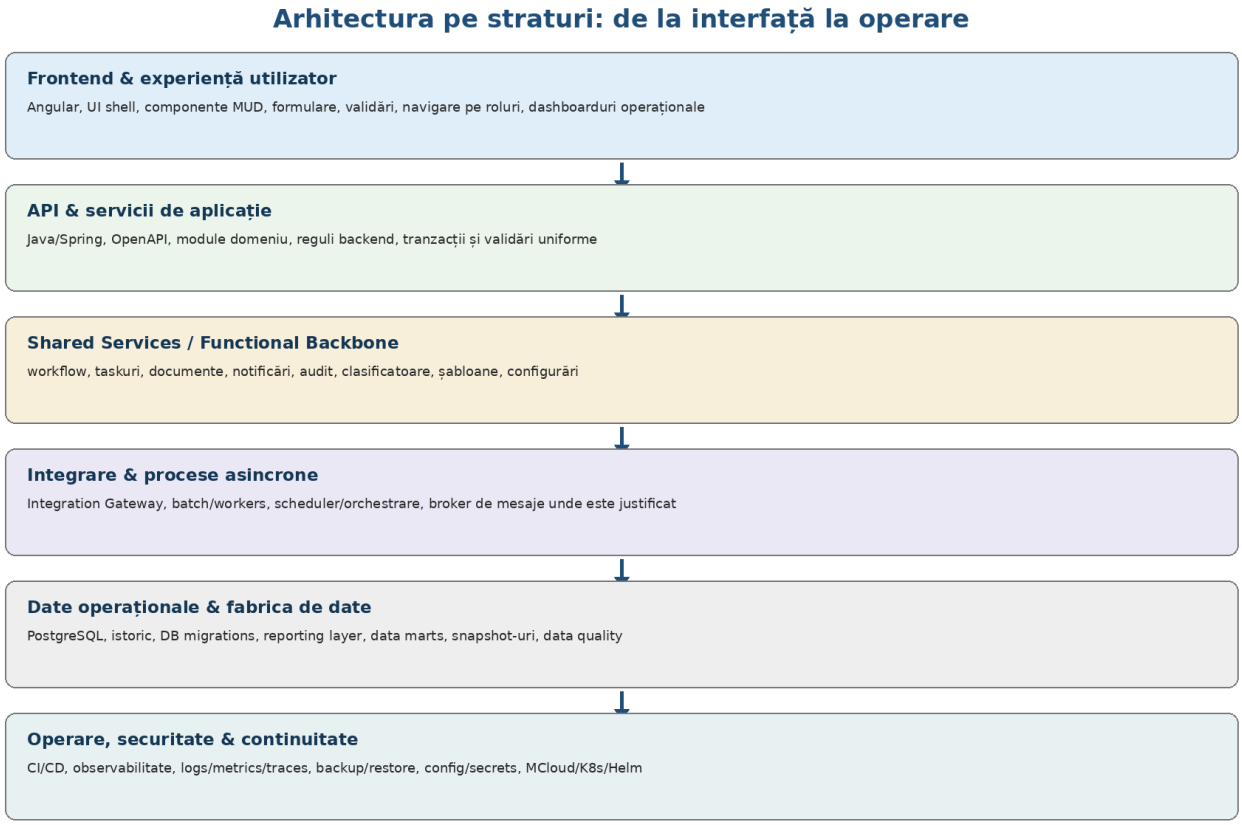


Figura Arhitectura pe straturi: fiecare strat are responsabilitate și mecanisme proprii

9.2 Poziționarea arhitecturii: tehnologie ca mecanism de control

Furnizorul va proiecta arhitectura SI „Protecția Socială” ca mecanism de control operațional. Tehnologia nu este aleasă pentru a bifa un stack modern, ci pentru a reduce riscuri concrete: fragmentare funcțională, reguli aplicate inconsistent, acces necontrolat la date personale, rapoarte lente, procese batch opace, integrări fragile, migrare greu de reconciliat, release-uri greu de reprodus și suport dependent de persoane.

Această poziționare răspunde naturii sistemului CNAS. Contribuțiile, contul individual, pensiile, prestațiile, deciziile, plățile, raportarea și interoperabilitatea produc efecte instituționale. O arhitectură suficientă pentru aplicații simple nu este suficientă aici. Sistemul trebuie să păstreze istoric, să explice decizii, să ruleze procesări masive, să se integreze cu servicii guvernamentale, să producă rapoarte reproductibile și să rămână operabil după go-live.

Prin urmare, capitolul separă explicit straturile și mecanismele interne ale soluției. Java 25 LTS / Spring, React și PostgreSQL sunt puncte de plecare; valoarea arhitecturală reală apare în modul în care sunt organizate serviciile comune, workflow-ul, integrarea, batch-ul, datele, observabilitatea, CI/CD-ul, securitatea și continuitatea. Fără acest strat aplicativ și operațional, sistemul ar avea limbaj, interfață, bază de date și containere, dar nu ar avea mecanism instituțional complet.

9.3 Principiul arhitectural: separare, control, reutilizare și operabilitate

Soluția va fi organizată pe limite de responsabilitate stabile. Interfața prezintă și ghidează lucrul utilizatorului. Backend-ul aplică regulile și tranzacțiile. Shared Services furnizează mecanismele comune. Integration Gateway gestionează schimbul de date. Batch/workers execută procesele de durată. PostgreSQL păstrează datele operaționale și istorice. Reporting layer-ul pregătește datele pentru rapoarte. Observabilitatea arată starea sistemului. Platforma de deployment asigură instalarea și operarea.

Straturile sunt conectate prin contracte, evenimente, API-uri, modele comune și audit. Scopul separării este ca fiecare problemă să aibă locul ei de rezolvare. O problemă de integrare se investighează în gateway și logurile de schimb de date. O problemă de raportare statistică se investighează în reporting layer și data marts. O problemă de autorizare se verifică în modelul de roluri și în backend. O problemă de release se urmărește în CI/CD, artefacte și scripturi versionate.

Această disciplină protejează și implementarea paralelă. Echipele de contribuții, pensii și beneficii pot avansa simultan doar dacă folosesc același model de persoană, cerere, dosar, decizie, document, workflow, notificare și audit. Reutilizarea nu este recomandare informală; ea devine regulă arhitecturală controlată prin Design Authority și prin catalogul Shared Services / Shared Artefacts.

9.4 Stack pe straturi: mecanisme asumate ale soluției

Oferta asumă explicit straturile și mecanismele necesare pentru SI „Protecția Socială”. Stack-ul nu este prezentat ca listă de opțiuni negociabile, ci ca arhitectură de livrare: fiecare strat are rol, instrumente, responsabilitate operațională și evidențe care vor fi detaliate în SDD, catalogul componentelor și planul de deployment. Detalierea versiunilor, parametrilor de infrastructură și configurărilor finale nu schimbă angajamentul de bază: Furnizorul va livra aceste mecanisme ca parte a soluției integrate.

În această logică, Java 25 LTS / Spring, React/TypeScript și PostgreSQL sunt nucleul aplicativ și de date asumat. Soluția include și mecanismele care fac sistemul administrabil: autorizare internă peste autentificare, workflow și taskuri, integrare controlată, batch și orchestrare, cache, căutare, stocare de documente, fabrică de date pentru raportare, observabilitate, CI/CD, versionarea bazei de date și controlul deployment-ului.

CNAS va putea verifica aceste mecanisme prin livrabile, diagrame, cataloage, teste, release packages, runbook și evidențe de operare.

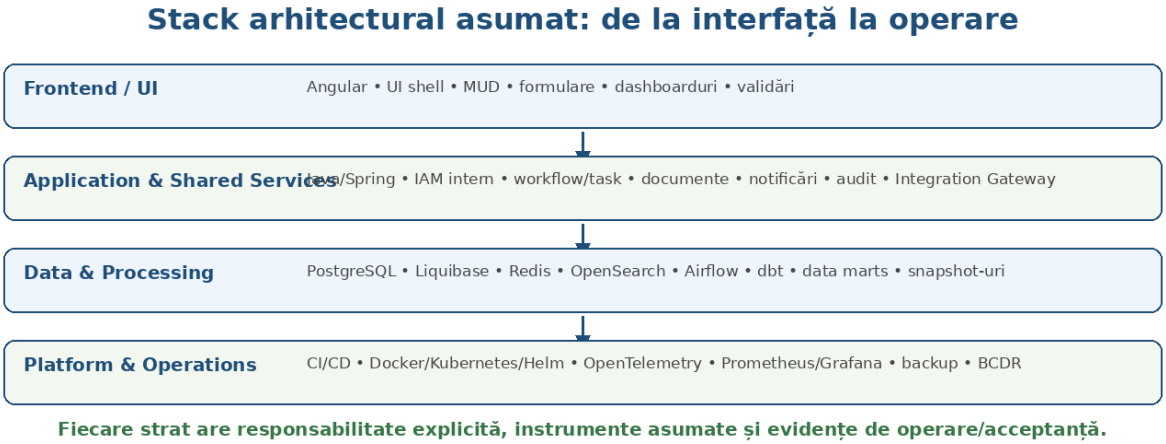


Figura Stack arhitectural asumat pe straturi

Strat / segment	Capabilitate	Mecanism propus	Explicație de ofertă
Application & API	Backend application platform	Java 25 LTS / Spring Boot / Spring Security / Spring Data / Spring Batch	Asigură API-uri, validări backend, tranzacții, autorizare și procesări de durată în același ecosistem tehnic.
Identity & Authorization	Model intern de autorizare	MPass pentru autentificare + roluri, permisiuni, organizații, acțiuni și scope de date în aplicație	Autentificarea confirmă identitatea; sistemul CNAS trebuie să decidă ce poate face utilizatorul și ce date poate accesa.
Shared Services	Workflow & Task Service	serviciu comun de stări, tranziții, sarcini, termene și audit	Cererile, dosarele, deciziile și plățile au nevoie de control de proces, nu doar de formulare.
Integration	Integration Gateway	adaptoare, contracte, retry, timeout, snapshot, audit, tratarea erorilor	Modulele de business nu trebuie să consume direct servicii externe în mod diferit.
Data persistence	PostgreSQL operațional și istoric	scheme operaționale, istoric versionat, indexuri, partiționare unde e cazul	Datele CNAS trebuie să rămână consistente, auditate și pregătite pentru volum.
Database governance	Database migrations	versionarea schimbărilor de schemă	Schimbările de schemă trebuie legate de release, nu executate manual.
Document management	Document & attachment storage	metadate în PostgreSQL + object storage pentru fișiere, atașamente, decizii și exporturi	Fișierele mari, deciziile, atașamentele și exporturile trebuie gestionate separat de datele tranzacționale.
Reporting data factory	Reporting layer / data factory	staging, transformări versionate, data marts, snapshot-uri, materialized views, orchestrare pipeline-uri, teste de calitate	Rapoartele statistice grele nu rulează direct pe baza operațională și nu depind de SQL manual.
Observability & audit	Observabilitate și audit	health checks, logs, metrics, traces, correlation-id, audit business	Suportul trebuie să poată explica erori tehnice și acțiuni instituționale.
CI/CD & deployment	CI/CD și deployment controlat	build, teste, artefacte, imagini, release notes, scripturi DB, promovare între medii	Un release trebuie să fie reproductibil și verificabil.
Performance & cache	Cache distribuit	Redis / cache engine; TTL, invalidare, refresh și coordonare tehnică	Reduce presiunea pe baza de date pentru nomenclatoare, configurări, rate limiting, lock-uri sau date de referință citite frecvent; nu este sursă de adevăr.
Search & retrieval	Search index	Elasticsearch ca index dedicat derivat și reconstruibil	Persoanele, dosarele, plătitorii, documentele, auditul și autocomplete-ul necesită căutare rapidă și filtrări complexe fără încărcarea bazei operaționale.
Async processing	Broker / event streaming	Kafka/message broker pentru evenimente, cozi, retry, dead-letter și decuplare producer/consumer	Susține notificări, procese asincrone, evenimente între domenii și încărcări variabile, în completarea batch/workers/scheduler.
Data pipeline orchestration	Orchestrare pipeline-uri date	Airflow pentru dependențe, programări, rerun, alertare și monitorizare	Ajută la închideri lunare, data marts, migrare, data quality, rerun, dependențe și monitorizare.

Strat / segment	Capabilitate	Mecanism propus	Explicație de ofertă
Transformări & data quality	Transformări versionate și data quality	dbt Core pentru transformări testabile și controale automate	Elimină SQL-ul manual nereproductibil, face indicatorii testabili și controlează datele migrate/raportate înainte de utilizare.
API governance	Contract testing / generated API clients	OpenAPI, contract testing și clienți generați pentru consum frontend/API intern	Reduce riscul între echipe paralele și stabilizează integrarea internă.

9.5 Application & API Layer

Backend-ul va fi construit pe Java 25 LTS / Spring și va concentra logica decisivă a sistemului: reguli de business, validări, tranzacții, autorizare, workflow, integrare, audit și efecte asupra datelor. Deciziile care produc efect juridic, financiar sau de securitate nu vor fi implementate doar în interfață și nu vor depinde de comportamente fragile la nivel de browser.

Serviciile backend vor fi organizate pe domenii funcționale și pe mecanisme comune. Domeniile vor acoperi contribuții, persoane asigurate, cont individual, pensii, beneficii, plăți, documente, raportare și administrare. Mecanismele comune vor include workflow/task, documente, notificări, audit, integrări, clasificatoare, configurări și autorizare. Această organizare permite dezvoltare paralelă fără duplicarea acelorași mecanisme în fiecare modul.

API-urile vor fi documentate și versionate. Pentru fiecare API relevant se vor defini resursele, payload-urile, erorile, codurile de răspuns, regulile de autorizare, scenariile negative și impactul asupra auditului. Contractele API vor susține atât frontend-ul, cât și integrarea internă între echipe și servicii. Unde există dependențe critice între fluxuri, API-urile vor fi stabilizate înainte ca echipele să dezvolte în paralel pe interpretări diferite.

API-urile interne și externe vor fi versionate astfel încât evoluția sistemului să nu rupă integrările existente. Pentru contractele expuse sau consumate de mai multe componente, Furnizorul va defini versiuni explicite, de exemplu v1/v2, reguli de compatibilitate, perioade de tranziție, erori standardizate și contract tests în pipeline. O modificare breaking nu va fi introdusă ca schimbare tăcută într-un release, ci va fi documentată, testată și coordonată prin release notes și catalogul de integrare.

9.6 Identity, autentificare și autorizare: MPass nu înlocuiește controlul intern al accesului

Integrarea cu MPass sau cu mecanismul de autentificare aprobat va confirma identitatea utilizatorului. Totuși, identificarea utilizatorului nu este suficientă pentru SI „Protecția Socială”. Sistemul trebuie să decidă ce rol/identitate are utilizatorul, în ce unitate/organizație acționează, ce acțiuni poate executa, ce date poate vedea, ce exporturi poate genera, ce documente poate semna sau aproba și ce operațiuni trebuie auditate.

Modelul intern de autorizare este bazat pe roluri, permisiuni, acțiuni, contexte organizaționale și scope de date. Acest model va fi aplicat în backend pentru UI, API-uri, batch-uri și integrări. Interfața poate ascunde sau afișa acțiuni pentru confortul utilizatorului, dar decizia finală de autorizare va fi la nivel de serviciu backend.

Administrarea utilizatorilor, rolurilor și permisiunilor se va integra cu capitolul de configurabilitate și administrare operațională. Orice schimbare critică de acces va fi auditată. Pentru scenariile de testare și UAT, Furnizorul va pregăti profiluri reprezentative astfel încât CNAS să poată verifica nu doar funcționalitatea, ci și accesul corect pe roluri.

9.7 Functional Backbone & Shared Services: mecanismul care ține sistemul unitar

Functional Backbone-ul definit în metodologie va fi susținut arhitectural prin servicii și modele comune. Cererea, dosarul, decizia, sarcina, workflow-ul, documentul, notificarea, atașamentul, clasificatorul, integrarea și auditul nu vor fi implementate separat pentru fiecare domeniu. Ele vor fi gestionate ca shared artefacts și shared services, cu extensii specifice acolo unde regulile de pensii, beneficii sau contribuții sunt diferite.

Workflow & Task Service va gestiona stări, tranziții, responsabilități, termene, acțiuni permise și istoric. Document Service va gestiona documente generate, atașamente, metadate, stocare, checksum, versiuni și audit de acces. Notification Service va trimite sau programa notificări pe canalele aprobate. Audit/Event Log va păstra evenimente business relevante. Classifier/Configuration Service va oferi nomenclatoare și configurări versionate. Template Service va controla șabloanele de documente și rapoarte.

Această arhitectură protejează sistemul de fragmentare. O cerere de pensie și o cerere de beneficiu pot avea formulare și reguli diferite, dar folosesc același model de solicitant, documente, sarcini, statusuri, decizie, notificare și audit. Prin urmare, CNAS primește un sistem cu comportament unitar, iar Furnizorul poate dezvolta domeniile în paralel fără să creeze trei aplicații diferite sub aceeași interfață.

Shared Service	Responsabilitate	Presiune arhitecturală controlată
Workflow & Task Service	Stări, tranziții, sarcini, termene, responsabili, acțiuni permise, istoric.	Previne fluxuri duplicate și permite dashboard unic de lucru.
Document & Attachment Service	Documente generate, atașamente, metadate, stocare fișiere, versiuni, checksum, audit.	Separă fișierele de baza tranzacțională și păstrează trasabilitate pe documente.
Notification Service	Notificări programate, canale aprobate, șabloane, status livrare, retry, audit.	Evită trimiterea mesajelor din fiecare modul în mod diferit.
Audit / Business Event Log	Evenimente instituționale: cine, ce, când, obiect, rezultat, context.	Permite reconstrucția deciziilor și investigarea acțiunilor.
Classifier & Configuration Service	Nomenclatoare, parametri, versiuni, perioade de valabilitate, aprobări.	Reduce intervențiile directe în baza de date și susține schimbări controlate.
Template Service	Șabloane documente/rapoarte, versiuni, limbă, activare, audit.	Face deciziile și documentele controlabile în timp.

9.8 Messaging, evenimente și asincronie

Sistemul va separa cererile interactive de procesele asincrone. Unele acțiuni trebuie să răspundă imediat utilizatorului: salvare formular, schimbare de stare, verificare drepturi de acces, consultare dosar. Alte acțiuni trebuie executate în fundal: generare documente în lot, notificări, exporturi mari, recalculări, refresh data marts, procesare importuri, transmitere către sisteme externe sau reluare după eroare.

Procesele asincrone și joburile de durată vor utiliza două mecanisme complementare. Spring Batch, workers și scheduler acoperă loturi, calcule programate, importuri, exporturi și refresh-uri controlate. În paralel, oferta asumă un strat de mesagerie / message broker / event streaming pentru decuplarea producer/consumer, notificări, evenimente între domenii, retry, cozi de procesare și tratarea încărcărilor variabile. Brokerul nu înlocuiește Integration Gateway-ul sau workflow-ul, ci completează arhitectura acolo unde evenimentele și procesele de fundal trebuie operate independent de tranzacția interactivă.

Kafka este tratat ca mecanism de bază pentru asincronie enterprise, nu ca dezvoltare suplimentară. Configurația exactă se va dimensiona în SDD: topicuri/queue-uri, producători/consumatori, politici de retry și dead-letter, retenție, securitate, monitorizare, volum, proceduri de operare și scenarii de degradare.

Această formulare separă prezența capabilității, care este asumată, de dimensiunea tehnică și operațională, care se validează în proiectare.

9.9 Batch, workers și orchestration

Procesele de durată vor fi executate în afara cererii interactive a utilizatorului. Importurile, exporturile masive, recalculările, generarea documentelor în lot, actualizarea data marts, migrarea, închiderea lunară, reconcilierea și unele integrări programate vor fi tratate ca joburi cu stare și evidență.

Fiecare job critic va avea parametri, perioadă, inițiator, timp de start/final, volum procesat, rezultat, erori, obiecte afectate, log și posibilitate de reluare controlată. Unde natura procesului permite, joburile vor avea checkpoint-uri și vor evita reluarea inutilă a întregului volum. Erorile vor fi vizibile în interfețe de administrare sau dashboarduri operaționale, nu ascunse în loguri tehnice inaccesibile utilizatorilor responsabili.

Procesele batch critice vor fi proiectate pentru reluare controlată. Dacă un calcul masiv, o generare de plăți, o recalculare sau o închidere lunară se oprește la 80%, reluarea nu trebuie să dubleze plăți, să creeze decizii duplicate sau să lase obiecte într-o stare ambiguă. Furnizorul va utiliza identificatori de lot, chei de idempotentă, checkpoint-uri, stări de procesare, marcarea obiectelor tratate și rapoarte de rezultat pentru a permite reluarea fără efecte duble.

Pentru operațiunile cu impact financiar sau juridic, batch-ul va separa pregătirea, validarea, confirmarea și aplicarea rezultatului. Acolo unde este necesar, un lot va fi mai întâi calculat și reconciliat, apoi aprobat sau confirmat înainte de a produce efect final. Această separare protejează CNAS de scenariile în care un proces parțial executat produce efecte greu de reconstruit.

Pentru procesele de reporting, migrare, calitate a datelor și închidere de perioadă, orchestration-ul va fi tratat ca parte a arhitecturii de date. Orchestratorul va controla ordinea pașilor: extragere, staging, transformare, teste de calitate, valori de control, snapshot, publicare data mart, generare rapoarte și notificare la eroare. SDD-ul va preciza instrumentul și granularitatea workflow-urilor, dar oferta asumă existența unui mecanism versionat, monitorizat și repetabil.

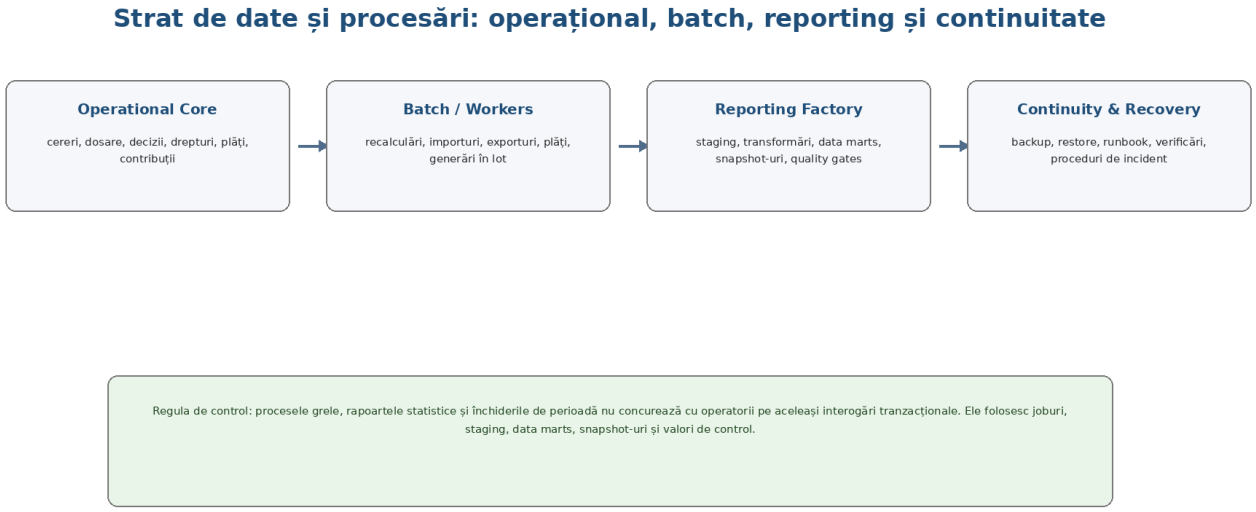


Figura Date și procesări: procesele grele rulează controlat, separat de interacțiunea operatorilor

9.10 Data Persistence Layer

PostgreSQL va fi utilizat ca bază relațională principală pentru date operaționale, istorice, audit, configurări și structuri pregătite pentru raportare. Modelul de date va urmări integritate, volum, istoric, reconciliere și audit. Pentru procesele critice se vor defini chei, constrângeri, indexuri, strategii de partitionare unde profilul datelor o justifică și structuri de citire optimizate pentru scenarii frecvente.

Modelul de date va distinge între starea curentă, istoricul versionat și snapshot-urile de perioadă. Pentru obiectele care evoluează în timp — drepturi, decizii, plăți, profiluri, contribuții, cereri, dosare — sistemul nu va suprascrie tăcut informația relevantă pentru raportare, audit sau justificare. Modificările vor fi tratate prin versiuni, evenimente, stări, ajustări sau rectificări, în funcție de natura lor funcțională.

Schimbările de schemă vor fi gestionate prin database migrations versionate. Fiecare release va include scripturile DB aferente, ordinea de aplicare, dependențele, verificările și procedura de rollback/forward când scenariul o cere. Această disciplină este obligatorie pentru a evita situația în care baza de date devine diferită de codul instalat sau de documentația predată.

Pentru volumele CNAS, performanța bazei de date va fi tratată ca disciplină de proiectare, nu ca optimizare târzie. Modelul PostgreSQL va utiliza indexuri proiectate pe scenarii reale, partitioning pentru tabele mari pe perioade sau domenii unde profilul datelor o justifică, read models pentru interogări frecvente și separarea structurilor operaționale de structurile de raportare. Query-urile complexe nu vor fi lăsate să concureze necontrolat cu tranzacțiile zilnice ale operatorilor.

Datele istorice vor fi tratate prin politici de arhivare și acces diferențiat. Sistemul va separa datele active, datele istorice consultabile, snapshot-urile de perioadă și arhiva operațională. Arhivarea nu va însemna pierderea capacității de audit sau de regenerare a rapoartelor, ci mutarea controlată a datelor vechi din zona activă în structuri optimizate pentru consultare, raportare istorică și restaurare.

Pentru fiecare tabel sau grup de tabele cu volum ridicat se vor defini reguli de creștere, retenție, partitioning, arhivare, indexare și monitorizare. Aceste reguli vor fi incluse în SDD și în runbook-ul operațional, astfel încât CNAS să poată urmări evoluția volumelor și să prevină degradarea performanței înainte ca aceasta să afecteze utilizatorii.

9.11 Reporting Data Factory: strat de raportare industrializat

Arhitectura va include un strat dedicat pentru producerea datelor de raportare. Rapoartele statistice, operative, profilurile, contingentele și dashboardurile nu vor depinde de SQL manual executat direct pe baza operațională. Datele vor fi pregătite prin staging, transformări versionate, data marts, materialized views, snapshot-uri de perioadă, teste de calitate, valori de control și audit de generare.

În această arhitectură, instrumentul de raportare este stratul de prezentare. Logica de selecție, curățare, agregare, indicatori și tratare a corecțiilor va fi gestionată în reporting layer și în data marts. SQL-ul rămâne un instrument tehnic utilizat în transformări și modele de date, dar nu devine mecanism manual de producere a rapoartelor instituționale.

Pentru fiecare raport important se va defini produsul de date care îl alimentează: sursă, perioadă, reguli de includere/excludere, indicatori, valori de control, frecvență de actualizare, responsabil funcțional și mecanism de regenerare. Rapoartele istorice vor fi regenerate din snapshot-ul sau data mart-ul aferent perioadei, iar rapoartele rectificative vor fi tratate distinct de rapoartele inițiale.

Clarificare. Această secțiune este puntea între arhitectură și capitolul privind raportarea, documentele și guvernanța șabloanelor. JasperReports este motorul asumat pentru rapoarte oficiale și documente; logica principală de date rămâne în reporting layer, data marts, snapshot-uri și stratul semantic/analitic. Instrumentul de prezentare consumă surse pregătite și controlate, nu devine locul principal al transformării datelor.

9.12 Cache, căutare și fișiere: reducerea presiunii pe baza operațională

Mecanismele de cache sunt utilizate pentru datele accesate repetat, atunci când citirea directă ar încărca inutil baza operațională. Nomenclatoarele, configurările, datele de referință, parametrii citiți frecvent și unele rezultate stabile pot fi păstrate într-un cache distribuit sau mecanism echivalent, cu reguli clare de invalidare și refresh. Cache-ul nu va fi sursă de adevăr; el va accelera citirea datelor administrate în sistem.

Căutarea operațională simplă va utiliza indexuri și interogări optimizate în PostgreSQL, însă pentru un sistem cu dosare istorice, persoane, plătitori, documente, audit, autocomplete și filtrări complexe, oferta asumă un search index dedicat. PostgreSQL rămâne sursa de adevăr, iar indexul de căutare rămâne structură derivată, versionată și reconstruibilă. SDD-ul va detalia domeniile indexate, politicile de actualizare, securitatea, retenția și modul de reconciliere, fără a trata motorul de căutare ca opțiune post-contract.

Documentele, atașamentele, deciziile generate, exporturile mari și fișierele asociate dosarelor vor fi tratate printr-un mecanism de document/object storage. PostgreSQL va păstra metadatele, relația cu obiectele business, starea, checksum-ul, drepturile de acces și auditul, iar fișierul efectiv va fi păstrat într-un storage aprobat pentru proiect. Această separare protejează baza tranzacțională și face administrarea documentelor mai controlabilă.

Strategia de stocare a documentelor și fișierelor mari

Documentele scanate, fișierele generate, atașamentele dosarelor, exporturile mari și pachetele de evidență nu vor încărca inutil baza relațională. Mecanismul asumat este separarea conținutului de metadate: fișierele se păstrează într-un object storage compatibil S3 sau mecanism echivalent aprobat în infrastructura proiectului, iar PostgreSQL păstrează metadatele, drepturile de acces, checksum-ul, starea, versiunea, legătura cu obiectele business și auditul de acces. Mențiunea S3 descrie compatibilitatea de interfață, nu impunerea unui produs anume.

Pentru fișierele critice se vor aplica reguli de integritate și operare: checksum, control de acces, scanare antivirus unde infrastructura o permite, versiune, retenție, arhivare, backup și posibilitate de reconstrucție a legăturii dintre document și dosar/decizie/raport. Astfel, documentele rămân parte controlată a procesului CNAS, nu fișiere izolate într-un spațiu de stocare greu de auditat.

9.13 Observabilitate și operabilitate: sistemul explică ce se întâmplă

Sistemul va produce informații operaționale suficiente pentru diagnostic, suport și prevenirea incidentelor. Observabilitatea va include health checks, metrici de performanță, loguri structurate, correlation-id, audit de business, stare joburi, stare integrări, alerte și dashboarduri operaționale. Furnizorul va evita un model în care suportul poate înțelege starea sistemului doar prin acces manual la servere sau prin citirea fragmentară a logurilor.

Logurile tehnice vor fi separate conceptual de auditul de business. Logurile ajută la diagnosticarea componentelor, a timpilor de răspuns, a erorilor, a conexiunilor și a resurselor. Auditul de business explică

acțiunea instituțională: cine a accesat, ce obiect, ce acțiune a executat, când, cu ce rezultat și în ce context. Ambele sunt necesare, dar au scopuri diferite și reguli diferite de acces.

Pentru integrări și joburi, sistemul va afișa stare operațională, durată, volum procesat, rezultat, eroare, acțiuni de reluare și obiecte afectate. O integrare eșuată, un job de recalculare blocat sau un refresh de data mart cu erori nu trebuie descoperite doar prin reclamația utilizatorilor. Ele trebuie să apară în dashboarduri, alerte și registre operaționale.

Validarea performanței sub sarcină reală

Înainte de go-live, Furnizorul va executa teste de sarcină pe scenarii reprezentative: autentificare, dashboard, căutare persoană/dosar, salvare formular, schimbare stare, generare document, apel integrare, job batch, raport masiv și acces concurent la date. Testele vor urmări timpi de răspuns, concurență, consum de CPU/RAM, conexiuni DB, blocări, latență integrare, backlog de joburi și comportamentul sistemului la vârf.

Testele de performanță nu vor verifica doar aplicația web. Ele vor include baza de date, cache-ul, search index-ul, Integration Gateway, batch workers, reporting layer și platforma de deployment. Rezultatul va fi un raport de performanță cu scenarii, volum, configurație testată, valori obținute, limitări cunoscute și recomandări de operare.

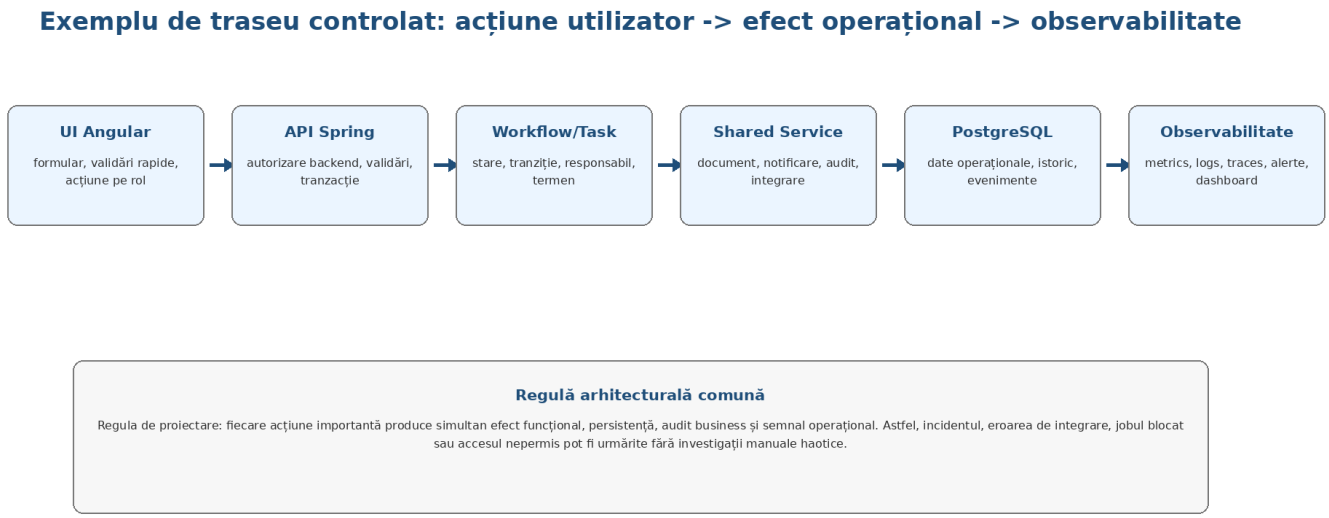


Figura Traseu controlat: acțiune utilizator, efect operațional, audit și observabilitate

9.14 Platformă de deployment: containere, Kubernetes, Helm și MCloud ca strat de execuție

Clarificare de interpretare: Kubernetes/Helm/MCloud reprezintă stratul de împachetare, rulare și operare a componentelor, nu o tehnologie care modifică logica de business, modelul de date sau mecanismele funcționale ale SI. Oferta asumă deployment containerizat pentru MCloud, cu charturi/manifestări, configurări pe medii, health checks, secrets, rollout/rollback și runbook. Dacă STISC/MCloud oferă servicii gestionate sau mecanisme echivalente pentru anumite funcții de platformă, acestea se integrează în aceeași disciplină de deployment, fără reducerea livrabilelor și fără schimbarea arhitecturii aplicative.

Containerizarea, Kubernetes, Helm și mecanismele similare aparțin stratului de deployment și operare. Ele nu înlocuiesc serviciile aplicative, workflow-ul, integrarea, raportarea sau auditul. Rolul lor este să permită împachetarea, configurarea, scalarea, promovarea între medii, rollback-ul și administrarea componentelor aplicației în infrastructura aprobată.

Ținta de operare este MCloud ca infrastructură guvernamentală pentru proiect. Această țintă nu schimbă stack-ul aplicativ asumat; ea stabilește condițiile de packaging, deployment, configurare și operare. Furnizorul va livra artefactele aplicației, imaginile/container packages, charturile sau manifestele de deployment, scripturile de bază de date, cerințele de mediu, smoke tests, release notes și suportul pentru instalare. Serviciile gestionate sau mecanismele echivalente aprobate în MCloud se documentează în matricea de compatibilitate, dar nu transformă deployment-ul într-un subiect incert sau într-un change request.

Configurările sensibile vor fi externalizate și gestionate securizat. Secretele, tokenurile, certificatele, cheile API, parolele și connection strings nu vor fi păstrate în cod sursă. Pentru fiecare mediu se va documenta sursa configurărilor, modul de actualizare, responsabilitatea de operare și impactul asupra deployment-ului.

Deployment cu întreruperi minime și self-healing

Soluția va fi proiectată pentru deployment controlat și pentru reducerea întreruperilor operaționale la actualizări. Pentru componentele stateless, Furnizorul va utiliza mecanisme de rolling update, replicare, readiness/liveness probes și scoaterea automată din trafic a instanțelor care nu sunt pregătite. Pentru release-uri majore, unde compatibilitatea datelor, migrațiile de schemă sau schimbările funcționale o impun, Furnizorul va pregăti strategii de deployment controlat, inclusiv blue-green sau ferestre de mentenanță aprobate, după natura schimbării.

Actualizările de aplicație nu vor fi tratate identic cu migrațiile de bază de date. Pentru schimbările de schemă se va aplica o disciplină de database migration versionată, cu strategie de compatibilitate acolo unde este posibil: extindere, rulare paralelă, migrare date, schimbare controlată a aplicației și curățare ulterioară. Această abordare reduce riscul ca o actualizare de aplicație să blocheze producția sau să creeze incompatibilități între versiuni.

Mecanismele de self-healing ale platformei vor fi utilizate pentru repornirea automată a componentelor blocate, menținerea numărului de replici, verificarea stării serviciilor și alertarea echipei de suport. Self-healing-ul infrastructural nu înlocuiește însă consistența aplicativă. Procesele batch, recalculările, exporturile, migrările și generările masive vor fi proiectate cu checkpoint-uri, idempotency și reluare controlată, astfel încât repornirea unei componente să nu dubleze plăți, să nu repete necontrolat o migrare și să nu lase date în stare intermediară ambiguă.

Mecanism	Cum este utilizat	Control oferit
Rolling update	înlocuire treptată a instanțelor stateless, cu verificare readiness înainte de trafic	reducerea întreruperilor la release-uri compatibile
Blue-green / release controlat	două versiuni pregătite în paralel pentru schimbări majore, acolo unde platforma și resursele permit	posibilitate de comutare controlată și reducere risc la upgrade
Liveness / readiness probes	platforma verifică dacă un serviciu rulează și dacă poate primi trafic	evită trimiterea utilizatorilor către instanțe defecte
Idempotency batch	rularea repetată a aceluiași pas produce același rezultat, fără duplicare	permite reluare după eșec la 80% fără dublarea rezultatelor
Checkpoint-uri	procesele lungi salvează progresul pe loturi și pot continua controlat	reduce timpul de recuperare după eșec

Complexitatea Kubernetes controlată prin sizing, runbook și transfer operațional

Kubernetes și Helm aduc beneficii de deployment, scalare și izolare, dar introduc și cerințe operaționale suplimentare. Furnizorul va trata acest strat cu disciplină de sizing și operare: requests/limits pentru resurse, health probes, readiness/liveness checks, strategii de rollout/rollback, namespaces, configurări pe medii, politici de logare, monitorizare și alerte.

Pentru ca arhitectura să poată fi întreținută de CNAS, Furnizorul va livra nu doar manifests/Helm charts, ci și explicații de operare: cum se pornește/oprește o componentă, cum se verifică starea serviciilor, cum se citește o eroare de pod/job, cum se aplică un release, cum se revine la versiunea anterioară, cum se scalează o componentă și cum se investighează consumul de resurse. Această documentație va fi completată prin sesiuni de handover tehnic și shadowing pentru echipa IT CNAS.

9.15 CI/CD, release control și trasabilitate deployment

Furnizorul va utiliza CI/CD ca mecanism de control al versiunilor livrate. Fiecare schimbare relevantă va fi legată de cerință, UC, defect, decizie, schimbare aprobată sau observație CNAS. Codul, scripturile de bază de date, șabloanele, configurările, testele și documentația vor fi gestionate astfel încât release-ul să poată fi reconstituit ulterior.

Un release nu va fi doar un pachet instalat. Release-ul va include codul aplicației, imaginile/container artefacts, scripturile DB/migrațiile, șabloanele, configurările, release notes, raportul de teste, lista defectelor cunoscute, instrucțiunile de deployment, smoke tests și, când scenariul o cere, procedura de rollback sau remediere. Acest pachet permite CNAS să urmărească ce versiune este instalată, ce schimbări conține și ce evidențe o susțin.

Promovarea între medii va fi controlată prin gates: build reușit, teste relevante, verificări de securitate/dependențe unde este cazul, migrații validate, defecte critice tratate, documentație actualizată și aprobare pentru mediul următor. În acest mod, CI/CD nu este doar automatizare tehnică, ci mecanism de control al calității, trasabilității și operabilității.

Pipeline-ul CI/CD va include verificări automate de calitate și securitate înainte de promovarea pe medii superioare. Furnizorul va integra static code analysis, dependency scanning, container image scanning, verificări pentru secrete expuse accidental, teste automate relevante și raportarea rezultatelor în pachetul de release. Instrumente acceptate pe larg sau mecanisme echivalente vor fi utilizate în funcție de detaliile aprobate, fără a modifica obligația de a produce evidențe de calitate și securitate.

Un release cu vulnerabilități critice, secrete expuse sau defecte blocate nu va fi promovat ca versiune pregătită pentru UAT/producție fără decizie documentată. Această regulă transformă securitatea din verificare târzie în control integrat al livrării.

Separarea mediilor SDLC și rolul Pre-Production

Furnizorul va organiza fluxul de livrare pe medii separate, astfel încât dezvoltarea, testarea, validarea funcțională, verificarea de performanță și producția să nu fie amestecate. Separarea mediilor este condiție de control pentru un sistem critic: o versiune nu trebuie să ajungă în producție fără să fi fost construită, testată, configurată și demonstrată în medii adecvate.

Fluxul SDLC propus va utiliza cel puțin următoarea logică: Development pentru integrarea tehnică inițială, Test pentru verificare internă și regresie, UAT/Model Office pentru demonstrarea funcțională cu CNAS, Pre-Production pentru verificări apropiate de producție și Production pentru exploatarea oficială. Mediul Pre-

Production va avea un rol distinct: va fi utilizat pentru testare de performanță, rehearsal de deployment, testare de migrare, verificare de backup/restore, validare integrări, verificare raportare masivă și go-live readiness.

Pre-Production nu va fi tratat ca simplu mediu de test suplimentar. El va fi configurat, în măsura resurselor aprobate în MCloud, cât mai apropiat de producție: aceleași tipuri de componente, aceleași mecanisme de deployment, aceleași modele de configurare, volume de date reprezentative, integrare controlată și observabilitate activă. Această abordare reduce riscul ca sistemul să funcționeze în test, dar să eșueze în condiții reale de exploatare.

Figura propusă. Flux SDLC și rolul mediului Pre-Production
Development → Test → UAT / Model Office → Pre-Production → Production
Development: integrare tehnică și verificări rapide ale componentelor.
Test: verificare internă, regresie, contract tests, defecte și stabilizare increment.
UAT / Model Office: scenarii CNAS, roluri funcționale, feedback și observații.
Pre-Production: performanță, migrare, backup/restore, release rehearsal, integrări și go-live readiness.
Production: exploatare oficială, monitorizare, suport și raportare operațională.

Flux SDLC și rolul mediului Pre-Production

Mediu	Rol principal	Ce nu trebuie făcut în acel mediu
Development	integrare tehnică, build-uri frecvente, verificare rapidă a componentelor	nu se validează acceptanță funcțională sau performanță oficială
Test	QA intern, regresie, contracte API, verificare tehnică a release-ului	nu se confundă cu UAT CNAS
UAT / Model Office	validare funcțională, scenarii reale, feedback CNAS, observarea utilizabilității	nu se fac experimente tehnice instabile
Pre-Production	mirror operațional al producției pentru load test, migrare, deployment rehearsal, backup/restore	nu se acceptă configurare radical diferită față de producție
Production	exploatare oficială și monitorizare	nu se aplică schimbări manuale neversionate

9.16 Securitate arhitecturală și privacy by design

Capitolul dedicat securității va detalia modelul complet de protecție. În arhitectură, securitatea va fi inclusă ca limită transversală: autentificare, autorizare pe rol/acțiune/context, segregare de responsabilități, protecție date personale, control exporturi, audit, logare minimizată, criptare când documentul sau procesul o solicită, securitatea API-urilor și protejarea configurărilor sensibile.

Controalele de securitate nu vor fi implementate doar în interfață. Backend-ul va valida fiecare acțiune critică, iar API-urile, batch-urile și integrările vor respecta aceleași reguli. Listele, dashboardurile, rapoartele și exporturile vor fi filtrate în funcție de rol, scop și drept de acces. Evenimentele de acces la date sensibile vor fi auditate conform modelului aprobat.

Mediile de testare și dezvoltare nu vor utiliza date personale reale neprotejate decât dacă CNAS aprobă explicit scenarii controlate și măsuri compensatorii. Unde este posibil, se vor utiliza date anonimizate, mascate sau sintetice. Această regulă protejează atât persoanele vizate, cât și echipele de implementare, testare și suport.

Zero Trust aplicat pragmatic între utilizatori, servicii și date

Arhitectura va aplica principiul că niciun utilizator, serviciu sau componentă nu primește încredere implicită doar pentru că se află în rețeaua internă sau în același cluster. Accesul va fi autentificat, autorizat și auditat pe rol, acțiune, context și scop. Comunicarea între servicii va utiliza mecanisme controlate de autentificare tehnică, cum ar fi tokenuri JWT, mTLS sau mecanisme echivalente aprobate de infrastructură, acolo unde profilul de risc și platforma o justifică.

Serviciile vor utiliza conturi tehnice cu privilegii minime, iar accesul la baze de date, obiect storage, broker, search index sau servicii externe va fi acordat numai pentru scopul necesar. Această abordare reduce impactul unei componente compromise și sprijină auditul accesului la date personale și operațiuni critice.

Configurările și secretele tehnice vor fi gestionate separat de codul aplicației. Parolele, tokenurile, certificatele, cheile API, connection string-urile și parametrii sensibili nu vor fi păstrați în repository sau în fișiere livrate necontrolat. Furnizorul va utiliza mecanismele de secrets management disponibile în MCloud/Kubernetes sau mecanisme echivalente aprobate, cu acces limitat pe roluri tehnice și cu proceduri pentru rotație, actualizare și revocare.

Soluția va aplica un model pragmatic de Zero Trust între componente: un serviciu nu va avea încredere implicită în alt serviciu doar pentru că se află în același cluster sau în aceeași rețea. Comunicațiile interne relevante vor fi protejate prin tokenuri, certificate, politici de acces, validarea identității serviciului și limitarea drepturilor la strictul necesar. API-urile interne vor aplica autorizare în backend și vor păstra audit pentru acțiunile cu impact funcțional, financiar, operațional sau de securitate.

Caching-ul este mecanism de bază pentru performanță și reducerea presiunii pe baza de date operațională, fără a deveni sursă de adevăr. Redis va susține nomenclatoare, configurări citite frecvent, rate limiting, coordonare tehnică, rezultate temporare și date de referință reconstruibile, cu TTL, invalidare și refresh documentate. Datele cu efect juridic, financiar sau operațional critic rămân în sursele persistente controlate, iar cache-ul trebuie să poată fi reconstruit fără pierdere de informație.

Zonă	Regulă aplicată	De ce este necesară
Secrete	fără parole/tokenuri/certificate în cod; utilizare secrets management aprobat pe medii	reduce riscul de expunere și permite rotație controlată
Configurații	parametri externalizați pe medii, versionați și documentați	același build poate fi promovat controlat între medii
Zero Trust intern	serviciile se autentifică/autoriză; drepturile sunt limitate la necesar	reduce impactul unui incident sau al unei configurări greșite
Cache	TTL, invalidare și reconstrucție; cache-ul nu este sursă primară	evită date expirate și dependență de memorie temporară
Audit securitate	accesul, exporturile, operațiunile administrative și acțiunile critice sunt jurnalizate	permite investigare și responsabilizare

9.17 Continuitate operațională, backup, restore

Continuitatea operațională va fi tratată ca parte a arhitecturii. Sistemul va avea proceduri documentate pentru backup, restore, verificări de restaurare, deployment, rollback, incident response, funcționare degradată unde este posibil, reluarea joburilor și comunicarea operațională în caz de incident.

Pentru Business Continuity și Disaster Recovery, Furnizorul va documenta, în limitele infrastructurii puse la dispoziție, scenarii de continuitate la nivel de procese: indisponibilitate aplicație, indisponibilitate bază de

date, indisponibilitate integrare externă, eșec job critic, raportare indisponibilă, eșec la deployment, restaurare după eroare și reluare de proces batch. Pentru fiecare scenariu se vor indica acțiunile de diagnostic, escaladare, contingență și revenire.

Runbook-ul operațional va include proceduri pentru verificări zilnice, verificări post-deployment, monitorizarea integrărilor, reluarea joburilor, verificări backup/restore, escaladare incident, comunicare cu CNAS, confirmare după remediere și actualizarea documentației. Astfel, continuitatea nu rămâne declarație generală, ci procedură de exploatare.

Ținte BCDR: RPO, RTO și verificarea restaurării

Planul BCDR va defini ținte explicite pentru pierderea acceptabilă de date și timpul de restaurare. Ca ținte de proiectare, Furnizorul va urmări RPO de maximum 15 minute pentru datele tranzacționale critice și RTO de maximum 4 ore pentru repunerea în funcțiune a serviciilor critice, în limitele infrastructurii puse la dispoziție și ale mecanismelor aprobate. Țintele finale vor fi confirmate în planul BCDR și în SDD, împreună cu CNAS.

Backup-ul nu va fi considerat suficient fără verificări de restaurare. Furnizorul va include în runbook proceduri de test restore, verificare integritate, verificare legături documente/metadata, reluare joburi după incident și confirmare operațională post-restaurare. Pentru procesele critice, planul de continuitate va descrie și modul de operare degradată sau reluare controlată după indisponibilitate.

Load testing, RPO/RTO și continuitate operațională

Înainte de go-live, Furnizorul va executa testare de sarcină pe scenarii reprezentative pentru exploatarea CNAS: autentificare, dashboard, căutare persoane/dosare, procesare cerere, schimbare stare, generare document, apel integrare, raportare operativă, raportare statistică, job batch și acces concurent. Testarea nu va urmări doar media timpilor de răspuns, ci și percentilele, rata de erori, consumul de resurse, conexiunile la baza de date, durata batch-urilor, backlog-ul de joburi și comportamentul la vârf.

Pentru baza de date PostgreSQL, Furnizorul va defini strategia de partiționare, indexare, arhi-vare și separare a datelor active de date istorice sau de raportare. Datele vechi nu vor rămâne necontrolat în același profil de acces cu datele active dacă acest lucru afectează performanța. Arhitectura va utiliza scheme/straturi dedicate, materialized views, data marts și mecanisme de arhivare acolo unde profilul volumelor o impune. Această abordare permite menținerea performanței pe termen lung, nu doar la momentul lansării.

Obiectivele RPO și RTO vor fi propuse, validate și confirmate în faza de proiectare împreună cu CNAS, în funcție de criticitatea proceselor și mecanismele MCloud disponibile. RPO va defini pierderea maximă acceptabilă de date în caz de incident, iar RTO va defini timpul țintă de restabilire a serviciului. Aceste valori vor fi legate de backup, restore, replicare, runbook, proceduri de verificare după incident și test de restaurare înainte de intrarea în producție.

Figura propusă. Readiness de performanță și continuitate înainte de go-live
Pre-Production cu date reprezentative → Load Test → Observability Review → DB/Batch Tuning
Backup/Restore Test → RPO/RTO Confirmation → Go-live Readiness → Production Monitoring
Dacă testele nu ating pragurile: raport cauză-impact, optimizare, resurse necesare, decizie CNAS/STISC.

Readiness de performanță și continuitate înainte de go-live

Zonă verificată	Scenariu de testare	Evidență produsă
Utilizatori concurenți	operatori multipli pe dashboard, căutare, cereri și dosare	load test report, percentile, error rate

Zonă verificată	Scenariu de testare	Evidență produsă
Rapoarte grele	rapoarte statistice/exporturi pe data marts și snapshot-uri	durată, consum DB, impact operațional
Batch masiv	recalculare/generare/export cu checkpoint și reluare controlată	batch report, idempotency evidence
Integrare lentă	timeout, retry, circuit breaker, cache/snapshot unde este permis	integration resilience test
Recovery	restore din backup și verificare consistență post-restore	backup/restore evidence, RTO/RPO confirmation

9.18 Livrabile și evidențe de acceptanță pentru arhitectură și stack

Furnizorul va demonstra arhitectura, stiva tehnologică și operabilitatea prin livrabile verificabile. Acceptanța acestei secțiuni nu se va baza pe descrierea tehnologiilor, ci pe existența artefactelor care permit instalarea, testarea, operarea, monitorizarea, restaurarea și predarea sistemului.

Livrabil / evidență	Conținut minim	Rol în acceptanță
Software Design Document	arhitectură logică, straturi, componente, API-uri, date, securitate, deployment	demonstrează că soluția este proiectată complet și coerent
Catalog componente stack	componentă, rol, versiune, licență, responsabilitate, dependențe	arată ce se livrează și ce se operează
Catalog Shared Services	workflow, taskuri, documente, notificări, audit, clasificatoare, template-uri	dovedește reutilizarea și evitarea duplicării
Catalog integrare	contracte, payload-uri, erori, timeout/retry, audit, snapshot	dovedește controlul schimburilor externe
Model date + migration scripts	schema, istoric, snapshot-uri, scripturi versionate, strategie de migrare DB	leagă codul de baza de date și de release
Reporting data factory design	staging, transformări, data marts, materialized views, snapshot-uri, quality gates	demonstrează că rapoartele grele au sursă controlată
CI/CD și deployment pack	build, artefacte, imagini, charturi/configurări, release notes, smoke tests	permite instalare reproductibilă
Observability pack	health checks, logs, metrics, traces, dashboards, alerte, correlation-id	permite exploatare și diagnostic
Runbook operațional	proceduri zilnice, incident, backup/restore, joburi, integrări, deployment	permite suport și handover

Evidențe suplimentare pentru riscurile arhitecturale critice

Pentru a demonstra că arhitectura nu este doar descrisă, ci poate fi operată și verificată, Furnizorul va include în pachetul de acceptanță arhitecturală evidențe specifice pentru zonele cu risc ridicat: performanță, integrări, batch-uri, securitate, deployment, continuitate și transfer operațional.

Zonă critică	Evidență livrată / verificare propusă
Performanță DB și query-uri complexe	strategie de indexare/partitioning, raport de load testing, recomandări de arhivare și monitorizare volum
Integrări lente sau indisponibile	catalog integrare, scenarii de timeout/retry/circuit breaker, loguri și raport de test negativ
Batch-uri cu volum mare	checkpoint-uri, idempotentă, reluare controlată, raport de lot și test de rerun fără dublare efecte
Deployment și operare Kubernetes	Helm charts/manifests, sizing, probes, proceduri de rollout/rollback, runbook și sesiuni de handover
Securitate și DevSecOps	rapoarte SAST/dependency/container scan, teste de acces, evidență Zero Trust/least privilege
BCDR și restaurare	plan BCDR cu RPO/RTO, test restore, verificare integritate și proceduri de reluare operațională
UX și protecția lucrului operatorului	prototipuri validate, scenarii auto-save/draft, testare formulare lungi și mesaje de eroare

9.19 Rezultatul arhitectural livrat către CNAS

Prin această arhitectură, CNAS primește o platformă operațională coerentă, nu o colecție de componente instalate. Soluția va separa responsabilitățile tehnice, va reutiliza mecanisme comune, va proteja regulile critice în backend, va gestiona integrarea prin gateway, va executa procesele de durată ca joburi controlate, va pregăti raportarea prin produse de date, va produce observabilitate și va livra release-uri trasabile.

Valoarea principală pentru CNAS este controlul pe termen lung. Sistemul va putea fi dezvoltat incremental, monitorizat în exploatare, diagnosticat în caz de incident, restaurat în scenarii de continuitate, actualizat prin release-uri controlate și predat cu artefacte suficiente pentru operare. Astfel, stack-ul tehnologic nu rămâne listă de instrumente, ci devine mecanism de funcționare, acceptanță și suport pentru SI „Protecția Socială”.

Prin arhitectura propusă, CNAS primește un sistem construit pe tehnologii standardizate, larg utilizate și documentate: Java 25 LTS / Spring, React, PostgreSQL, Kubernetes/Helm, OpenAPI, CI/CD, observabilitate, migrații de bază de date versionate, reporting layer și artefacte de deployment reproductibile. Această alegere reduce dependența instituției de tehnologii obscure, runtime-uri proprietare greu de înlocuit sau mecanisme informale cunoscute doar de Furnizor.

Independența CNAS nu rezultă doar din alegerea tehnologiilor. Ea rezultă din modul de livrare: cod sursă predat, repository organizat, documentație de build și deployment, runbook operațional, contracte API, catalog de configurări, matrice de compatibilitate, release notes, diagrame, proceduri de backup/restore, ghiduri de administrare și transfer de cunoștințe către echipa tehnică desemnată. Astfel, o echipă IT calificată va putea înțelege, opera, audita și continua sistemul fără dependență informală de persoane sau explicații neverificabile.

Această abordare oferă CNAS control pe termen lung. Furnizorul livrează sistemul, dar și condițiile prin care sistemul poate fi preluat, verificat, extins și susținut în timp. Arhitectura nu devine o cutie neagră, ci un ansamblu de componente, standarde, documente, proceduri și evidențe care pot fi administrate în infrastructura guvernamentală și pot fi supuse mentenanței de către resurse tehnice competente.

Element de transferabilitate	Ce primește CNAS	Efect
Cod sursă și repository	cod, structură proiect, reguli build, branch/release model	poate reconstrui și audita aplicația
OpenAPI și contracte	contracte API versionate, modele de erori, exemple payload	reduce dependența de implementări informale
Helm/deployment artefacts	pachete instalabile, configurări pe medii, release notes	deployment reproductibil
Runbook și operare	proceduri de start/stop, monitorizare, backup, restore, incident handling	operare mai sigură după go-live
Documentație shared services	workflow, audit, documente, notificări, integrare, reporting layer	înțelegerea mecanismelor centrale ale sistemului

Compatibilitatea cu MCloud și controlul resurselor de infrastructură

SI „Protecția Socială” va fi proiectat pentru găzduire pe platforma tehnologică guvernamentală comună MCloud. Această condiție este tratată ca parte a arhitecturii soluției, nu ca simplă mențiune de deployment. Furnizorul va livra aplicația, componentele, configurările, mecanismele de deployment, observabilitatea,

documentația și runbook-urile astfel încât sistemul să poată fi instalat, operat, monitorizat și susținut în infrastructura pusă la dispoziție prin MCloud.

Găzduirea în MCloud nu modifică responsabilitatea Furnizorului asupra soluției livrate. Furnizorul va rămâne responsabil pentru proiectarea arhitecturii aplicative, dimensionarea necesarului de resurse, containerizarea componentelor, configurarea deployment-ului, definirea cerințelor de stocare, logare, backup, observabilitate, performanță și continuitate. În același timp, resursele fizice sau virtuale efectiv disponibile, politicile de rețea, mecanismele de stocare, serviciile de backup, restricțiile de securitate și mediile tehnice puse la dispoziție prin MCloud trebuie confirmate împreună cu CNAS și STISC înainte de deployment-ul final.

Din acest motiv, oferta nu presupune tacit că orice resursă necesară va exista automat doar prin faptul că sistemul este găzduit în MCloud. Furnizorul va pregăti un dosar de dimensionare și compatibilitate tehnică, care va indica explicit resursele necesare pentru fiecare mediu: dezvoltare, testare, UAT/pre-producție, producție și restabilire/dezastru, dacă aceste medii sunt aprobate în proiect. Dosarul va include necesarul de CPU, memorie, stocare, baze de date, volume pentru documente/atașamente, spațiu pentru backup, loguri, artefacte de deployment, trafic estimat, cerințe de rețea, certificate, acces securizat, monitorizare și retenție operațională.

Pentru CNAS, această abordare transformă MCloud dintr-o presupunere generală de găzduire într-un mecanism verificabil de readiness. Înainte de trecerea către UAT, testare de performanță, go-live sau stabilizare, Furnizorul va verifica dacă mediile MCloud alocate corespund profilului de încărcare și arhitecturii asumate. Dacă resursele sunt insuficiente sau anumite servicii nu sunt disponibile în forma estimată, Furnizorul va documenta impactul, opțiunile tehnice și recomandarea de ajustare, iar CNAS va putea decide și coordona solicitările necesare către STISC.

Matrice de control pentru resursele MCloud

Zonă tehnică	Ce livrează Furnizorul	Ce trebuie confirmat cu CNAS/STISC	Evidență de readiness
Medii tehnice	Definirea mediilor necesare: dev, test, UAT/pre-prod, producție, recovery.	Numărul de medii disponibile, separarea lor, politicile de acces și rețea.	Environment readiness checklist.
Compute și memorie	Sizing inițial pentru componente backend, frontend, batch, gateway, reporting, observability.	Resursele virtuale alocate și posibilitatea de extindere.	Sizing sheet, rezultat load test, recomandări de scalare.
PostgreSQL și date	Model de baze operaționale, istorice, reporting layer, partiționare, backup și retenție.	Tipul de serviciu DB disponibil, limitele de stocare, backup, replicare și administrare.	DB readiness report, backup/restore test.
Documente și atașamente	Model de stocare pentru fișiere, metadate în DB, checksum, audit acces.	Existența unui spațiu dedicat pentru documente/atașamente sau serviciu compatibil.	Storage readiness, test upload/download, test restaurare.
Kubernetes / deployment	Helm charts/manifestări de deployment, configurări pe medii, health checks, readiness/liveness probes, rollout/rollback și runbook.	Platforma de rulare MCloud/STISC, registry, namespace-uri, politici de resurse și servicii gestionate echivalente dacă sunt disponibile.	Deployment readiness report, release package validat, test smoke și procedură rollback.

Observabilitate	Metrics, logs, traces, alerte, correlation ID, dashboarduri operaționale.	Serviciile aprobate pentru colectare loguri, retenție și acces operațional.	Monitoring dashboard, alert test, log retention policy.
Backup și recovery	Runbook, proceduri backup/restore, test de restaurare, recomandări RPO/RTO.	Mecanismele efective oferite de infrastructură și ferestrele de backup.	Backup/restore evidence, DR rehearsal report.
Securitate și acces	Configurări aplicație, certificate, secrete, roluri tehnice, audit.	Politici MCloud/STISC pentru rețea, certificate, acces securizat și segmente.	Security readiness checklist.

Sizing, performanță și extindere controlată

Arhitectura propusă va permite dimensionarea și extinderea controlată a componentelor, dar performanța finală depinde de resursele efectiv alocate și de profilul real al datelor CNAS. Furnizorul va pregăti un sizing inițial pe baza cerințelor de volum, număr de utilizatori, tranzacții, procese batch, raportare statistică, documente și integrări. Acest sizing va fi validat prin testare de performanță pe mediul disponibil, nu doar prin estimări teoretice.

Pentru componentele interactive, Furnizorul va urmări timpii de răspuns, concurența, consumul de CPU/memorie, conexiunile la baza de date și comportamentul în vârf de sarcină. Pentru procesele batch, raportare și închidere de perioadă, Furnizorul va urmări durata joburilor, checkpoint-urile, posibilitatea de reluare, impactul asupra bazei de date și consumul de resurse. Pentru integrare, Furnizorul va urmări latența serviciilor externe, timeouts, retry, circuit breaker și comportamentul degradat.

Dacă testele arată că resursele disponibile nu susțin pragurile asumate, Furnizorul nu va masca problema prin optimizări locale nesigure sau prin reducerea funcționalității. Situația va fi tratată prin mecanism de readiness: raport de performanță, cauză, impact, opțiuni de optimizare, necesar suplimentar de resurse și decizie CNAS privind coordonarea infrastructurală. Astfel, performanța devine un criteriu verificabil.

Pentru a evita interpretări diferite privind responsabilitățile de infrastructură, Furnizorul va livra o matrice de compatibilitate tehnică pentru instalarea SI „Protecția Socială” în MCloud. Matricea va traduce arhitectura propusă în cerințe verificabile pentru platforma de rulare, stocare, baze de date, rețea, securitate, observabilitate și medii de lucru. Această matrice nu transferă către CNAS sau STISC responsabilitatea soluției aplicative; ea stabilește condițiile tehnice în care soluția poate fi rulată, testată, scalată, restaurată și operată conform arhitecturii asumate de Furnizor.

Pachetul de deployment este containerizat și pregătit pentru rulare pe o platformă Kubernetes disponibilă în MCloud, cu suport pentru deployment controlat, servicii de rețea, configurări pe medii, secrete, volume persistente, health probes și limite de resurse. Baza de date țintă pentru soluție este PostgreSQL, cu utilizarea capabilităților necesare pentru sistemul CNAS: indexare, partiționare, materialized views, backup/restore, monitorizare și separarea zonelor operaționale de cele de raportare. Pentru documente, atașamente, exporturi mari și fișiere generate, stocarea persistentă dedicată păstrează conținutul fișierelor separat de tabelele tranzacționale, iar metadatele rămân în baza de date.

Matricea de compatibilitate va fi utilizată în readiness-ul infrastructural și va permite CNAS să coordoneze cu STISC alocarea mediilor, resurselor și serviciilor necesare. Dacă în MCloud anumite servicii sunt furnizate prin mecanisme gestionate echivalente față de cele descrise în ofertă, compatibilitatea se documentează în SDD și în checklisturile de readiness, fără reducerea principiilor arhitecturale asumate: containerizare, configurare pe medii, stocare persistentă, observabilitate, backup, securitate și deployment trasabil.

Zonă tehnică	Cerință de compatibilitate propusă	De ce contează pentru CNAS	Evidență de readiness
Platformă Kubernetes	Suport pentru Deployments/StatefulSets unde este cazul, Services, Ingress/Route, ConfigMaps, Secrets, Persistent Volumes, liveness/readiness probes și resource limits.	Permite rularea controlată, scalarea, izolarea pe medii și self-healing-ul componentelor.	Matrice compatibilitate, deployment test, health check report.
Bază de date PostgreSQL	PostgreSQL ca platformă relațională țintă, cu partiționare, indexare, materialized views, backup/restore, monitorizare și mecanism de migrații DB.	Susține date operaționale, istoric, audit, reporting layer și procese de volum.	DB readiness report, migration scripts, backup/restore test.
Stocare documente	Stocare persistentă dedicată pentru documente/atașamente/exporturi, preferabil object storage sau volum dedicat administrat, cu backup și control acces.	Baza de date nu va fi încărcată cu fișiere mari; documentele rămân accesibile, auditate și restaurabile.	Storage readiness, test upload/download, test restaurare.
Observabilitate	Colectare de logs, metrics, traces/correlation ID, dashboarduri și alerte operaționale.	CNAS și echipa de suport pot vedea cauza incidentelor, nu doar efectul lor.	Monitoring dashboard, alert test, log retention policy.
Rețea și integrare	Rute controlate către MConnect/servicii externe, certificate, politici de acces și timeouts.	Integrarea cu ecosistemul guvernamental nu trebuie să blocheze fluxurile interne când un serviciu extern răspunde lent.	Integration connectivity report, timeout/retry test.
Backup și recovery	Mecanisme de backup, restaurare, retenție, test de restaurare și scenarii RTO/RPO agreate.	Continuity readiness trebuie verificat înainte de go-live, nu presupus.	Backup/restore evidence, DR rehearsal report.

Continuitate, recovery și dependență de infrastructura comună

Pentru un sistem critic, continuitatea nu poate fi lăsată doar la nivelul declarației că aplicația este găzduită în cloud. Furnizorul va defini împreună cu CNAS scenariile de continuitate și restaurare: indisponibilitate parțială a unei componente, indisponibilitate bază de date, indisponibilitate stocare documente, degradare integrare externă, eșec proces batch, eșec deployment și restaurare din backup.

Obiectivele RPO și RTO vor fi propuse în ofertă și confirmate în faza de proiectare, în funcție de mecanismele MCloud disponibile și de criticitatea proceselor CNAS. Furnizorul va pregăti runbook-uri pentru restaurare și proceduri de verificare după incident, iar înainte de go-live se va executa cel puțin un test de restaurare pentru componentele critice, în măsura în care mediile și accesul permit acest lucru.

Această abordare protejează CNAS și Furnizorul de interpretări diferite. Furnizorul proiectează și livrează sistemul pentru operare în MCloud, dar readiness-ul final al infrastructurii se confirmă pe baza resurselor, mediilor, politicilor și serviciilor efectiv disponibile. CNAS rămâne autoritatea care coordonează cu STISC alocarea și validarea resurselor necesare, iar Furnizorul livrează toate informațiile tehnice, evidențele și recomandările necesare pentru această decizie.

10. Securitate informațională, audit și protecția datelor personale

10.1 Poziționarea securității

Securitatea SI „Protecția Socială” va fi tratată ca mecanism de protecție împotriva accesului extern neautorizat, dar și împotriva riscurilor interne generate de eroare umană, abuz de drepturi legitime, intervenții tehnice privilegiate, exporturi excesive, sesiuni lăsate deschise, configurări greșite sau modificări directe ale datelor. Pentru un sistem care gestionează drepturi, decizii, plăți și date personale sensibile, amenințarea relevantă nu este doar atacatorul extern, ci și operațiunea internă care ocolește fluxul controlat al aplicației.

Furnizorul va construi securitatea pe trei niveluri complementare: controlul accesului utilizatorilor, controlul operațiunilor privilegiate și controlul evidențelor. Utilizatorii vor lucra prin roluri, permisiuni, scope de date și acțiuni validate în backend. Administratorii tehnici vor lucra prin conturi separate, drepturi limitate, proceduri aprobate și audit. Evenimentele relevante vor fi jurnalizate astfel încât acțiunile asupra datelor, deciziilor, plăților, documentelor, configurărilor și exporturilor să poată fi reconstruite ulterior.

Această abordare permite CNAS să controleze nu doar cine poate intra în sistem, ci și ce poate face, în ce context, asupra cărui obiect, cu ce justificare și cu ce urmă auditabilă. Securitatea devine astfel parte a guvernanței operaționale a sistemului, nu doar un strat tehnic adăugat la autentificare.

Securitatea informațională pentru SI „Protecția Socială” este tratată ca mecanism operațional al sistemului, nu ca anexă tehnică. Sistemul va gestiona date personale, date contributive, dosare, decizii, drepturi, plăți, documente, rapoarte, integrări și evenimente de business. Din acest motiv, abordarea ofertată va controla nu doar autentificarea utilizatorilor, ci întregul traseu al datelor: cine le vede, cine le modifică, cine le exportă, cine le transmite, ce reguli s-au aplicat și ce evidență rămâne pentru audit, suport și control intern.

Furnizorul va livra o arhitectură de securitate multi-strat, aliniată cerințelor din Caietul de sarcini, principiilor de protecție a datelor cu caracter personal, practicilor de securitate web și modelului operațional CNAS. Abordarea se bazează pe Secure by Design, least privilege, need-to-know/need-to-act, protecția datelor confidențiale, audit business centralizat, validare independentă pe mai multe niveluri și integrare controlată cu serviciile guvernamentale relevante.

Capitolul este ancorat direct în UC18 — administrarea utilizatorilor și controlul accesului — și UC23 — jurnalizarea evenimentelor. În același timp, securitatea nu se limitează la aceste două UC-uri. Ea susține UC03, UC04, UC05, UC09, UC11, UC14, UC19, UC20, UC22 și toate lanțurile operaționale unde se consultă date, se procesează cereri, se generează documente, se rulează proceduri automate, se exportă rapoarte sau se schimbă date cu sisteme externe.

Zonă de securitate	Ce livrează soluția	Efect pentru CNAS
Identitate și acces	Autentificare prin MPass/mecanisme aprobate, profil intern, roluri, grupuri, delegări, permisiuni pe obiect și acțiune.	Acces acordat în funcție de rol, context, competență și scop operațional.
Protecția datelor personale	Minimizare, mascare, clasificare, protecție suplimentară pentru date deosebit de confidențiale, control export și reguli pentru medii non-producție.	Reducerea expunerii nejustificate și respectarea principiilor de confidențialitate și protecție a vieții private.
Securitate aplicație/API	Validări server-side, protecție OWASP, control upload, rate limiting, securizare endpointuri, versionare API și reguli de acces în backend.	Funcționalitățile nu pot fi ocolite prin UI, API sau date manipulate.

Zonă de securitate	Ce livrează soluția	Efect pentru CNAS
Audit business și jurnalizare	Componentă centrală de audit, politici granular configurabile, evenimente pe obiect, utilizator, rol, acțiune, rezultat și context.	Trasabilitate completă pentru acces, modificări, documente, rapoarte, integrări și proceduri automate.
Securitate operațională	DevSecOps, scanări, configurări pe medii, secrete, monitorizare, alertare, incident response și backup/recovery.	Sistem pregătit pentru exploatare, suport, investigație și continuitate.

Figura 1. Model multi-layer security pentru SI „Protecția Socială”

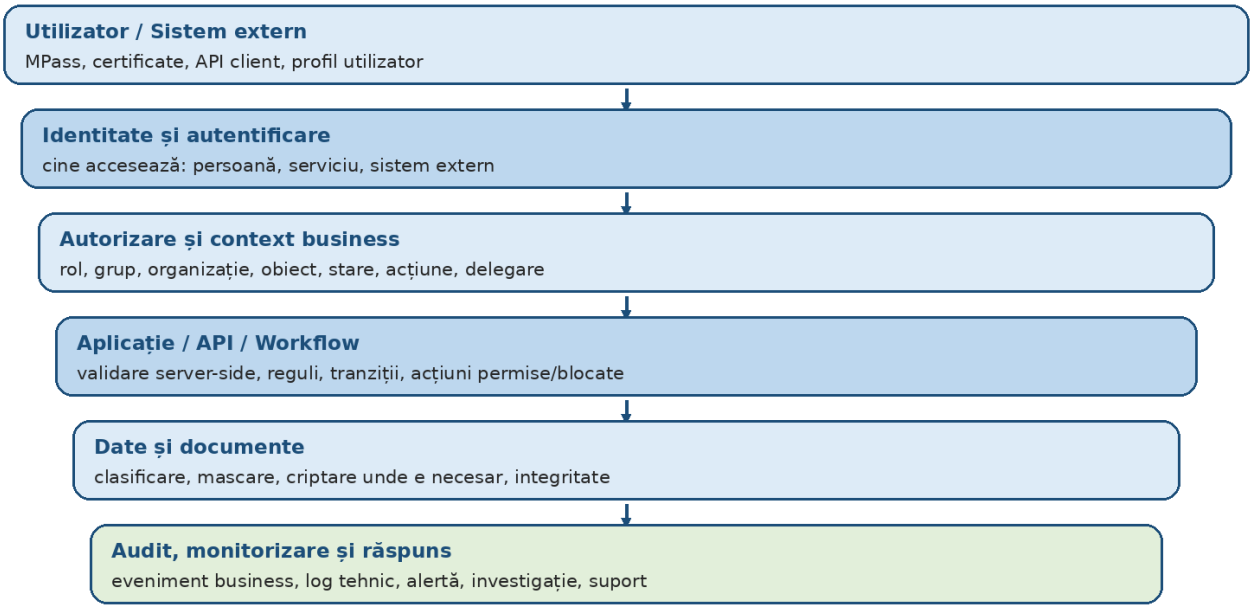


Figura Model multi-layer security pentru SI „Protecția Socială”

10.2 Ancora în cerințele ToR, UC-uri și standarde

Caietul de sarcini cere ca SI „Protecția Socială” să permită controlul adecvat al riscurilor de securitate, să fie aliniat politicilor de securitate ale CNAS, să prevină, detecteze și trateze incidentele și să implementeze o abordare multi-layered security. Abordarea ofertată transformă aceste cerințe în mecanisme livrabile: arhitectură de securitate documentată, matrice de comunicare între servicii, privilegii minime pentru procese, credentiale configurabile și protejate, autentificare sigură, protecție pentru interfața publică, validare de date, control acces, audit centralizat, protecție date confidențiale, backup/recovery și reziliență.

Oferta tratează cerințele SEC ca parte a proiectării, implementării și acceptanței. Matricea de conformitate va păstra maparea cerință-cu-cerință, iar această secțiune explică mecanismul prin care cerințele devin funcționalitate, arhitectură, proceduri, teste și evidențe de acceptanță.

Cerințe / UC	Interpretare în ofertă	Mecanism propus
SEC 001–SEC 010	Arhitectură Secure by Design, privilegii minime, credentiale protejate, autentificare sigură, protecție OWASP și control interfață publică.	model multi-layer security, matrix comunicare, secrets management, Spring Security, rate limiting/CAPTCHA unde este cazul, DevSecOps

Cerințe / UC	Interpretare în ofertă	Mecanism propus
SEC 024–SEC 029 / UC18	Administrare utilizatori, grupuri, roluri, permisiuni, reguli business, delegări, rapoarte de acces și MPass.	IAM intern + MPass, RBAC/ABAC pragmatic, matrice rol-permisiune, delegare temporară, recertificare acces
SEC 030–SEC 037	Validarea datelor, prevenirea manipulării, marcaje de securitate, protecție date confidențiale, integritate și anti-tampering.	validare client/server/backend/DB, formulare specializate, clasificator securitate, mascare, criptare unde este justificată, checksums, constrângeri, joburi integritate
SEC 038–SEC 043 / UC23	Audit centralizat, politici de audit configurabile, evenimente pe componentă, categorie de date, obiect și stare.	Business Audit Service, audit policy catalog, event store, correlation ID, interfață de căutare și rapoarte audit
SEC 058–SEC 066	Erori, excepții, notificări, backup, integritate în caz de cădere, restabilire, SPOF și reziliență.	observabilitate, alertare, backup/restore, idempotency, checkpoint-uri, readiness/liveness probes, DR runbook

Clarificare terminologică. „Secure by Design” înseamnă că mecanismele de securitate sunt proiectate în arhitectură, fluxuri, API-uri, date și operare de la început. Nu reprezintă o etapă de testare aplicată la final.

Clarificare terminologică. „Zero Trust” este folosit în sens pragmatic: niciun utilizator, serviciu sau componentă nu este considerată implicit de încredere doar pentru că se află în aceeași rețea sau platformă. Accesul se acordă explicit, pe identitate, rol, context, scop și politică.

10.3 Identitate, autentificare și autorizare granulară

Soluția va separa autentificarea de autorizare. Autentificarea stabilește identitatea utilizatorului sau a sistemului care accesează SI „Protecția Socială”. Autorizarea stabilește ce poate face acea identitate în contextul concret al obiectului accesat. Această separare este esențială: MPass sau un alt mecanism aprobat poate confirma cine este utilizatorul, dar sistemul trebuie să decidă intern dacă utilizatorul poate vedea un dosar, modifica o cerere, aproba o decizie, genera un raport, exporta date sau administra roluri.

Furnizorul va implementa un model de acces intern care combină roluri, grupuri, drepturi explicite, apartenență organizațională, delegări temporare, reguli business și starea obiectului. Drepturile nu vor fi doar „meniuri vizibile”. Ele vor fi aplicate în backend, la nivel de API și servicii, astfel încât o acțiune nepermisă să fie blocată chiar dacă este apelată direct prin endpoint sau printr-un client modificat.

Modelul de autorizare va susține scenarii de acces permis și blocat pentru date, documente, rapoarte, exporturi, configurări, aprobări și administrare. Pentru acțiuni critice sau date deosebit de confidențiale, soluția va putea aplica protecție suplimentară: reautentificare, confirmare, justificare, verificare de context sau mascare parțială.

Element de acces	Cum va funcționa	Control livrat
Utilizator / identitate	Identitatea vine prin MPass sau mecanism aprobat și este legată de profilul intern al utilizatorului.	utilizator intern, status, organizație, roluri, grupuri, date profil
Roluri și grupuri	Rolurile definesc pachete de acțiuni, iar grupurile pot reflecta structuri operaționale CNAS/CTAS.	matrice roluri-permisiuni, rapoarte de acces, administrare prin UC18
Reguli business	Accesul poate depinde de autorul obiectului, starea dosarului, termen, unitate teritorială, tip serviciu sau sensibilitate.	politici need-to-know/need-to-act aplicate în backend
Delegare temporară	Drepturile pot fi atribuite temporar, cu perioadă, motiv, scope și audit.	delegare, suspendare/păstrare drepturi, expirare, raport delegări

Element de acces	Cum va funcționa	Control livrat
Segregare atribuții	Operațiuni administrative sau funcționale sensibile pot necesita separarea inițierii de confirmare.	scenarii maker-checker pentru configurări/decizii cu risc ridicat
Audit acces	Accesul, refuzul, modificarea, exportul și acțiunile critice sunt jurnalizate conform politicilor de audit.	eveniment audit cu utilizator, rol, obiect, acțiune, rezultat, timp, context

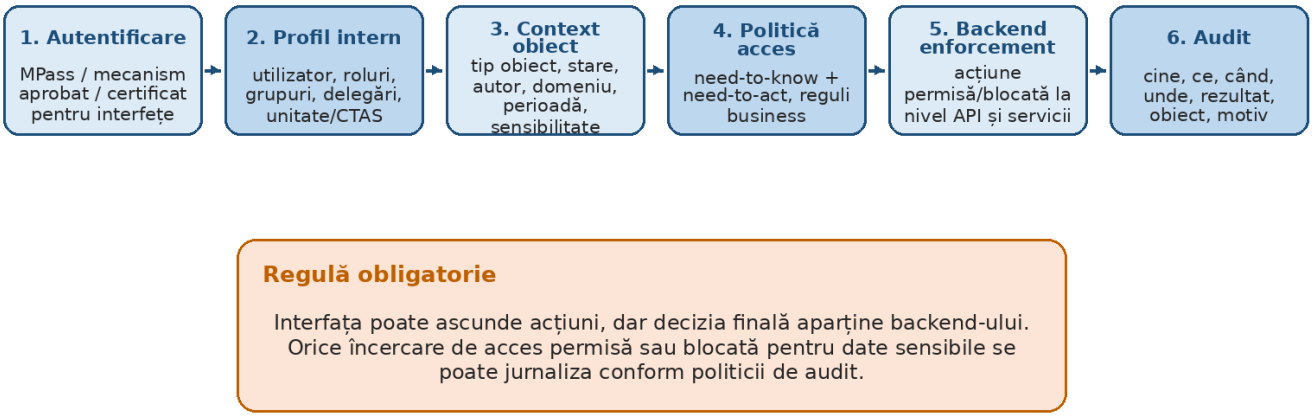


Figura Decizia de acces: de la autentificare la audit

Controlul accesului privilegiat și al intervențiilor directe în baza de date

În mediul de producție, modificările directe în baza de date nu vor fi mecanism operațional normal pentru corectarea datelor sau rezolvarea incidentelor. Orice intervenție tehnică asupra datelor operaționale va fi tratată ca operațiune controlată: tichet de suport sau schimbare aprobată, justificare, script versionat, analiză de impact, fereastră de execuție, rezultat verificat și evidență de închidere. În acest mod, accesul tehnic privilegiat nu devine canal paralel de modificare a datelor CNAS.

Soluția va separa conturile aplicative, conturile umane, conturile administrative și conturile de integrare. Conturile aplicative vor avea drepturile minime necesare pentru funcționare și nu vor utiliza conturi de administrator al bazei de date. Conturile privilegiate vor fi limitate, atribuite nominal, monitorizate și utilizate numai pentru operațiuni tehnice justificate. Conturile comune sau anonime nu vor fi utilizate pentru operațiuni care pot modifica date, configurări sau drepturi.

Pentru operațiunile cu risc ridicat, Furnizorul va livra proceduri de lucru și evidențe tehnice: registru de intervenții privilegiate, jurnal de scripturi rulate, legătură cu tichetul aprobat, backup sau punct de revenire când scenariul o cere, rezultat de verificare și raport de impact. Astfel, chiar dacă infrastructura permite acces administrativ tehnic, sistemul și procedura de operare fac intervenția vizibilă, justificată și verificabilă.

Tip intervenție	Control propus	Evidență livrată
Corecție date în producție	tichet aprobat, script versionat, verificare înainte/după, audit DB și audit operațional	change/support record, script, rezultat verificare, semn-off
Operațiune DBA	cont nominal, acces limitat, fereastră aprobată, jurnal tehnic	DB activity log, action log, raport intervenție

Tip intervenție	Control propus	Evidență livrată
Schimbare configurare critică	aprobare funcțională, versiune, motiv, testare în mediu non-producție	configuration history, decision log, test evidence
Acces de urgență / break-glass	activare excepțională, durată limitată, justificare, review post-incident	break-glass record, audit, post-incident review
Export sau modificare masivă	drept dedicat, justificare, limitare scope, audit și alertă	export log, approver, parametri, fișier generat

10.4 Clasificarea datelor, marcaje de securitate și reguli de afișare

Soluția va implementa clasificarea datelor și marcajul de securitate pentru afișările de date, conform cerinței din ToR privind marcarea datelor. Clasificarea nu va fi tratată ca text decorativ pe ecran, ci ca regulă operațională care influențează afișarea, exportul, jurnalizarea, accesul, caching-ul, mascare și protecția suplimentară.

În SRS/SDD se va defini împreună cu CNAS clasificatorul de securitate aplicabil: public, intern, confidențial, deosebit de confidențial sau alte niveluri stabilite de CNAS. Fiecare nivel va avea reguli de manipulare: cine poate vedea, dacă datele se maschează, dacă pot fi exportate, ce audit este necesar, ce retenție se aplică și dacă sunt permise în medii non-producție.

Nivel date	Exemple posibile	Reguli de tratament în sistem
Public / depersonalizat	informații publice, date de interes public fără identificatori personali	publicare controlată, fără expunere PII, audit unde este necesar
Intern operațional	sarcini, stări dosar, indicatori operaționali fără date excesive	acces pe rol, dashboarduri, log tehnic minimizat
Confidențial	IDNP, date personale, date despre drepturi, plăți, cereri, documente	acces need-to-know, mascare în liste, audit acces/modificare/export
Deosebit de confidențial	date sensibile, combinații de date cu risc ridicat, documente justificative, date cu impact major asupra persoanei	mascare implicită, reautentificare/confirmare unde este cazul, criptare sau protecție suplimentară, audit strict
Date tehnice sensibile	secrete, tokenuri, certificate, parole, connection strings	secrets management, acces tehnic limitat, interdicție hard-coded, rotație/control acces

10.5 Protecția datelor personale pe ciclul de viață

SI „Protecția Socială” va prelucra date personale în scopuri instituționale stabilite de cadrul normativ și de procesele CNAS. Soluția va susține principiile de legalitate, confidențialitate, integritate, neexcesivitate, pertinență și protecție a vieții private prin mecanisme tehnice și operaționale vizibile: limitare acces, minimizarea datelor afișate, mascarea în liste, control export, audit și reguli pentru utilizarea datelor în testare, suport și raportare.

Furnizorul nu va multiplica datele personale pentru comoditate tehnică. Datele vor fi utilizate prin surse controlate, read models, data marts, snapshot-uri sau documente cu reguli clare de acces. În mediile de dezvoltare, testare și instruire nu se vor utiliza date reale neprotejate decât dacă CNAS aprobă explicit și sunt aplicate măsuri de protecție adecvate. Unde este posibil, seturile de test vor fi sintetice, mascate, anonimizate sau pseudonimizate.

Pentru datele afișate în interfață, soluția va aplica principiul „minimum util pentru acțiune”: listele și dashboardurile vor afișa date suficiente pentru identificarea obiectului de lucru, dar nu vor expune inutil câmpuri sensibile. Accesul la detalii complete va fi controlat pe rol, context, obiect și scop operațional.

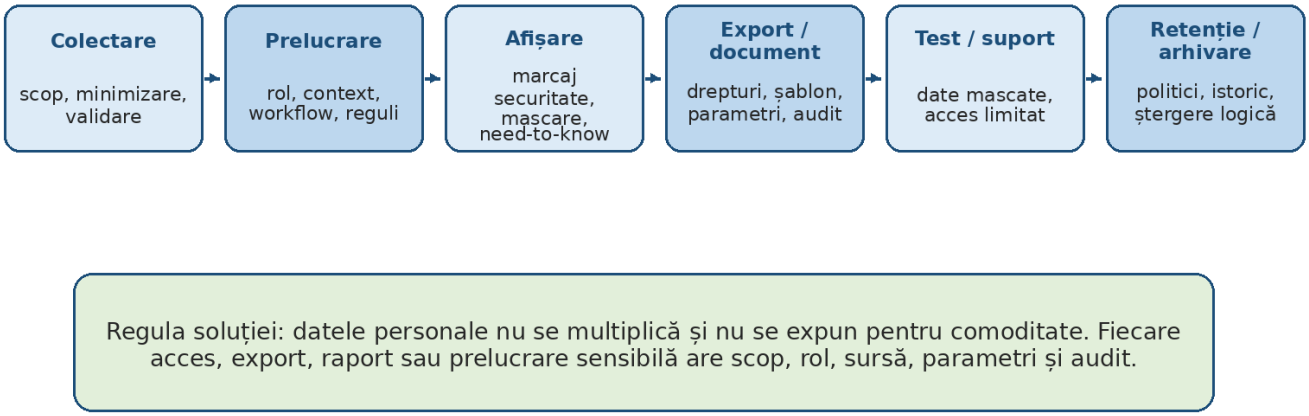


Figura Protecția datelor pe ciclul de viață

10.6 Securitatea interfețelor, API-urilor și integrărilor externe

Sistemul va expune și consuma servicii prin canale controlate. Interfețele expuse vor utiliza metode sigure de autentificare și autorizare, certificate sau tokenuri conform arhitecturii aprobate, iar accesul către servicii externe va fi centralizat prin Integration Gateway/WSAdapter. Modulele de business nu vor implementa apeluri externe dispersate, deoarece acest model ar slăbi controlul asupra autentificării tehnice, jurnalizării, timeout-urilor, erorilor și protecției datelor transmise.

Integration Gateway va gestiona contractele de integrare, transformarea payload-urilor, validarea, timeouts, retry, circuit breaker, jurnalizarea minimizată, snapshot-urile relevante și auditul schimburilor de date. Dacă un serviciu extern este indisponibil sau răspunde lent, sistemul nu va îngheța fluxul operațional: va returna o stare controlată, va înregistra evenimentul, va notifica responsabilul unde este cazul și va permite reluarea verificării conform fluxului.

API-urile interne și externe vor fi documentate, versionate și testate. Versionarea API-urilor va permite evoluția sistemului fără ruperea integrărilor existente. În cazul API-urilor cu date personale sau efect operațional, payload-urile vor fi minimizate, logurile nu vor păstra date confidențiale în clar, iar accesul va fi legat de scop și rol tehnic.

Zonă integrare	Mecanism de securitate	Rezultat verificabil
API frontend-backend	token/session validat, CSRF/CORS controlat, server-side authorization, rate limiting unde este cazul	apeluri permise/blocate, loguri, teste de securitate
Sisteme externe prin MConnect/servicii guvernamentale	Integration Gateway, certificate, contracte, snapshot, audit, circuit breaker	contract tests, erori tratate, audit schimb date
Servicii interne	autentificare serviciu, autorizare tehnică, network policy/matrix comunicare, mTLS/JWT unde este aprobat	matrice comunicare, test conectivitate, evidență deployment
Interfață publică	CAPTCHA/rate limiting unde se justifică, validare input, limitare date expuse, anti-scraping pragmatic	scenarii publice testate, log abuz, protecție suprasolicitare
Exporturi și descărcări	drept explicit, parametri, limitare volum, audit generare/descărcare	raport audit export, scenarii UAT, evidență acces

10.7 Securitate aplicație, validare și protecție OWASP

Proiectarea și testarea acoperă riscurile relevante din OWASP Top 10, cu accent pe broken access control, injection, insecure design, security misconfiguration, vulnerable components, authentication failures, software/data integrity failures, logging/monitoring failures și SSRF pentru componentele expuse acestui tip de risc. Controlul nu va fi doar declarativ: validarea, autorizarea, configurările de securitate, scanarea dependențelor și testarea cazurilor negative vor fi integrate în procesul de livrare.

Toate datele introduse de utilizatori, primite din formulare, fișiere sau aplicații externe vor fi validate. Validarea client-side va susține experiența utilizatorului, dar validarea server-side și validarea în serviciile backend rămân autoritative. Pentru date critice sau sensibile, schimbările se vor face prin formulare specializate și fluxuri controlate, cu stare, responsabil, verificare și audit.

Fișierele încărcate vor fi tratate ca input nesigur până la verificare. Soluția va aplica reguli de tip fișier, dimensiune, extensie, conținut, scanare antivirus unde infrastructura o permite, stocare separată, metadate în baza de date, checksum și acces controlat. Descărcarea fișierelor va fi verificată prin autorizare și audit.

10.8 Secrete, criptare, caching și protecția datelor confidențiale

Credențialele, cheile, certificatele, tokenurile, parolele și connection string-urile nu vor fi hard-coded și nu vor fi stocate în clar în cod, fișiere de configurare sau baza de date. Secrets management-ul aprobat pentru MCloud/Kubernetes sau un mecanism echivalent acceptat în infrastructura de găzduire controlează aceste valori sensibile. Configurările vor fi separate pe medii, iar accesul la secrete va fi limitat la procesele și rolurile tehnice necesare.

Datele în tranzit vor fi protejate prin canale securizate. Pentru datele deosebit de confidențiale, soluția va susține protecție suplimentară în funcție de clasificarea datelor și deciziile SRS/SDD: mascare, criptare la nivel de stocare sau câmp unde este justificat, reautentificare sau confirmare suplimentară la acces, jurnalizare strictă și restricții de export.

Cache-ul nu devine sursă de adevăr pentru date cu efect juridic, financiar sau operațional critic. Dacă este inclus în SDD, Redis/cache engine-ul va fi limitat la nomenclatoare, configurări citite frecvent, date temporare, rate limiting sau coordonare tehnică, cu TTL, invalidare, reguli de acces și monitorizare. Datele confidențiale nu vor fi păstrate nesecurizat în cache sau loguri.

10.9 Audit business, jurnalizare centralizată și trasabilitate

Soluția va livra o componentă centrală de audit care colectează și gestionează evenimente de audit la nivelul componentelor sistemului. Auditul nu va fi redus la loguri tehnice. Logurile tehnice ajută suportul și operarea; auditul business explică acțiunile instituționale: cine a consultat date, cine a modificat un obiect, cine a aprobat o decizie, cine a generat un document, cine a exportat un raport, ce integrare a fost apelată și ce rezultat a fost obținut.

Politicile de audit vor fi configurabile granular: pe componentă funcțională, zonă de interfață, categorie de date, tip eveniment, stare obiect, interval, acțiune și nivel de sensibilitate. Această configurabilitate permite CNAS să ajusteze auditul în funcție de risc și cerințe interne, fără a transforma auditul într-un volum inutil de loguri greu de analizat.

Fiecare eveniment de audit relevant va include cel puțin: identificator eveniment, utilizator/serviciu, rol/context, obiect afectat, acțiune, rezultat, dată/oră, sursă/IP sau context tehnic când scenariul o cere,

correlation ID, parametri relevanți fără expunere excesivă a datelor, motiv/justificare când fluxul o cere și referință către document, raport, integrare sau job.

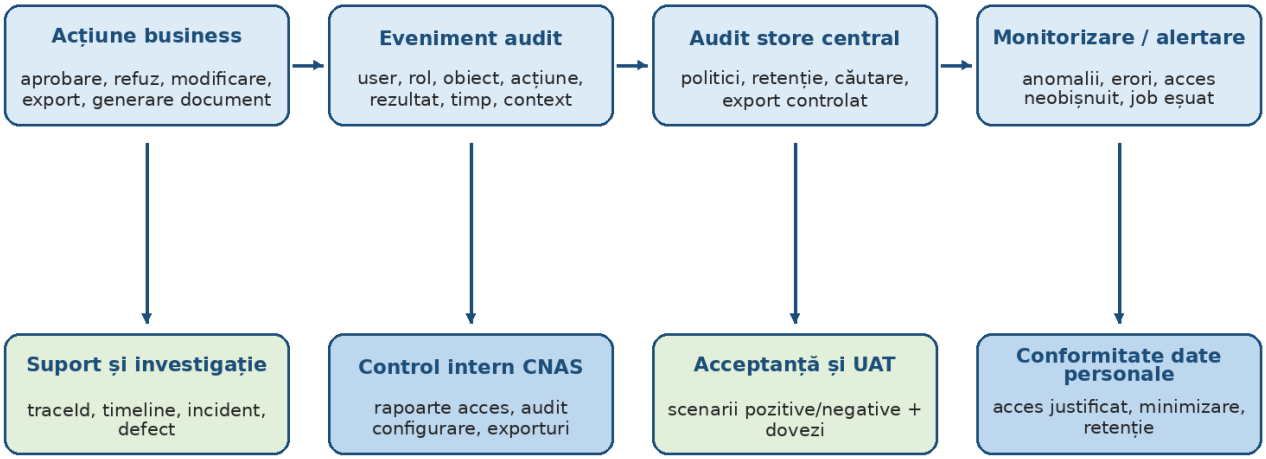


Figura Lanțul evenimentului de securitate și audit

Eveniment auditat	De ce contează	Evidență pentru CNAS
Acces la profil/dosar/date personale	demonstrează cine a consultat date sensibile și în ce context	audit filtrabil pe utilizator, obiect, perioadă, rol
Modificare date critice	protejează integritatea și permite reconstrucția schimbării	before/after sau referință versiune, flux, aprobare, motiv
Aprobare/refuz/decizie	explică efectul juridic sau operațional asupra persoanei/dreptului	utilizator, rol, rezultat, document generat, stare dosar
Export/raport/descărcare	controlează exfiltrarea și utilizarea datelor în afara ecranului	parametri, volum, șablon, utilizator, moment, fișier
Configurare rol/flux/șablon	arată cine a modificat funcționarea sistemului	versiune, aprobare, activare, utilizare ulterioară
Integrare externă	arată ce date au fost solicitate/transmise și cu ce rezultat	contract, sistem extern, status, snapshot, eroare
Job/procedură automată	arată execuția proceselor de volum și erorile	run ID, start/stop, număr procesate, excepții, reluare

10.10 Integritatea datelor și prevenirea manipulării

Soluția va proteja integritatea datelor prin validări, constrângeri, tranzacții, versiuni, istoric și controale de rutină. Pentru datele cu efect asupra drepturilor, deciziilor, plăților, contribuțiilor sau rapoartelor, sistemul nu va permite modificări informale directe în baza de date ca mecanism operațional. Modificările vor trece prin formulare, fluxuri, API-uri și servicii controlate, cu audit și validare.

Procesele batch, recalculările, importurile, migrarea, generarea plăților și raportarea utilizează checkpoint-uri, idempotency, reconciliation și error bucket. Dacă o procedură de volum se oprește la 80%, reluarea trebuie să fie controlată și să nu dubleze rezultate, plăți, notificări sau documente. Această regulă este parte a securității și integrității, nu doar a performanței.

Vor fi implementate verificări de integritate asupra relațiilor critice: cerere-dosar-decizie-document, drept-plată, plătitor-contribuții-cont, raport-snapshot, șablon-document, rol-permisiune și integrare-snapshot. Rezultatele verificărilor vor putea alimenta rapoarte de excepții și notificări către persoane responsabile.

10.11 DevSecOps, testare de securitate și readiness

Securitatea va fi integrată în procesul de dezvoltare și livrare. Pipeline-urile CI/CD vor include verificări precum code review, SAST, scanare dependențe, scanare imagini container, verificări de configurare, teste de securitate funcțională și, unde se aprobă, DAST pe medii de test/pre-producție. Vulnerabilitățile vor fi înregistrate, clasificate, remediate și retestate în funcție de severitate și impact.

Testarea de securitate va acoperi scenarii pozitive și negative: acces permis, acces blocat, acțiune nepermisă prin UI, acțiune nepermisă prin API, export fără drept, upload fișier neacceptat, date manipulate, CSRF/CORS unde este relevant, încercări de injection, acces la document fără rol, acces la raport cu parametri neautorizați și apel integrare cu credentiale invalide.

Readiness-ul de securitate înainte de UAT, go-live și stabilizare va include evidențe: matrice roluri-permisiuni, rezultate test acces, raport scanări, stare vulnerabilități, politici audit, configurări secrete, matrice comunicare, proceduri incident, loguri de test, raport backup/restore și confirmarea că datele din medii non-producție sunt protejate conform regulilor agreate.

10.12 Monitorizare, incidente de securitate și răspuns operațional

Sistemul va livra semnale operaționale și de securitate care permit detectarea incidentelor, erorilor și comportamentelor anormale. Observabilitatea va include logs, metrics, traces, correlation ID, dashboarduri tehnice și alerte. Evenimente precum creșteri neobișnuite de autentificări eșuate, acces repetat la date sensibile, exporturi voluminoase, eșecuri de integrare, joburi blocate, erori de validare sau indisponibilități vor putea fi urmărite și escalate.

Răspunsul la incidente va fi conectat la modelul de suport și SLA. Pentru fiecare incident relevant se va putea reconstrui timeline-ul: moment, componentă, utilizator/serviciu, acțiune, efect, date afectate, remedieri și confirmare de revenire. Furnizorul va livra runbook-uri pentru incidente tehnice și de securitate, iar CNAS va putea integra aceste proceduri în politicile sale instituționale.

Backup-ul, recovery-ul, integritatea datelor și reziliența sunt tratate ca parte a securității. Sistemul va susține proceduri de backup/restore, verificări de restaurare, protecție împotriva punctelor singulare de cădere acolo unde infrastructura MCloud permite și mecanisme de restabilire operativă conform parametrilor stabiliți în SDD/SLA.

10.13 Separarea mediilor și protecția datelor în testare, instruire și suport

Mediile de dezvoltare, testare, UAT/pre-producție și producție vor fi separate logic și operațional. Accesul la datele de producție nu se extinde automat către medii non-producție. Dacă scenariile de testare, migrare sau instruire necesită date apropiate de realitate, seturile vor fi pregătite controlat: sintetice, mascate, anonimizate, pseudonimizate sau aprobate explicit de CNAS cu măsuri suplimentare.

Suportul tehnic nu va presupune acces liber la date personale. Investigațiile de suport vor utiliza loguri minimizate, correlation ID, date tehnice și, când este absolut necesar, acces controlat și jurnalizat la obiectul afectat. Orice acces operațional al echipei de suport la date sensibile va fi limitat, justificat și auditat conform politicilor agreate.

Mediu	Regulă de securitate	Evidență
Development	fără date reale neprotejate; secrete separate; acces doar echipei autorizate	configurări mediu, scanări, date test
Test	date mascate/sintetice, verificări automate, acces QA/dezvoltare controlat	test reports, data masking evidence
UAT / Model Office	date reprezentative aprobate, utilizatori CNAS, drepturi pe roluri reale	UAT pack, roluri de test, audit acces
Pre-production	configurație apropiată de producție, teste de performanță/securitate, fără expunere necontrolată	readiness checklist, scanări, deployment rehearsal
Production	acces minim, monitorizare, audit strict, schimbări prin release control	release notes, audit, incident log, backup evidence

10.14 Evidențe de acceptanță pentru securitate și protecția datelor

Acceptanța pentru securitate nu se va baza pe afirmația că sistemul este securizat. Furnizorul va prezenta evidențe concrete, corelate cu cerințele SEC, UC18, UC23 și scenariile funcționale. Pentru CNAS, aceste evidențe arată că sistemul aplică securitatea în fluxurile reale: acces, dosar, decizie, raport, document, integrare, configurare și procedură automată.

Zonă verificată	Scenariu minim	Evidență așteptată
UC18 - roluri și drepturi	utilizator cu rol permis accesează acțiunea; utilizator fără rol este blocat în UI și backend	matrice roluri, capturi, test API, audit acces/refuz
Delegare drepturi	drept temporar acordat, utilizat, expirat/revocat și auditat	istoric delegare, audit, raport drepturi active
Date confidențiale	afișare cu marcaj securitate, mascare în listă, acces detaliu doar pe rol	capturi, configurare clasificator, audit consultare
Export raport/document	export permis/blocat după rol și parametri, cu jurnalizare	fișier generat, log export, parametri, utilizator
Integrare externă	apel reușit, timeout, eroare și retry/circuit breaker controlat	log integrare, snapshot, alertă, audit eveniment
Audit business	modificare dată critică, aprobare decizie, generare document și job automat jurnalizate	jurnal central filtrabil, correlation ID, raport audit
Validare și anti-manipulare	date manipulate prin client/API sunt respinse server-side	test negativ, eroare controlată, log securitate
DevSecOps	scanare cod/dependințe/container și remediere vulnerabilități	raport scanare, defect log, retestare
Medii non-producție	date de test mascate sau sintetice, acces controlat	evidence masking, listă utilizatori, audit acces

MSign pentru acțiuni și documente cu efect juridic sau financiar

Pentru acțiunile care produc efect juridic sau financiar major, simpla autentificare a utilizatorului nu este întotdeauna suficientă ca nivel de confirmare. Integrarea cu MSign sau cu mecanismul guvernamental aprobat de semnătură electronică este prevăzută pentru documentele și acțiunile critice stabilite în SRS/SDD împreună cu CNAS.

Acțiunile care pot intra în această categorie includ aprobarea finală a unei decizii, semnarea documentelor oficiale, confirmarea unor liste sau comenzi de plată, validarea unor rectificări cu impact financiar, aprobarea unor schimbări administrative sensibile sau alte operațiuni stabilite de CNAS ca necesitând semnătură

electronică. Semnarea nu va fi aplicată mecanic asupra tuturor acțiunilor, pentru a nu bloca exploatarea curentă, ci asupra punctelor în care sistemul produce efect oficial și unde CNAS decide că este necesară confirmare juridică suplimentară.

Pentru fiecare document sau acțiune semnată, sistemul va păstra legătura dintre obiectul operațional, utilizator, rol, moment, versiunea documentului, rezultat, semnătură, audit și eventualele notificări sau plăți asociate. Această legătură permite reconstruirea traseului deciziei și reduce riscul contestării ulterioare a acțiunilor critice.

Audit asincron, anti-tampering și audit la nivel de bază de date

Auditul va acoperi evenimentele relevante de securitate, business, administrare și protecție a datelor, fără a transforma fiecare interacțiune tehnică într-o operațiune blocantă pentru interfața utilizatorului. Pentru evenimentele cu volum mare, jurnalizarea va fi proiectată astfel încât să poată funcționa asincron sau prin mecanisme de buffer/queue, păstrând consistența și posibilitatea de reluare. Astfel, sistemul poate jurnaliza operațiunile importante fără a degrada inutil experiența utilizatorului sau timpii de răspuns.

Auditul aplicativ va fi completat de controale la nivel de bază de date pentru operațiuni privilegiate, modificări directe, scripturi de producție, exporturi și operațiuni administrative cu risc ridicat. Auditul de bază de date nu înlocuiește auditul business al aplicației, ci îl completează pentru scenariile în care o acțiune tehnică ar putea ocoli fluxurile aplicației.

Evenimentele de audit critice vor fi protejate împotriva alterării. Sistemul va utiliza mecanisme append-only, drepturi limitate de administrare, retenție controlată, jurnalizare centralizată și, unde este justificat, semnare/hash sau alte mecanisme de integritate asupra seturilor de loguri. Scopul este ca un utilizator sau administrator să nu poată șterge ori modifica urmele unei acțiuni sensibile fără a lăsa la rândul său o evidență.

Acțiune sensibilă	Audit aplicativ	Audit DB / tehnic	Jurnal centralizat	Verificare / alertă
aprobare, export, modificare, acces date	utilizator, rol, obiect, rezultat, context	script, cont privilegiat, tabel, volum modificat	append-only, retenție, acces controlat	anomalii, review, evidență incident
eveniment business	legat de UC/flux/decizie	nu se aplică dacă nu există operațiune DB directă	corelat prin correlation ID	reconstrucție traseu
intervenție privilegiată	tichet / decizie / motiv	DB activity monitoring	log securizat	review post-intervenție

Model RBAC cu politici contextuale controlate, fără ABAC neadministrabil

Modelul de acces va porni de la roluri operaționale clare și administrabile. Rolurile vor defini responsabilitățile de bază ale utilizatorilor, iar permisiunile vor controla acțiunile disponibile: vizualizare, creare, examinare, aprobare, respingere, semnare, export, configurare, administrare sau suport.

Pentru a reflecta realitatea CNAS, modelul va utiliza și reguli contextuale controlate: apartenență organizațională, teritoriu/CTAS, tip serviciu, stare dosar, tip document, nivel de aprobare, proprietar de sarcină sau scopul accesului. Aceste reguli nu vor fi introduse ca expresii arbitrare și greu de administrat în producție. Ele vor fi documentate, versionate, testate și aprobate în modelul de securitate.

Furnizorul va evita transformarea politicilor de acces într-un mecanism opac. Pentru fiecare regulă contextuală se va defini scopul, domeniul de aplicare, datele utilizate, efectul asupra acțiunilor, cazurile

negative și testele aferente. CNAS va putea verifica nu doar lista de roluri, ci și modul în care sistemul decide accesul într-un caz concret.

Element de acces	Se gestionează prin	Control de administrabilitate
Rol operațional	catalog roluri și permisiuni	denumire, scop, acțiuni permise, proprietar funcțional
Scope organizațional / teritorial	atribut utilizator + date obiect	reguli documentate și testate pe cazuri pozitive/negative
Stare obiect	workflow și tranziții permise	backend blochează acțiunile nepermise
Acțiune sensibilă	drept dedicat + posibilă reautentificare / MSign	audit extins și justificare
Export / vizualizare masivă	permisiune separată + limitare parametri	audit și alertă anomalie

Managementul sesiunilor și protecția stațiilor nesupravegheate

Sistemul va include politici de management al sesiunilor pentru a reduce riscul utilizării neautorizate a unei sesiuni valide. Autentificarea prin mecanismul guvernamental aprobat va fi completată de timeout de inactivitate, invalidarea sesiunii la logout, protecție împotriva session fixation, cookie-uri securizate, rotație de token când documentul sau procesul o solicită și reautentificare sau reconfirmare pentru acțiuni sensibile.

Pentru formularele lungi sau operațiunile care presupun completare graduală, soluția va putea utiliza mecanisme de draft/autosave controlat, astfel încât expirarea sesiunii sau întreruperea temporară să nu conducă automat la pierderea datelor introduse. Autosave-ul nu va transforma datele incomplete în date oficiale; acestea vor rămâne în stare de draft până la validare și transmitere conform workflow-ului.

Politicile de sesiune vor fi corelate cu nivelul de risc al acțiunii. Consultarea generală poate avea reguli diferite de aprobarea unei decizii, exportul masiv, modificarea rolurilor sau semnarea unui document. Această diferențiere protejează sistemul fără a face utilizarea zilnică inutil de greoaie.

Drepturile persoanei vizate, corectarea datelor și retenția legală

Soluția va susține mecanismele necesare pentru identificarea, consultarea, corectarea și exportul datelor personale în limitele temeiurilor legale aplicabile. Pentru un sistem public de evidență, anumite date trebuie păstrate conform obligațiilor legale, iar ștergerea completă nu poate fi tratată ca regulă generală. Sistemul va permite tratarea solicitărilor persoanelor vizate într-un mod controlat, fără compromiterea evidențelor legale, a auditului sau a trasabilității deciziilor.

Corectarea datelor va fi diferențiată de ștergerea datelor. Dacă un câmp este eronat, sistemul trebuie să poată păstra istoricul modificării, motivul, utilizatorul, momentul, documentul justificativ și efectul asupra proceselor. Dacă o solicitare vizează restricționarea, accesul sau portabilitatea datelor, sistemul va furniza datele și evidențele în forma permisă de cadrul legal și de rolurile aprobate.

Retenția datelor va fi tratată prin politici clare: date operaționale, date istorice, documente generate, loguri de audit, backupuri, exporturi și date din medii non-producție. Furnizorul va documenta aceste categorii în SRS/SDD și în documentația de operare, astfel încât CNAS să poată administra datele pe durata ciclului lor de viață.

Suport pentru evaluarea impactului asupra protecției datelor și mascarea datelor non-producție

Furnizorul va sprijini CNAS cu informațiile tehnice și funcționale necesare pentru evaluarea impactului asupra protecției datelor personale, acolo unde aceasta este necesară. Sprijinul va include descrierea

categoriilor de date, fluxurilor de prelucrare, rolurilor, integrărilor, stocării, retenției, accesului, jurnalizării, exporturilor, mediilor tehnice și măsurilor de securitate implementate.

În medii de dezvoltare, testare, instruire sau demonstrare, utilizarea datelor reale cu caracter personal va fi limitată și controlată. Furnizorul va propune mecanisme de mascare, pseudonimizare sau utilizare a datelor sintetice, în funcție de scopul mediului și de testele necesare. Datele reale vor fi utilizate în medii non-producție numai dacă este justificat, aprobat și protejat prin acces limitat, jurnalizare și retenție controlată.

Mascarea datelor va ține cont de necesitățile de testare. Unele teste au nevoie de date realiste ca distribuție, coduri, perioade și combinații funcționale, dar nu au nevoie de identitatea reală a persoanelor. Prin separarea realismului funcțional de identitatea reală, sistemul poate fi testat corect fără expunerea inutilă a datelor personale.

Verificare independentă înainte de go-live

Înainte de go-live, Furnizorul va include verificări de securitate asupra aplicației, API-urilor, configurației, autentificării, autorizării, managementului sesiunilor, exporturilor, auditului și protecției datelor. Testarea va acoperi vulnerabilitățile cunoscute, cazuri negative, acces nepermis, escaladare de privilegii, manipulare parametri, control insuficient în backend și expunere accidentală de date.

Pentru un nivel suplimentar de încredere, proiectul poate include testare VAPT independentă sau terță parte înainte de go-live, conform deciziei CNAS și condițiilor contractuale. Raportul de testare va include vulnerabilități identificate, severitate, dovadă, recomandare, responsabil, termen de remediere și retestare. Defectele critice sau înalte cu impact asupra securității nu vor fi tratate ca observații minore înainte de lansarea în producție.

Furnizorul va susține remedierea vulnerabilităților identificate și va furniza evidențe de retestare. Această abordare transformă securitatea din declarație de conformitate în verificare efectivă înainte de exploatarea reală a sistemului.

Detecția anomaliilor și protecția împotriva abuzului intern

Sistemul va permite detectarea comportamentelor neobișnuite care pot indica eroare, abuz sau compromis al unui cont valid. Protecția nu se va limita la blocarea accesului neautorizat; ea va include monitorizarea operațiunilor legitime executate în volum, context sau frecvență neobișnuită.

Evenimentele care pot genera alertă includ exporturi masive, accesarea unui număr neobișnuit de dosare într-un interval scurt, consultarea datelor în afara scope-ului obișnuit, login-uri în intervale neobișnuite, multe încercări eșuate, modificări repetate ale rolurilor, schimbări masive de configurări, operațiuni privilegiate în afara ferestrei aprobate sau generarea repetată a rapoartelor sensibile.

Detecția anomaliilor va fi implementată pragmatic, prin reguli, praguri, rapoarte de monitorizare și alerte operaționale. Scopul nu este introducerea unui mecanism opac, ci oferirea de vizibilitate asupra comportamentelor care merită revizuite de CNAS sau de echipa de securitate. Pragurile și alertele vor fi ajustate în faza de stabilizare, pe baza utilizării reale a sistemului.

Comportament urmărit	De ce contează	Răspuns operațional
Export masiv sau repetat	risc de scurgere de date personale	alertă, audit extins, justificare, revizuire acces
Acces neobișnuit la dosare	posibil abuz intern sau cont compromis	raport anomalie, corelare cu rol/scope
Operațiune administrativă sensibilă	modificare roluri, șabloane, configurări critice	audit, notificare, review post-acțiune

Comportament urmărit	De ce contează	Răspuns operațional
Login-uri sau încercări eșuate repetate	risc credential stuffing sau utilizare incorectă	blocare/alertare conform politicii
Intervenție DB sau script producție	risc de ocolire flux aplicație	DB audit, tichet, raport intervenție

Cultura securității și instruirea împotriva erorii umane

Furnizorul va trata securitatea ca proces operațional, nu doar ca proprietate a codului. Pentru utilizatorii CNAS, instruirea va include comportamente de lucru sigur: protejarea sesiunii, utilizarea corectă a drepturilor, atenția la exporturi, verificarea destinatarilor, raportarea incidentelor, evitarea partajării conturilor și recunoașterea tentativelor de social engineering.

Pentru administratori și suport, instruirea va include utilizarea conturilor privilegiate, procedura de intervenție în producție, citirea auditului, tratarea incidentelor, managementul secretelor, restaurare, escaladare și documentarea acțiunilor. Un sistem securizat poate fi compromis prin proceduri greșite; de aceea, handover-ul de securitate va include atât mecanisme tehnice, cât și reguli de operare.

Această abordare oferă CNAS un sistem securizat și un mod de operare securizat. Securitatea livrată nu se oprește la autentificare, criptare sau scanare de vulnerabilități; ea include responsabilități clare, audit, instruire, proceduri și capacitatea de a detecta și trata abateri în exploatarea zilnică.

10.15 Rezultatul livrat pentru CNAS

Prin această abordare, CNAS primește un sistem în care securitatea nu se bazează pe încredere informală, rețea internă sau disciplină manuală. Accesul este decis pe identitate, rol, context, obiect și acțiune. Datele personale sunt afișate, exportate, jurnalizate și reutilizate numai conform regulilor definite. Integrările sunt controlate prin gateway. Logurile tehnice și auditul business sunt separate, dar corelabile. Modificările critice trec prin fluxuri, nu prin intervenții directe în date.

Prin jurnalizare, audit și corelarea evenimentelor, CNAS poate demonstra cine a accesat date, cine a modificat un obiect, ce raport a fost generat, ce document a fost descărcat, ce integrare a fost apelată, ce configurare a fost activată și ce rezultat a produs o procedură automată. Această trasabilitate este esențială pentru protecția datelor personale, audit intern, suport, investigație, acceptanță și exploatare pe termen lung.

Prezentul capitol stabilește poziția ofertei: securitatea SI „Protecția Socială” va fi livrată ca sistem de controale aplicate în arhitectură, funcționalitate, date, integrare, raportare, audit, CI/CD, operare și suport. Matricea de conformitate va demonstra acoperirea cerințelor SEC, iar SRS/SDD va detalia politicile, rolurile, componentele, fluxurile, regulile de audit, datele protejate, testele și evidențele finale de acceptanță.

11. Migrare, phase-in, punere în producție și stabilizare

11.1 Rolul capitolului si legatura cu metodologia generala

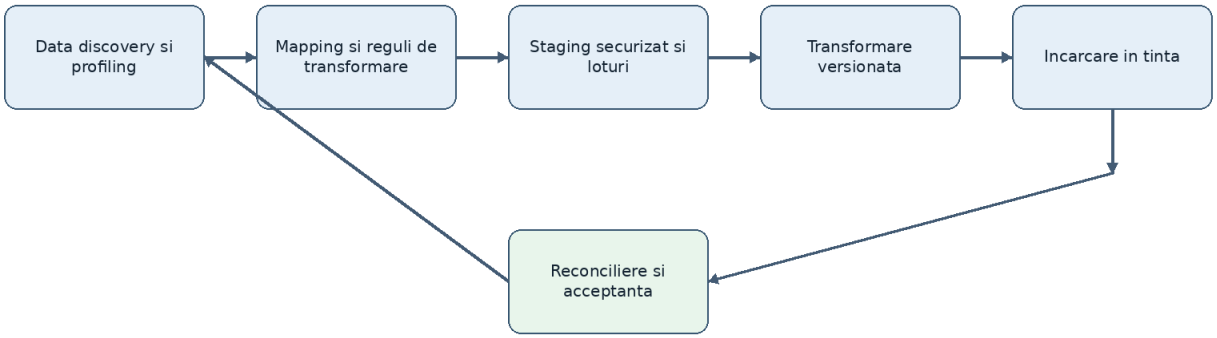
Acest capitol operaționalizează metodologia de livrare pentru una dintre cele mai sensibile părți ale proiectului: transferul controlat de la sistemele si datele existente către noul SI „Protecția Socială”, punerea in producție si stabilizarea utilizării reale. Metodologia generala stabilește principiile - Waterfall guvernat pe milestone-uri, incrementuri lunare, Delivery Assurance, Functional Backbone, Shared Services, Data & Migration Assurance si readiness gates. Capitolul de fata transforma aceste principii in mecanisme concrete de migrare, phase-in, cutover, rollback/forward-fix si stabilizare.

Furnizorul va trata migrarea si go-live-ul ca tranziție instituționala, nu ca activitate tehnica finala. Sistemul nou va prelua date istorice, nomenclatoare, contribuții, conturi individuale, cereri, dosare, decizii, drepturi, plăti, documente, raportare si integrări. Fiecare dintre aceste zone are efect funcțional si instituțional; de aceea intrarea in producție nu se va baza pe faptul ca aplicația este instalata, ci pe evidenta ca datele, fluxurile, utilizatorii, integrațiile, rapoartele si suportul sunt pregătite.

Capitolul este separat de metodologia generala deoarece riscurile sunt diferite. Metodologia raspunde la întrebarea cum se guvernează si livrează proiectul. Acest capitol răspunde la întrebarea cum se trece efectiv din regimul actual in regimul operațional nou, fără pierderea controlului asupra datelor, fara doua surse oficiale concurente, fără lansare prematura si fără descoperirea problemelor majore in primele zile de exploatare.

Zona	Ce preia capitolul din metodologie	Cum se concretizeaza in migrare/go-live
Delivery Assurance	Progres pe evidente, nu pe declarații.	Rapoarte de migrare, reconciliere, testare, rehearsal, readiness si stabilizare.
Functional Backbone	Cerere, dosar, decizie, drept, plata, document, audit.	Migrarea si cutover-ul se verifica pe lanțuri operaționale, nu doar pe tabele.
Shared Services / Artefacts	Roluri, workflow, documente, notificări, audit, raportare.	Foundation readiness inainte de migrare si pilot; nu se lansează domenii fără mecanisme comune pregătite.
Data & Migration Assurance	Date profilate, mapping, teste de calitate, reconciliere.	Migration factory, sandbox, error bucket, valori de control, sign-off CNAS.
Readiness gates	Trecere pe baza de criterii si evidenta.	Foundation readiness, migration readiness, pilot readiness, go-live readiness, stabilization exit.

In acest capitol, termenul „phase-in” inseamna trecerea controlata catre noul sistem pe domenii, capabilitati, grupuri de utilizatori sau perioade, atunci cand aceasta separare este sigura.



Daca apar erori: error bucket -> decizie CNAS -> corectie mapping/date -> rerun controlat
Migrarea finala este executia controlata a unui mecanism demonstrat anterior, nu prima rulare completa.

11.2 Obiective operationale si cerinte acoperite

Furnizorul va acoperi prin acest capitol cerintele privind migrarea si popularea initiala a datelor, strategia de punere in productie, coordonarea lansarii cu CNAS, participarea Furnizorului la etapele de go-live, pregatirea rollback-ului si stabilizarea operațională dupa lansare. Abordarea propusa nu reduce aceste cerinte la o lista de activitati, ci le leaga de mecanisme verificabile si de livrabile care pot fi examinate de CNAS.

Pentru fiecare zona sensibila se vor defini criterii de trecere si evidenta: migration plan, mapping, instrumentar software de migrare, rapoarte de reconciliere, registru de exceptii, production rehearsal, plan de punere in productie, go/no-go checklist, rollback/forward-fix plan, runbook operational, suport intensificat si raport de stabilizare.

Obiectiv	Risc controlat	Livrabil / evidenta
Migrare si populare initiala	Import unic, nereproductibil, cu erori ascunse.	Plan migrare, mapping, instrumentar, loguri, rapoarte de reconciliere, error bucket.
Reconciliere si calitate date	Date migrate numeric, dar inutilizabile functional.	Valori de control, comparatii sursa-tinta, esantioane functionale, exceptii clasificate.
Phase-in si co-existenta	Doua surse oficiale, inconsistente intre domenii.	Plan phase-in, matrice sursa-oficiala, ferestre de sincronizare/freeze, decizii CNAS.
Production rehearsal	Echipa invata go-live-ul in ziua lansarii.	Raport rehearsal, timpi masurati, lista probleme, smoke tests, rollback testat.
Go-live readiness	Lansare prematura doar pentru ca deployment-ul a reusit.	Checklist readiness, release candidate, UAT, date, integrări, training, suport, backup/restore.
Stabilizare	Sistem lansat, dar fara suport operational real.	Plan stabilizare, command center, defect log, rapoarte zilnice/saptamanale, PV acceptanta finala.

11.3 Migration factory

Furnizorul va organiza migrarea ca migration factory: un mecanism repetabil, versionat si reluabil de extragere, validare, transformare, incarcare, reconciliere si acceptare a datelor. Aceasta abordare protejeaza proiectul de scenariul in care migrarea este tratata ca operatie finala, executata o singura data, cu loguri tehnice greu de interpretat si cu exceptii descoperite in apropierea go-live-ului.

Migration factory va avea trei proprietati obligatorii. Prima este trasabilitatea: fiecare set de date migrat va avea sursa, mapping, transformari, reguli aplicate, lot, timp de executie, rezultat si exceptii. A doua este idempotenta: reluarea unui lot nu va produce dublari sau rezultate contradictorii. A treia este reconcilierea:

migrarea nu se considera reusita doar pentru ca scriptul a rulat, ci pentru ca rezultatele sunt comparate cu sursa si validate pe criterii tehnice si functionale.

Instrumentarul de migrare va fi operat in infrastructura controlata de CNAS/MCloud, conform regulilor de securitate si protectie a datelor. Fisierele temporare, logurile, rapoartele de eroare, staging-ul si rezultatele de reconciliere vor ramane in perimetrul autorizat.

Etapa migration factory	Ce face Furnizorul	Ce verifica / decide CNAS
Data discovery si profiling	Inventariaza surse, tabele, volume, chei, calitate, duplicate, lipsuri si dependente.	Confirma sursele relevante, prioritatile si zonele care necesita verificare functionala.
Mapping si reguli	Defineste corespondenta sursa-tinta, transformari, normalizari, reguli de completare si validare.	Aproba interpretarile functionale si regulile care afecteaza sensul datelor.
Staging si loturi	Incarca date brute in staging securizat, cu batch_id, hash, sursa, timestamp, stare si erori.	Verifica vizibilitatea pe loturi si modul de tratare a exceptiilor.
Transformare versionata	Aplica reguli versionate, teste de calitate si control al integritatii referentiale.	Valideaza cazurile unde transformarea implica decizie business.
Load in tinta	Incarca date in modelul nou, cu idempotenta, log si stare de executie.	Verifica utilizarea datelor in fluxuri reale si scenarii UAT.
Reconciliere si rerun	Produce rapoarte sursa-tinta, valori de control, error bucket si rerun controlat.	Accepta rezultatul, cere corectii sau aproba exceptii documentate.

Procesele și scenariile din anexele funcționale vor fi utilizate și pentru delimitarea scope-ului de migrare și validare a datelor. Migrarea nu va urmări doar transferul tehnic al tabelelor istorice, ci capacitatea noului sistem de a executa procesele descrise în caiet pe datele migrate: plătitori, contribuții, persoane asigurate, cont individual, drepturi, decizii, plăți, registre, rapoarte și documente.

Pentru fiecare domeniu de migrare, Furnizorul va lega obiectele migrate de procesele care le consumă. De exemplu, datele despre persoana asigurată și contul individual trebuie validate nu doar ca înregistrări existente, ci ca date utilizabile pentru stabilirea drepturilor, generarea extraselor, calcul, raportare și audit. Datele despre plăți trebuie validate nu doar ca sume, ci ca elemente care susțin conturi de plată, comenzi, rețineri, restituiri, rapoarte și reconciliere.

Această abordare permite CNAS să accepte migrarea pe criterii funcționale, nu doar pe număr de rânduri. Rapoartele de reconciliere vor include valori de control, excepții, diferențe, obiecte fără corespondent, duplicate, date lipsă și impact asupra proceselor din anexă. Cazurile care necesită decizie funcțională CNAS vor fi înregistrate în error bucket și tratate înainte de readiness-ul pentru UAT sau go-live.

11.4 Domenii de date migrate si reguli de prioritate

Migrarea va fi planificata pe domenii de date si pe dependente functionale. Furnizorul nu va trata toate tabelele istorice ca avand acelasi rol si aceeasi urgenta. Datele care sustin identificarea persoanei, platile, drepturile, contul individual, dosarele si deciziile vor avea prioritate in proiectarea mapping-ului, validarea functionala si reconciliere. Datele necesare pentru raportare istorica, audit sau consultare vor fi tratate conform regulilor stabilite in SRS/SDD si planul de migrare.

Pentru fiecare domeniu de date se va stabili daca migrarea produce date operationale active, date istorice consultabile, date necesare pentru calcul, date necesare pentru raportare, documente atasate, configurari sau date de referinta. Aceasta clasificare este importanta deoarece nu toate datele au acelasi comportament la cutover: unele trebuie sa fie active imediat, altele pot fi consultabile, iar altele pot fi migrate in loturi succesive fara sa blocheze go-live-ul unui domeniu.

Domeniu de date	Rol in noul sistem	Regula de migrare / validare
Nomenclatoare, clasificatoare si configurari	Baza comuna pentru fluxuri, rapoarte, documente si validari.	Se valideaza devreme; fara ele nu se poate confirma foundation readiness.
Persoane, platori si relatii relevante	Identificare, cautare, asociere cu contributii, dosare si drepturi.	Se migreaza cu verificare de duplicate, chei, surse si calitate identificatori.
Contributii, stagiu, cont individual	Baza pentru drepturi, pensii, calcul si verificari istorice.	Se reconciliaza pe perioade, sume, surse, legaturi persoana-plator si esantioane functionale.
Cereri, dosare, decizii, drepturi	Backbone operational pentru prestatii, pensii, modificari si audit.	Se verifica pe lanturi: cerere-dosar-decizie-drept-document-audit.
Plati, retineri, restituiri, solduri	Continuitate financiara si raportare institutionala.	Se reconciliaza pe sume de control, perioade, beneficiar, tip drept si stari.
Documente si atasamente	Evidente oficiale si suport pentru dosare/decizii.	Metadate in DB, fisiere in storage, checksum, legare la obiecte si audit acces.
Date de raportare istorica	Rapoarte statistice, profile, contingente si trenduri.	Se stabileste daca sunt migrate in marts/snapshots sau doar in istoricul consultabil.

11.5 Data cleansing, sandbox de migrare si decizii asupra datelor murdare

Furnizorul va include in procesul de migrare un sandbox de migrare: un cadru tehnic in care datele pot fi rulate repetat inainte de go-live, fara efect asupra productiei. Sandbox-ul permite descoperirea timpurie a problemelor de calitate, testarea mapping-ului, estimarea duratei de executie, masurarea ratei de exceptii si verificarea efectului datelor migrate in fluxuri reale.

Data cleansing nu va fi tratat ca pas abstractat de curatare a tuturor datelor istorice. Furnizorul va ajuta CNAS sa identifice, clasifice și decidă asupra datelor problematice. Unele probleme pot fi corectate automat prin reguli aprobate; altele necesita decizie functionala; altele pot fi migrate ca exceptii acceptate, daca nu blocheaza fluxurile critice. Diferenta dintre eroare tehnica, eroare de date sursa si caz functional exceptional va fi vizibila in error bucket si rapoartele de reconciliere.

Pentru a evita interpretari diferite, fiecare regula de curatare va avea descriere, domeniu, conditie de aplicare, efect asupra datelor, risc, evidenta si decizie CNAS unde este necesar. Curatarea datelor nu va ascunde informatia istorica si nu va modifica arbitrar sensul institutional al datelor.

Tip problema date	Tratament propus	Decizie / evidenta
Camp obligatoriu lipsa	Regula de completare doar daca exista sursa sigura; altfel exceptie.	Error bucket, decizie CNAS sau marcaj de date incomplete.
Duplicate	Detectie prin chei, reguli de potrivire si verificare functionala.	Lista duplicate, regula de consolidare, aprobare CNAS.
Cod vechi / nomenclator expirat	Mapping catre nomenclator nou sau pastrare istorica declarata.	Tabel mapping, raport valori neacoperite.
Conflict de istoric	Versiuni, perioade valid_from/valid_to, conflict report.	Decizie asupra sursei de adevar si tratament functional.
Sume / solduri care nu bat	Reconciliere pe valori de control si investigare pe esantioane.	Raport diferenta, justificare, corectie sau exceptie acceptata.
Document lipsa sau fisier invalid	Migrare metadata, marcaj fisier lipsa, verificare checksum pentru fisiere existente.	Raport documente, lista cazuri, decizie CNAS.

11.6 Reconciliere, cockpit de calitate si acceptanta migrarii

Furnizorul va livra mecanisme de reconciliere care permit CNAS sa vada ce s-a migrat, ce nu s-a migrat, ce a fost transformat, unde exista diferente si ce exceptii necesita decizie. Reconcilierea va combina controale tehnice si functionale. Controalele tehnice verifica volume, chei, integritate, formate, erori si durata de executie. Controalele functionale verifica sume, drepturi, conturi, decizii, plati, rapoarte, documente si cazuri reprezentative.

Data quality and reconciliation cockpit va centraliza indicatori de rulare: numar inregistrari sursa, numar inregistrari staging, numar inregistrari incarcate, respingeri, duplicate, erori de mapping, integritate referentiala, sume de control, diferente fata de sursa, procent exceptii si cazuri care necesita decizie CNAS. Acest cockpit poate fi implementat ca dashboard operational, raport de rulare sau combinatie de rapoarte si tabele de control, in functie de arhitectura aprobata.

Acceptanta migrarii se va baza pe pachet de evidenta: mapping aprobat, rulare executata, reconciliere, lista exceptii, decizii asupra exceptiilor, rerun acolo unde este cazul si confirmarea ca datele pot fi utilizate in fluxurile noului sistem.

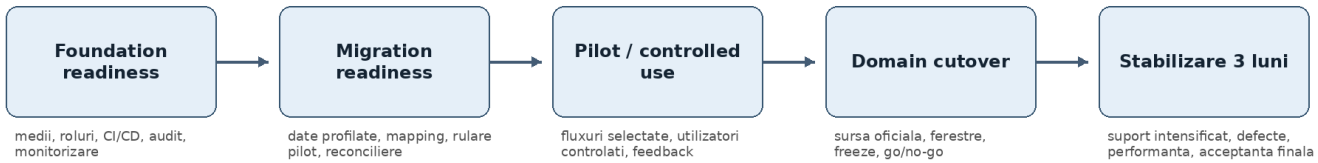
Indicator de reconciliere	Intrebare la care raspunde	Exemplu de evidenta
Volum sursa vs tinta	Au fost preluate toate obiectele asteptate?	count sursa, count staging, count tinta, diferente.
Integritate referentiala	Exista obiecte orfane sau relatii rupte?	persoane fara dosare, decizii fara dosar, plati fara drept.
Valori de control	Sumele si agregatele bat cu sursa?	total contributii, total plati, solduri, total beneficiari.
Calitate nomenclatoare	Codurile vechi sunt mapate complet?	lista coduri fara corespondent, regula de mapping.
Esantion functional	Cazurile reale arata corect in noul sistem?	cazuri alese cu CNAS, rezultate verificare, observatii.
Exceptii acceptate	Ce nu se corecteaza automat si de ce?	error bucket, decizie, justificare, impact.

11.7 Strategia de phase-in si co-existenta controlata

Strategia propusa este phase-in controlat, nu big-bang nejustificat si nu functionare nedefinita in paralel. Furnizorul va propune impreuna cu CNAS gruparea domeniilor in valuri de lansare, pe baza dependentelor reale: date, fluxuri, integrări, rapoarte, utilizatori, plati si suport. Unele capabilitati pot fi pilotate sau lansate pe grupuri limitate. Altele trebuie comutate impreuna, deoarece separarea ar crea inconsistente intre cont individual, drept, decizie, plata si raportare.

In co-existenta controlata, se va defini explicit sursa oficiala pentru fiecare domeniu, subdomeniu, perioada si tip de informatie. Noul sistem poate fi folosit initial pentru pilot, validare comparativa, fluxuri izolate sau raportare, dar nu va exista doua surse oficiale active pentru acelasi obiect si aceeasi perioada. Orice sincronizare temporara, freeze, delta migration sau blocare de modificari va fi documentata in planul de phase-in si cutover.

Phase-in-ul va fi legat de readiness gates. Un domeniu nu trece la noul sistem doar pentru ca modulul sau este dezvoltat. El trece numai cand exista date migrate si reconciliate, fluxuri testate, utilizatori instruiti, integrări confirmate, rapoarte critice validate, suport pregatit si decizie CNAS de go/no-go.



Val phase-in	Continut posibil	Criteriu de intrare	Criteriu de extindere
Foundation	Identitate, roluri, nomenclatoare, workflow minim, audit, CI/CD, monitorizare.	Mediile sunt pregatite; componentele comune ruleaza.	Shared services sunt reutilizabile in primele fluxuri.
Pilot controlat	Flux selectat cu utilizatori si date controlate.	Date relevante migrate; scenarii definite; suport pregatit.	Feedback tratat; defecte majore inchise; utilizatorii confirma utilitatea.
Domeniu operational	Contributii/cont individual, pensii, beneficii sau alt bloc functional.	Cutover plan, date reconciliate, UAT, rapoarte critice, training.	Stabilitate in exploatare, defecte in prag acceptat, monitorizare activa.
Extindere pe teritoriu/utilizatori	Valuri pe CTAS, roluri, servicii, volume.	Primele grupuri sunt stabile; runbook si suport functioneaza.	Nu creste necontrolat numarul incidentelor; performanță ramane in prag.

11.8 Sursa oficiala, freeze, delta si cutover pe date

Pentru fiecare val de lansare, Furnizorul va propune o matrice de sursa oficiala. Matricea va arata ce sistem este sursa pentru date curente, istoric, raportare, plati si documente intr-o anumita perioada. Aceasta matrice este necesara deoarece riscul major al phase-in-ului este aparitia unei duble adevaruri: operatorii modifica intr-un sistem, rapoartele citesc din altul, iar platile se bazeaza pe o stare intermediara.

Inainte de cutover, se poate aplica freeze selectiv. Freeze-ul nu inseamna oprirea globala a institutiei, ci blocarea sau limitarea controlata a modificarilor pe datele si domeniile care intra in cutover. Pentru modificarile operate intre ultima migrare completa si momentul lansarii, Furnizorul va executa delta migration: extragerea, validarea si incarcarea modificarilor finale. Delta-ul va avea propriile loguri, valori de control si reconciliere.

Dupa cutover, datele din domeniul lansat vor fi modificate in noul sistem. Sistemul vechi poate ramane sursa de consultare sau verificare comparativa pentru o perioada limitata, daca CNAS decide acest lucru, dar nu va ramane sursa operațională pentru acelasi domeniu fara o regula explicita.

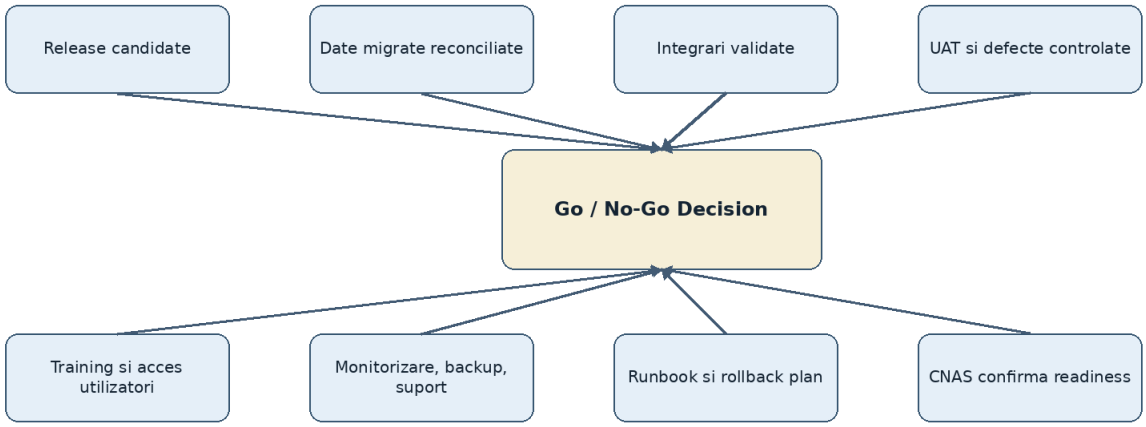
Element	Regula propusa	Evidenta
Sursa oficiala	Un singur sistem este sursa operațională pentru fiecare domeniu/perioada.	Matrice sursa-oficiala, decizie CNAS.
Freeze selectiv	Se aplica numai unde modificarea in timpul cutover-ului poate crea inconsistenta.	Lista obiecte/domenii blocate, perioada, responsabili.
Delta migration	Preia modificarile dintre ultima rulare completa si momentul cutover.	Log delta, count, valori control, erori, reconciliere.
Read-only legacy	Sistemul vechi poate fi pastrat temporar pentru consultare/comparatie.	Regula de acces, durata, obiective, audit.
Corectii post-cutover	Se trateaza in sistemul nou sau prin procedura controlata stabilita.	Tichet, decizie, script/release, audit.

11.9 Production rehearsal si go-live readiness

Furnizorul va executa production rehearsal pe un mediu cat mai apropiat de productie. Rehearsal-ul nu este demonstratie de interfata, ci repetitie operațională a lansarii: deployment, configurari, migrare/delta, verificari de integrare, smoke tests, acces utilizatori, rapoarte critice, backup/restore, monitorizare, rollback/forward-fix si functionarea suportului.

Scopul este ca ziua lansarii sa nu fie prima data cand echipa executa pasii reali. Rehearsal-ul va masura durata operatiunilor, va identifica punctele manuale, va confirma runbook-ul, va verifica ordinea dependentelor si va arata daca exista resurse insuficiente, scripturi instabile, migrari lente sau integrări nesigure. Problemele identificate in rehearsal vor fi tratate inainte de decizia de go-live.

Go-live readiness va fi un gate formal, cu participarea CNAS. Furnizorul va pregati pachetul de evidenta, iar CNAS va confirma readiness-ul functional si operational. Decizia de lansare va fi documentata ca go/no-go, nu presupusa automat din finalizarea dezvoltarii.



Decizia de lansare nu rezulta din instalare tehnica; ea rezulta din pachetul de evidenta si confirmarea CNAS asupra readiness-ului functional si operational.

Gate readiness	Criterii minime	Evidenta
Release candidate	Versiune identificata, build reproductibil, release notes, artefacte versionate.	Release package, CI/CD evidence.
Functional/UAT	Scenarii critice executate, defecte critice/blocante inchise, prag defecte acceptat.	UAT report, defect log, sign-off.
Data/Migration	Date migrate, reconciliate, exceptii tratate sau acceptate.	Migration report, reconciliation report, error bucket.
Integration	Servicii externe verificate, timeout/retry/circuit breaker, scenarii negative.	Integration test report, logs, dashboard.
Performance	Teste pe scenarii relevante, batch-uri, rapoarte, concurenta.	Performance report, recomandari operare.
Security	Acces, roluri, audit, scanari, secrete, VAPT daca este aplicabil.	Security readiness evidence.
Operational	Training, ghiduri, runbook, service desk, monitorizare, backup/restore.	Runbook, training evidence, support readiness.
CNAS go/no-go	CNAS confirma ca sistemul poate intra in exploatare pentru domeniul definit.	Proces-verbal / decizie go-live.

Hypercare dedicat în primele săptămâni după Go-Live

Furnizorul va activa, imediat după punerea în producție, un regim dedicat de hypercare pentru primele două săptămâni de exploatare operațională. Această perioadă nu va fi tratată ca suport obișnuit la distanță, ci ca mecanism intensificat de asistență, triere, intervenție și stabilizare, în care echipa Furnizorului va urmări direct comportamentul sistemului în condiții reale de utilizare CNAS.

Hypercare-ul va include prezență organizată în sediul central CNAS și, în funcție de planul de go-live aprobat, suport direct pentru cele mai mari sau mai critice CTAS-uri stabilite împreună cu CNAS. Prezența poate combina asistență fizică, command center centralizat, suport la distanță și canale rapide de escaladare, astfel încât problemele apărute în primele zile să fie clasificate, atribuite și tratate fără blocaje informale.

În perioada de hypercare, participarea coordonată a rolurilor necesare pentru decizie rapidă include: project manager, arhitect de soluție, analist business, responsabil QA, specialist migrare/date, specialist integrare, responsabil deployment/operare și suport aplicație. Scopul nu este doar remedierea incidentelor, ci și reducerea incertitudinii utilizatorilor, clarificarea modului corect de lucru, colectarea observațiilor operaționale, separarea defectelor de solicitările de schimbare și stabilizarea comportamentului sistemului în producție.

Pentru CNAS, hypercare-ul oferă un mecanism de siguranță în tranziția de la UAT la utilizarea reală. Utilizatorii vor avea posibilitatea să raporteze rapid dificultăți, operatorii din teritoriu vor primi ghidare operațională, iar conducerea proiectului va avea vizibilitate zilnică asupra incidentelor, observațiilor, workaround-urilor, remedierilor și deciziilor necesare. Furnizorul va menține un registru distinct de hypercare, conectat la registrul general de defecte, suport și schimbări.

Model de organizare a hypercare-ului

Componentă	Ce livrează Furnizorul	Rolul CNAS	Evidență produsă
Command center	coordonează incidentele, alocă responsabili, urmărește statusul zilnic	asigură puncte de contact decizionale și acces la utilizatori cheie	registru hypercare, raport zilnic, action log
Prezență centrală CNAS	arhitect/BA/suport pentru întrebări funcționale și tehnice critice	validează prioritatea incidentelor și impactul operațional	minute scurte, decizii, observații clasificate
Suport CTAS prioritare	asistență directă pentru fluxurile folosite intens la nivel teritorial	desemnează CTAS-urile prioritare și utilizatorii de contact	feedback local, listă probleme recurente, ghidări necesare
Triage incident/defect/schimbare	separă defectele de clarificări, training gaps și schimbări de scope	confirmă impactul și prioritatea acolo unde este necesar	defect log, change log, knowledge base updates
Remediere și comunicare	pregătește hotfix, workaround sau plan de remediere, după caz	confirmă acceptabilitatea workaround-urilor operaționale	release notes, retest evidence, comunicări operaționale

În primele două săptămâni, raportarea de stabilizare va avea cadență sporită. Pentru problemele de Severitate 1 și Severitate 2, command center-ul asigură triere imediată, desemnarea unui responsabil, comunicare periodică asupra statusului și evidență de retestare după remediere. Problemele de severitate mai redusă vor fi clasificate, prioritizate și tratate în registrul de stabilizare, fără a bloca fluxurile critice.

Fluxul de hypercare post-Go-Live

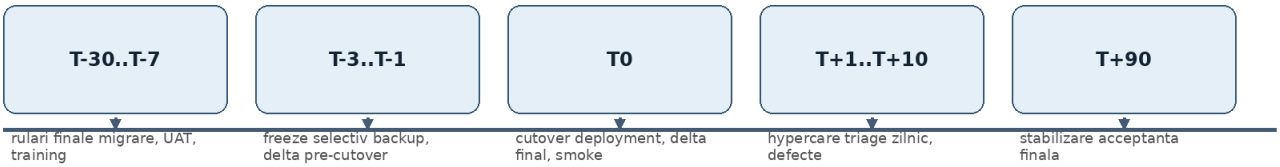
Go-Live	Hypercare 2 săptămâni	Triage zilnic	Remedieri / workaround	Stabilizare monitorizată
sistem în producție	echipă dedicată + command center	defect / clarificare / schimbare	hotfix, ghidare, retestare	trend defecte + exit criteria

11.10 Plan de punere in productie, cutover, rollback si forward-fix

Planul de punere in producție va fi livrabil formal si va fi coordonat cu CNAS. El va include calendar, ferestre de lucru, lista componentelor, versiuni, responsabilitati, contacte, pași de deployment, pași de migrare/delta, verificări, comunicare către utilizatori, smoke tests, criterii go/no-go, plan de rollback sau forward-fix si procedura de comunicare in caz de incident.

Rollback-ul va fi tratat realist. Pentru componente stateless sau configurări, rollback-ul tehnic la versiunea anterioara poate fi fezabil. Pentru date operaționale modificate după cutover, revenirea simpla poate fi riscanta sau imposibila fara pierderea consistentei. In aceste cazuri, planul va defini forward-fix: corectie controlata in noul sistem, cu tichet, script/release, audit si reconciliere. Oferta nu promite rollback universal acolo unde natura datelor nu permite acest lucru; promite un mecanism documentat de recuperare, revenire sau corecție controlata.

Pentru procesele batch critice - calcul, plati, migrare, reporting layer, inchidere de perioada - Furnizorul va aplica idempotenta, checkpoint-uri si reluare controlata. Daca un proces se oprește la 80%, reluarea nu va dubla plăti, nu va crea decizii duplicate si nu va altera datele deja confirmate.



Scenariu	Tratament propus	Evidenta
Deployment nereusit inainte de date operationale	Rollback tehnic la versiunea anterioara sau amanare go-live.	Log deployment, decizie no-go, plan remediere.
Migrare/delta cu erori peste prag	Blocare go-live pentru domeniul afectat, corectie mapping/date, rerun.	Error bucket, raport reconciliere, decizie CNAS.
Defect critic descoperit dupa cutover	Triage imediat, workaround/rollback daca sigur, altfel forward-fix controlat.	Incident ticket, hotfix release, audit.
Integrare externa indisponibila	Functionare degradată, retry, circuit breaker, comunicare catre suport/utilizatori.	Integration dashboard, incident log.
Batch intrerupt partial	Reluare din checkpoint/idempotent, fara duplicari.	Job log, checkpoint, raport rezultat.
Necesitate revenire pe sistem vechi	Numai daca domeniul si datele permit, conform planului aprobat.	Rollback decision, verificare consistenta, comunicare.

11.11 Stabilizare operațională si command center post-go-live

După lansare, proiectul intră într-o perioadă de stabilizare activă. Stabilizarea nu este perioada în care se așteaptă pasiv apariția incidentelor, ci regim intensificat de observare, suport, triage, remediere, ajustare si

măsurare a comportamentului sistemului in exploatare reală. Pentru SI „Protecția Socială”, stabilizarea va acoperi utilizatori, fluxuri, date, integrări, rapoarte, batch-uri, performanță, securitate si suport operațional.

In primele zile dupa go-live, Furnizorul va opera un command center/hypercare impreuna cu CNAS. Acesta va urmări incidentele, intrebarile utilizatorilor, defectele, performanță, erorile de integrare, batch-urile, rapoartele critice si logurile. Comunicarea va fi structurata: puncte zilnice de triage, raport de situatie, responsabil pentru fiecare problema, termen tinta, severitate, workaround si rezultat de retestare.

Pe durata celor 3 luni de stabilizare, ritmul de raportare poate scadea gradual in functie de stabilitatea sistemului, dar registrele de incidente, defecte si solicitari raman active. La finalul stabilizarii, Furnizorul va pregati raportul de stabilizare si pachetul de acceptanta finala.

Perioada	Activitate Furnizor	Participare CNAS	Rezultat
Primele zile	Command center, monitorizare continua, triage zilnic, suport rapid.	Raporteaza probleme, confirma impact operational, prioritizeaza fluxuri.	Incident log, daily status, remedieri rapide.
Primele saptamani	Analiza trenduri, defecte recurente, performanță, batch-uri, integrări.	Valideaza workaround-uri, accepta prioritati, verifica fluxuri critice.	Raport saptamanal, backlog stabilizare.
Luna 2-3	Stabilizare ritm normal, optimizari, completare documentatie, handover suport.	Confirma ca sistemul acopera exploatarea curenta.	Raport stabilizare, suport readiness.
Exit stabilizare	Pregateste pachet acceptanta finala si transfer catre suport/garantie.	Semneaza acceptanta finala daca criteriile sunt indeplinite.	PV acceptanta finala, transition report.

Ieșirea din faza de stabilizare și pregătirea procesului-verbal de acceptanță finală nu vor fi tratate ca efect automat al împlinirii perioadei calendaristice de stabilizare. Perioada de stabilizare oferă cadrul de monitorizare, suport și remediere, dar exit-ul operațional trebuie confirmat prin criterii de stabilitate, defecte controlate, evidențe de suport, documentație actualizată și capacitate de operare.

Furnizorul va propune ca Stabilization Exit să fie condiționat de îndeplinirea unui criteriu minim de stabilitate operațională: zero defecte deschise de Severitate 1 și Severitate 2 în ultimele 14 zile consecutive de monitorizare. Dacă în această perioadă apare un defect nou de Severitate 1 sau Severitate 2, fereastra de stabilitate se reia după remedierea, retestarea și confirmarea închiderii defectului. Această regulă protejează CNAS de acceptarea finală a unui sistem instabil și confirmă că Furnizorul nu transferă în garanție defecte critice nerezolvate.

Criteriul de 14 zile nu elimină celelalte condiții de acceptanță. El se adaugă la pachetul de evidențe necesar pentru finalizarea stabilizării: defecte critice închise, workaround-uri acceptate explicit, documentație actualizată, runbook operațional, rapoarte de suport, confirmarea canalelor de service desk, evidențe de monitorizare și predarea către regimul de garanție/mentenanță. Defectele de severitate mai redusă pot rămâne într-un plan controlat de remediere numai dacă CNAS confirmă că nu blochează funcționarea operațională și nu afectează acceptanța finală.

Criterii propuse pentru Stabilization Exit

Criteriu	Condiție de exit	Ce livrează Furnizorul	Confirmare CNAS
Stabilitate defecte critice	zero defecte deschise S1/S2 în ultimele 14 zile consecutive	defect log, retest evidence, raport de stabilizare	confirmă că nu există blocaje critice operaționale

Criteriu	Condiție de exit	Ce livrează Furnizorul	Confirmare CNAS
Defecte non-critice	defectele S3/S4 sunt închise sau incluse în plan acceptat	plan de remediere, priorități, termene	aprobă că nu blochează acceptanța finală
Suport și operare	service desk activ, canale, SLA, escaladări și responsabilități confirmate	proceduri suport, registru solicitări, rapoarte	confirmă trecerea la regimul de suport/garanție
Documentație și runbook	documentația operațională și tehnică reflectă versiunea stabilizată	runbook, ghiduri, release notes, known issues	confirmă pachetul de predare operațională
Monitorizare	dashboarduri, alerte și loguri critice funcționale în exploatare	evidențe monitoring, alerte testate, rapoarte trend	confirmă vizibilitatea operațională minimă
Date, migrare și reconciliere	nu există excepții critice nerezolvate care afectează funcționarea	reconciliation report, error bucket status, decizii excepții	confirmă acceptabilitatea rezultatelor

Această abordare transformă stabilizarea într-o etapă de calitate operațională, nu într-o simplă perioadă de așteptare. Furnizorul va putea demonstra că sistemul funcționează stabil în utilizare reală, iar CNAS va putea semna acceptanța finală pe baza unor evidențe concrete, nu doar pe baza expirării termenului calendaristic.

11.12 Defecte, incidente si criterii de acceptanta in stabilizare

Defectele si incidentele din stabilizare vor fi gestionate prin registru unic, nu prin comunicare informala. Fiecare înregistrare va avea sursa, descriere, componenta, UC/flux afectat, severitate, impact, responsabil, termen, workaround, versiune de remediere, evidenta de retestare si decizie de închidere. Prioritizarea va tine cont de impact asupra plaților, datelor, securității, utilizatorilor, fluxurilor critice si raportarii.

Acceptanta finala după stabilizare se va baza pe criterii clare: perioada de stabilizare încheiata, defecte critice/blocante închise, defecte majore in pragul acceptat sau tratate conform procedurii, rapoarte critice funcționale, batch-uri critice executate, integrări stabile, suport preluat, documentație actualizata si sistem operabil conform scopului lansat.

Nu toate observațiile post-go-live sunt defecte. Furnizorul va separa defectul de clarificare, ajustare operațională si schimbare de scope. Defectele se corectează ca parte a obligațiilor de livrare; schimbările de scop se analizează prin mecanismul de change control.

Categorie	Descriere	Tratament
Critic / blocant	Flux esential indisponibil, risc asupra datelor/platii/securitatii, imposibilitate de lucru.	Escalare imediata, workaround sau remediere prioritara, go/no-go afectat.
Major	Functionalitate importanta afectata, dar exista workaround controlat.	Plan remediere, termen, retestare, monitorizare.
Minor	Defect cu impact redus, cosmetica, mesaj, usurinta de utilizare.	Backlog stabilizare, remediere planificata.
Solicitare schimbare	Functionalitate noua sau modificare fata de cerinta/design aprobat.	Impact analysis si change control.
Clarificare / suport	Intrebare de utilizare, asistenta operațională, procedura.	Raspuns suport, actualizare ghid daca este cazul.

11.13 Pachetul de evidenta pentru migrare, go-live si acceptanta finala

Furnizorul va preda către CNAS un pachet de evidenta care permite verificarea fiecărei decizii importante: migrare, readiness, go-live, stabilizare si acceptanta finala. Acest pachet protejează ambele părți. CNAS poate verifica pe ce baza accepta sistemul, iar Furnizorul poate demonstra ca a livrat conform metodei asumate.

Pachetul de evidenta nu va fi compus doar din documente descriptive. El va include rezultate măsurabile: rapoarte de migrare, rapoarte de reconciliere, loguri de execuție, rapoarte de testare, defect log, release notes, checklisturi readiness, rapoarte de performanță, rapoarte de securitate, scenarii UAT, runbook-uri, rapoarte de stabilizare si decizii CNAS.

Moment	Pachet de evidenta
Migration readiness	Plan migrare, mapping, instrumentar, profiling, rezultate pilot, error bucket, raport reconciliere.
Pilot / controlled use	Scenarii, utilizatori, date, feedback log, defecte, decizii, actualizari SRS/SDD.
Production rehearsal	Runbook executat, timpi, probleme, smoke tests, rollback/forward-fix testat, raport rehearsal.
Go-live readiness	Checklist, release candidate, UAT, date, integrări, securitate, performanță, training, suport, backup/restore.
Cutover	Jurnal executie, decizie go/no-go, rezultate smoke, comunicari, incident log initial.
Stabilizare	Rapoarte zilnice/saptamanale, defect log, performanță, incidente, remediere, feedback utilizatori.
Acceptanta finala	Raport stabilizare, criterii indeplinite, defecte ramase acceptate/planificate, PV final.

11.14 Rolul CNAS in migrare, phase-in si acceptanta

CNAS nu va fi tratata ca observator pasiv al migrării si go-live-ului. CNAS este autoritatea funcționala asupra datelor, regulilor, priorităților, excepțiilor si acceptantei. Furnizorul va livra instrumentele, rapoartele, recomandările si evidenta; CNAS va confirma sursele de date, va decide asupra excepțiilor, va valida fluxurile, va prioritiza domeniile, va confirma readiness-ul si va aproba intrarea in producție.

Pentru a evita blocajele, Furnizorul va pregăti materialele de decizie in forma operațională: problema, impact, opțiuni, recomandare, risc, termen si consecința asupra planului. CNAS va putea decide informat si va putea exercita controlul instituțional asupra tranziției.

Zona	Responsabilitate Furnizor	Ce decide / confirma CNAS
Surse si mapping	Inventar surse, mapping, reguli, impact.	Sursele relevante si interpretarile functionale.
Excepții date	Error bucket, clasificare, recomandare.	Corectie, acceptare, excludere sau tratament special.
Phase-in	Propunere valuri, dependente, riscuri.	Ordinea domeniilor, pilot, extindere, go/no-go.
Cutover	Plan, runbook, freeze, delta, rollback/forward-fix.	Fereastra, autorizare lansare, comunicare institutionala.
Stabilizare	Raport incidente, defecte, performanță, suport.	Prioritati, acceptarea workaround-urilor, acceptanta finala.

11.15 Rezultatul livrat catre CNAS

Prin aceasta abordare, CNAS primește nu doar un sistem instalat, ci o tranziție controlata către exploatare. Datele vor fi migrate prin mecanism repetabil, nu prin import unic; reconcilierea va fi vizibila; exceptiile vor fi clasificate; phase-in-ul va evita doua surse oficiale concurente; go-live-ul va fi precedat de rehearsal si readiness; iar stabilizarea va functiona ca perioada activa de control operational.

Rezultatul urmarit este ca SI „Protecția Socială” sa intre in productie pe baza de evidenta: date, functional, integrare, performanță, securitate, utilizatori, suport si continuitate. Furnizorul va livra mecanismele si documentatia necesare, iar CNAS va putea decide si accepta fiecare etapa pe baza unei imagini clare asupra riscurilor, exceptiilor si conditiilor de operare.

Aceasta disciplina reduce riscul cel mai mare al proiectelor de modernizare institutionala: un sistem tehnic finalizat, dar nepregatit pentru date reale, utilizatori reali, fluxuri reale si responsabilitati reale. Oferta propusa trateaza migrarea, lansarea si stabilizarea ca parte centrala a livrarii, nu ca activitati de final executate sub presiunea calendarului.

12. Testare, UAT și acceptanță pe evidențe

12.1 Rolul secțiunii

Furnizorul va trata testarea ca mecanism de demonstrare a conformității, nu ca activitate finală de corectare a defectelor. Pentru SI „Protecția Socială”, acceptanța nu poate fi fundamentată doar pe demonstrații de interfață sau pe afirmații generale de conformitate. Sistemul va fi verificat prin cerințe, UC-uri, lanțuri operaționale, date migrate, integrări, rapoarte, securitate, performanță și operare.

Capitolul stabilește modul în care fiecare cerință testabilă va ajunge în scenarii, execuții, defecte, retestări și evidențe de acceptanță. Furnizorul va pregăti pachete de testare care permit CNAS să confirme nu doar că o funcție există, ci că ea funcționează în procese reale: plătitor, contribuție, cont individual, cerere, dosar, decizie, plată, raport, integrare și audit.

Testarea va fi integrată în incrementurile lunare din M2 și în milestone-urile ulterioare, dar UAT-ul formal va rămâne momentul în care CNAS validează funcțional și operațional sistemul pe scenarii aprobate. Incrementurile lunare vor reduce riscul, iar acceptanța formală va fi susținută prin evidențe.

Testarea ca lanț de evidențe

Figura Testarea ca lanț de evidențe: cerință → test → acceptanță

12.2 Ancorarea testării în UC-uri, cerințe ToR și livrabile

Testarea va porni de la cerințele documentației de atribuire, de la UC01-UC23 și de la anexele funcționale ale SI „Protecția Socială”. Furnizorul va utiliza matricea de conformitate, registrul cerințelor, SRS/SDD și matricea de test coverage ca instrumente active de lucru. Fiecare scenariu de testare va indica cerința sau grupul de cerințe acoperit, UC-ul sau lanțul operațional verificat, datele utilizate, rezultatul așteptat și evidența produsă.

Această ancorare este necesară deoarece testarea nu poate rămâne generică. Un test de „salvare formular” nu demonstrează acceptanța unui serviciu public dacă nu arată rolul utilizatorului, datele obligatorii, documentele, tranziția de workflow, efectul asupra dosarului, decizia, notificarea, auditul și comportamentul în cazuri negative. De aceea, testarea va urmări atât UC-urile individuale, cât și lanțurile operaționale care le leagă.

Zonă ToR / UC	Ce va fi testat	Evidență de acceptanță
UC01-UC04: interfață publică, servicii informative, căutare, vizualizare/descărcare	Acces anonim/controlat, conținut public, căutare, descărcări, minimizarea datelor, comportament la informații indisponibile.	scenarii publice, capturi/output, log acces, verificare anonimizare/depersonalizare
UC04-UC05: dashboard, sarcini și navigare operațională	Cozi de lucru, sarcini pe rol, priorități, statusuri, acțiuni disponibile, filtrare și legătură cu obiectele de proces.	scenarii rol, liste sarcini, test acces/acțiuni, feedback CNAS

Zonă ToR / UC	Ce va fi testat	Evidență de acceptanță
UC06-UC11 și UC21: cereri, formulare, dosare, procesare, decizie, documente/notificări	Depunere/înregistrare, documente obligatorii, verificări, calcul, aprobare/respingere, semnare unde este cazul, document generat, notificare, descărcare.	UAT pack pe fluxuri, defect log, output document, audit trail, decizie CNAS
Registre plătitori, persoane asigurate, cont individual, contribuții și anexe aferente	Înregistrare/actualizare, istoric, consolidare contribuții, perioade, solduri, extras de cont, legătură cu drepturi și rapoarte.	test cases date, reconciliere eșantioane, verificare istoric, valori de control
UC09 și UC19: rapoarte, statistici, exporturi și documente	Catalog rapoarte, parametri, sursă de date, snapshot/data mart, export, performanță, audit generare, regenerare istorică.	raport validat, valori de control, audit export, test performanță raport
UC14: interoperabilitate și schimb de date	Contracte, payload-uri, timeouts, retry, erori, snapshot, indisponibilitate externă, audit schimb date.	contract tests, loguri integrare, scenarii negative, PV interoperabilitate
UC15-UC18: configurare, administrare, roluri, acces și metadate	Roluri, permisiuni, utilizatori, nomenclatoare, șabloane, workflow, configurări cu efect funcțional.	test admin, test acces negativ, decision log, audit configurare
UC20, UC22, UC23: proceduri automate, notificări și jurnalizare	Joburi, notificări, audit business/tehnic, evenimente, reluare proces, idempotency, vizibilitate operațională.	job report, notification log, event log, retest, evidence pack

Clarificare privind ancorarea în cerințe. Detaliile exhaustive cerință-cu-cerință vor rămâne în matricea de conformitate și în planul de testare. Capitolul de față stabilește modul în care acele cerințe devin scenarii și evidențe, pentru ca testarea să nu fie ruptă de ToR.

Scenariile UAT nu vor fi derivate exclusiv din UC01–UC23. Furnizorul va construi UAT pack-ul și pe baza proceselor și scenariilor descrise în anexele funcționale ale caietului de sarcini. UC-urile reprezintă unități formale de comportament al sistemului, iar anexele descriu variantele operaționale concrete în care aceste comportamente trebuie să funcționeze pentru plătitori, persoane asigurate, servicii publice, plăți, rapoarte, documente și integrări.

Pentru fiecare domeniu operațional, UAT-ul va include scenarii standard, scenarii cu date incomplete, scenarii cu documente lipsă, scenarii cu verificări externe indisponibile, scenarii de respingere, corectare, recalculare, suspendare, restabilire, generare document, notificare, raportare și audit. Astfel, acceptanța nu se va limita la faptul că un ecran se deschide sau că un UC poate fi executat în condiții ideale, ci va verifica comportamentul instituțional real descris de anexele ToR.

Rezultatele UAT vor fi legate de registrul proceselor/scenariilor. Pentru fiecare scenariu acceptat, pachetul de evidențe va indica cerința/anexa, UC-ul asociat, datele de test, pașii executați, rezultatul obținut, defectele identificate, remedierea și concluzia CNAS. Această structură protejează atât CNAS, cât și Furnizorul: acceptanța se bazează pe scenarii documentate, nu pe interpretări ulterioare diferite ale aceleiași cerințe.

12.3 Strategie de testare bazată pe trasabilitate

Furnizorul va utiliza matricea de conformitate și registrul cerințelor ca instrumente active de testare. Fiecare cerință funcțională, UC, cerință non-funcțională, condiție de migrare, integrare, securitate, raportare, suport sau livrabil va fi legată de artefacte de proiectare, pachete de lucru, cazuri de test și evidențe.

Pentru UC-uri, testarea va avea două niveluri. Primul nivel confirmă acoperirea fiecărui UC: roluri, date, acțiuni, ecrane, API-uri, documente și rezultate. Al doilea nivel confirmă lanțurile operaționale: dashboard -> sarcină -> cerere/dosar -> verificare -> calcul/decizie -> document/notificare -> plată/raportare -> audit. Astfel, UC-ul rămâne verificabil contractual, iar sistemul rămâne demonstrat ca mecanism operațional.

Element urmărit	Legătură în testare	Evidență
Cerință ToR / UC	se leagă de SRS/SDD, scenariu test, roluri, date, rezultat așteptat	matrice cerințe-test, test case, rezultat execuție
Functional Backbone	cerere, dosar, sarcină, decizie, document, notificare, raportare, audit	scenarii end-to-end, UAT pe lanțuri
Shared Services / Shared Artefacts	workflow, notificări, documente, șabloane, audit, Integration Gateway, reporting layer	teste reutilizare, regresie, contracte interne
Cerințe non-funcționale	performanță, securitate, disponibilitate, recovery, observabilitate	rapoarte load/security/recovery, dashboards
Livrabile și acceptanță	documente, rapoarte, PV, release package, defect log, retest	pachet acceptanță pe milestone

12.4 Execuție, date de test și medii

Testarea va fi organizată progresiv, pe straturi complementare. Fiecare strat are rolul său și produce evidențe diferite. Scopul nu este multiplicarea formală a testelor, ci acoperirea riscurilor reale: reguli, date, integrare, performanță, securitate, migrare, raportare, operare și utilizare.

Nivel de testare	Ce verifică	Legătură cu cerințele / UC	Evidență
Unit / component	reguli locale, validări, transformări, servicii backend	cerințe tehnice și reguli de business din SRS/SDD	rezultate automate, build log
Integration / contract	API-uri interne, gateway, servicii externe, erori, retry, timeout	UC14, cerințe INT, scenarii de indisponibilitate	contract test report, logs
Functional / UC	comportamentul fiecărui UC pe roluri, date și acțiuni	UC01-UC23 și anexele funcționale	test cases, capturi/output, defect log
End-to-end chains	procese CNAS cap-coadă: cerere-dosar-decizie-plată-raportare-audit	functional backbone și scenarii critice	scenarii executate, feedback log
Migration / reconciliation	date migrate, mapping, valori control, duplicate, excepții	cerințe M4/migrare/populare	raport reconciliere, error bucket
Performance / load	timpi, concurență, rapoarte grele, batch, integrare	NFR/performance și volume asumate	raport performanță, profil încărcare
Security / privacy	roluri, acces, date personale, export, audit, cazuri negative	UC18, UC23, SEC/privacy	security readiness evidence
UAT	acceptanța funcțională pe scenarii aprobate de CNAS	UC, lanțuri, livrabile, criterii acceptanță	UAT report, observații, sign-off

Date de test, medii și condiții de execuție

Furnizorul va pregăti testarea pe medii și date potrivite scopului fiecărei etape. Testarea funcțională poate utiliza date controlate și scenarii sintetice, dar UAT-ul, testarea migrației, raportarea statistică și performanța trebuie să includă date reprezentative și volume suficient de apropiate de realitatea CNAS.

Mediul de pre-producție, dacă este disponibil prin infrastructura aprobată, va fi utilizat pentru testări apropiate de producție: performanță, integrare, migrare, rapoarte voluminoase, deployment rehearsal, backup/restore și go-live readiness. Datele folosite în medii non-producție vor respecta regulile de protecție, mascare sau pseudonimizare acolo unde este necesar.

- seturi de date pentru UC-uri și fluxuri standard;
- seturi de date pentru excepții: documente lipsă, date inconsistente, rol insuficient, integrare indisponibilă;
- date pentru migrare pilot, reconciliere și error bucket;
- date pentru raportare statistică, snapshot-uri și regenerare istorică;
- date pentru performanță, batch-uri și rapoarte grele.

12.5 UAT, defecte și testarea zonelor critice

UAT-ul va începe numai după ce Furnizorul transmite un pachet pregătit pentru verificare, nu o versiune în lucru fără evidențe. Intrarea prematură în UAT produce doar liste lungi de probleme; intrarea controlată permite CNAS să valideze sensul funcțional, nu să descopere lipsuri elementare.

Condiție de intrare în UAT	Ce verifică	Evidență transmisă CNAS
Versiune instalată pe mediu relevant	build, release notes, configurări, acces	release package, deployment note
Cerințe/UC mapate la scenarii	acoperirea UC și lanțurilor operaționale	UAT matrix, test pack
Date pregătite	date funcționale, migrare pilot, rapoarte, excepții	data readiness note
Roluri și conturi configurate	utilizatori, permisiuni, scope date	access matrix, test users
Defecte critice interne închise	stabilitatea înainte de UAT	defect baseline, retest evidence
Documentație disponibilă	manuale, ghiduri, instrucțiuni de lucru	user guide, quick guides

UAT controlat

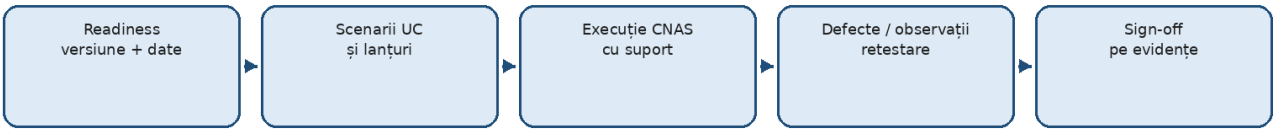


Figura UAT controlat: intrare pregătită, execuție, decizie

Defect management, severitate și retestare

Defectele vor fi gestionate într-un registru unic, cu descriere, pași de reproducere, severitate, prioritate, componentă afectată, cerință/UC, versiune de remediere, status, rezultat de retestare și decizie de închidere. Defectul nu va fi închis doar prin afirmația că a fost remediat; închiderea va necesita retestare și evidență.

Registrul va separa defectele de observații și de schimbările de scope. Un defect indică abatere de la cerință, design aprobat sau rezultat așteptat. O observație poate conduce la ajustare în limitele scope-ului. O

schimbare de scope va intra în mecanismul de change control. Această separare protejează atât CNAS, cât și Furnizorul de interpretări diferite în timpul UAT.

Performanță, securitate, recovery și testarea zonelor critice

Pentru performanță, testele vor utiliza scenarii apropiate de exploatarea reală: autentificare, căutare persoană/plătitor, deschidere dosar, salvare formular, tranziție workflow, interogare cont, generare document, raport greu, apel integrare, batch și proces de închidere. Rezultatele vor include configurația testată, volumul datelor, profilul de încărcare, metrici și concluzii de remediere.

Pentru securitate, testarea va include verificări de autentificare, autorizare, control pe rol/acțiune/obiect, sesiuni, input validation, exporturi, acces administrativ, audit și protecția datelor personale. Scenariile negative sunt obligatorii: utilizator fără rol, acces la dosar nealocat, export nepermis, tranziție invalidă, modificare configurare fără drept.

Pentru recovery și continuitate, testarea va verifica restaurarea, reluarea batch-urilor, comportamentul la indisponibilitatea unei integrări, rollback/forward fix și procedurile operaționale. Un sistem critic nu este acceptabil doar dacă funcționează în cazul ideal; el trebuie să răspundă controlat și la eșecuri.

12.6 Pachet de acceptanță și acoperirea testării

Acceptanța va fi construită din pachete de evidențe, nu din declarații generale. Pentru fiecare milestone și pentru fiecare capabilitate critică, Furnizorul va pregăti documentele, rapoartele, logurile, output-urile și procesele-verbale necesare. Pachetul va arăta cerința, implementarea, testul, rezultatul, defectele, retestarea și decizia CNAS.

Zona de acceptanță	Evidențe incluse
Funcțional / UC	matrice UC-test, scenarii executate, output-uri, defecte/retestări, sign-off
Migrare	mapping, rulări pilot, reconciliere, error bucket, decizii CNAS pe excepții
Integrare	contracte, payload-uri, scenarii negative, loguri, PV interoperabilitate
Raportare	catalog rapoarte, surse, valori de control, audit generare, teste performanță
Securitate	acces pe roluri, test negativ, audit trail, scanări/verificări, remedieri
Operabilitate	runbook, monitoring, backup/restore, readiness checklist, release package

Metoda de calcul pentru acoperirea testării

Baseline-ul de testare va fi aprobat împreună cu CNAS înainte de execuția UAT. Acoperirea se va calcula la nivel de cerințe testabile aprobate, nu ca acoperire de cod. O cerință se consideră acoperită numai dacă are scenariu aprobat, execuție documentată și rezultat verificabil. Scenariile blocate, neexecutate sau fără evidență nu vor fi considerate acoperite.

Cerințele critice pentru go-live — securitate, autentificare/autorizare, integritatea datelor, fluxurile operaționale principale, migrarea, integrările esențiale, calculul și operațiunile care influențează plăți sau decizii — vor avea criterii mai stricte decât funcțiile cu risc redus.

Rezultatul livrat către CNAS

Prin această abordare, CNAS primește nu doar un sistem testat, ci un sistem ale cărui rezultate pot fi verificate. Fiecare zonă critică — funcțional, date, integrare, raportare, performanță, securitate, migrare, operare — va avea scenarii, execuții, defecte, retestări și evidențe. Acceptanța devine astfel un act informat și demonstrabil, nu o formalitate bazată pe impresia unei demonstrații.

13. Instruire, documentație, cod sursă și handover operațional

13.1 Rolul secțiunii

Furnizorul va trata instruirea și handover-ul ca parte a pregătirii operaționale a sistemului, nu ca activități administrative executate la final. Pentru SI „Protecția Socială”, succesul implementării depinde de capacitatea CNAS de a utiliza, administra, susține, verifica și continua sistemul după acceptanță.

Capitolul stabilește modul în care Furnizorul va transfera cunoștințele către CNAS: instruire pe roluri și UC-uri, materiale de lucru, documentație funcțională și tehnică, cod sursă, artefacte de deployment, runbook operațional, shadowing tehnic și pachet de handover. Instruirea nu va fi prezentare de meniuri, iar handover-ul nu va fi o arhivă de fișiere; ambele vor fi legate de cerințe, fluxuri și responsabilități reale.

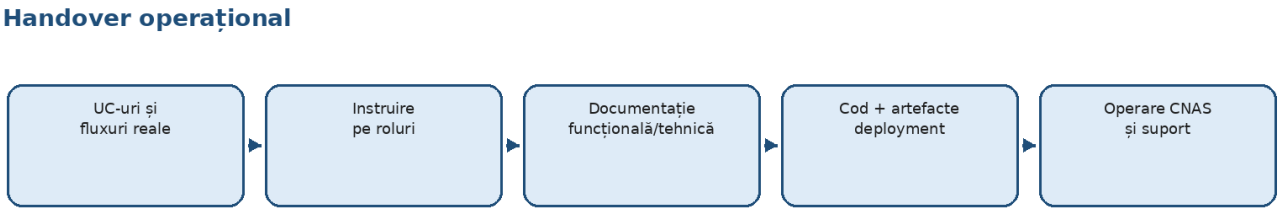


Figura Handover operațional: de la sistem livrat la capacitate de operare CNAS

13.2 Ancorarea instruirii și documentației în UC-uri și cerințe

Instruirea și documentația vor fi legate de UC01-UC23, de rolurile operaționale și de lanțurile funcționale definite în SRS/SDD. Furnizorul nu va preda utilizatorilor un manual abstract al aplicației, ci materiale și sesiuni care răspund la întrebarea: ce face utilizatorul în procesul său concret, ce date verifică, ce decizie ia, ce document generează, ce notificare primește/transmite și ce evidență rămâne.

Această ancorare este necesară pentru ca utilizatorii CNAS/CTAS, administratorii, formatorii, echipa de suport și echipa IT să poată opera sistemul în aceeași logică în care acesta a fost proiectat și testat. Dacă un UC este verificat în UAT, el trebuie să se regăsească și în training, ghiduri, scenarii de lucru și, după caz, în runbook-ul operațional.

Grup UC / cerințe	Ce trebuie învățat / documentat	Livrabile de instruire și handover
UC01-UC04: interfață publică și servicii informative	căutare, vizualizare, descărcare, limite de date publice, comportament la informații indisponibile	ghid public/administrator conținut, scenarii demo, FAQ
UC04-UC05: dashboard, sarcini și navigare	identificarea sarcinii, priorități, statusuri, acțiuni disponibile, escaladare	ghid operator/șef direcție, quick guide dashboard, exerciții practice
UC06-UC11 și UC21: cereri, formulare, dosare, decizii, documente	înregistrare cerere, documente, verificări, calcul, decizie, aprobare, documente, notificări	manual pe fluxuri, video scurte, scenarii de training, test practic
Registre, contribuții, plătitori, persoane asigurate, cont individual	căutare, istoric, interpretare date, corecții permise, legătură cu drepturi/rapoarte	ghid funcțional, exemple de cazuri, dicționar date
UC09/UC19: rapoarte și documente	selectare parametri, surse, snapshot-uri, exporturi, audit generare, interpretarea indicatorilor	catalog rapoarte, ghid raportare, descrieri indicatori
UC14: interoperabilitate	semnificația răspunsurilor, erori, indisponibilitate, reluare, snapshot	catalog integrare, runbook integrare, scenarii suport

Grup UC / cerințe	Ce trebuie învățat / documentat	Livrabile de instruire și handover
UC15-UC18 și UC20-UC23: administrare, workflow, notificări, audit	roluri, permisiuni, nomenclatoare, șabloane, proceduri automate, audit și jurnalizare	ghid administrator, runbook, training IT/suport, matrice drepturi

13.3 Instruire pe roluri și scenarii reale

Instruirea va fi organizată pe roluri operaționale, nu ca prezentare generală de ecrane. Fiecare categorie de utilizatori va lucra cu scenarii apropiate de activitatea reală: dashboard, căutare, înregistrare cerere, examinare, verificare documente, calcul, decizie, generare document, raportare, administrare, suport și escaladare.

Public țintă	Scenarii principale	Legătură cu UC / cerințe	Evidență
Operator CNAS/CTAS	sarcini, cereri, dosare, documente, statusuri, verificări, notificări	UC04-UC11, UC21, flux cerere-dosar-decizie	prezență, exerciții, evaluare practică
Șef direcție / management operațional	dashboard, monitorizare sarcini, aprobare, rapoarte, escaladare	UC04-UC05, UC09, UC19, UC22	scenarii management, feedback
Administrator funcțional	roluri, permisiuni, nomenclatoare, șabloane, workflow, notificări	UC15-UC18, UC20, UC23	test administrare, checklist
Echipă suport L1/L2	clasificare solicitări, reproducere defect, loguri, escaladare, workaround	cerințe suport/SLA, service desk, UC afectat	knowledge base, scenarii suport
Echipă IT CNAS	deployment, observability, DB/reporting, integrare, batch, backup/restore	cerințe operare, securitate, migrare, raportare	shadowing, runbook walkthrough

13.4 Materiale de instruire și suport post-training

Furnizorul va pregăti materiale adaptate rolurilor: ghiduri de utilizare, quick guides, descrieri de flux, exemple de cazuri, întrebări frecvente și materiale pentru administratori. Materialele vor fi structurate pe UC-uri și procese, astfel încât utilizatorul să poată găsi rapid instrucțiunea asociată acțiunii sale.

Materialele nu vor repeta doar meniurile aplicației. Ele vor explica acțiunile pe care utilizatorul trebuie să le facă în proces: cum identifică sarcina, cum verifică datele, cum interpretează mesajele sistemului, cum tratează o excepție, cum generează documente, cum folosește rapoarte și cum escaladează o problemă.

- manual de utilizare pe roluri și fluxuri, cu trimiteri la UC-uri relevante;
- ghiduri rapide pentru operațiuni frecvente;
- ghid administrator funcțional pentru roluri, nomenclatoare, șabloane și workflow-uri;
- ghid suport / service desk pentru clasificare solicitări și escaladare;
- FAQ și knowledge base inițial;
- materiale actualizate după stabilizare și după schimbările relevante.

13.5 Documentația funcțională, tehnică și operațională

Documentația va fi livrată ca pachet operațional complet, nu ca anexă formală. Fiecare document va avea rol în utilizare, mentenanță, suport, audit sau transfer. Documentația va fi actualizată progresiv, astfel încât versiunea predată să reflecte sistemul livrat și acceptat.

Document / artefact	Conexiune cu cerințele	Rol în exploatare / handover
SRS / specificații funcționale	UC01-UC23, anexe, reguli de domeniu, decizii CNAS	bază pentru testare, suport, evoluție funcțională
SDD / arhitectură și design tehnic	NFR, securitate, integrare, date, raportare, deployment	mentenanță, diagnostic, extindere, audit tehnic
Matrice conformitate / test coverage	ToR, UC, DEL/UAT/COM/NFR	demonstrarea acoperirii și acceptanței
Model de date și dicționar	registre, cereri, decizii, plăți, raportare, migrare	operare DB, raportare, transfer către alt furnizor
Catalog integrare	UC14 și cerințe INT	diagnostic, schimbări API, testare contracte
Catalog rapoarte/indicatori	UC09/UC19 și cerințe raportare	utilizare rapoarte, interpretare date, regenerare istorică
Runbook operațional	operabilitate, suport, BCDR, deployment, monitoring	intervenții controlate, suport L2/L3, service transition
Ghiduri utilizator/administrator	roluri, UC, workflow, administrare	instruire și exploatare curentă

13.6 Predare tehnică, handover operațional și criterii de finalizare

Furnizorul va preda codul sursă și artefactele tehnice într-o formă verificabilă și reutilizabilă. Predarea nu se va limita la o arhivă statică de fișiere. CNAS va primi repository-uri complete sau exporturi structurate, istoric/versiuni relevante, instrucțiuni de build, dependințe declarate, scripturi de baze de date, contracte API, configurări și artefacte de deployment asociate versiunii livrate.

Pentru deployment, pachetul va include artefacte containerizate sau instrucțiuni de reconstruire, Helm charts/configurări, variabile de mediu, mapping de configurări, proceduri de promovare între medii, release notes și, când scenariul o cere, instrucțiuni de rollback/forward-fix. Aceste artefacte trebuie să fie legate de versiunea acceptată, nu predate ca elemente separate fără relație cu release-ul.

13.7 Handover operațional și shadowing tehnic

Handover-ul operațional va conecta sistemul livrat de exploatarea reală. Furnizorul va organiza sesiuni de transfer pentru echipa IT CNAS și pentru administratorii desemnați, astfel încât aceștia să poată înțelege mecanismele critice: CI/CD, deployment MCloud, PostgreSQL, reporting layer, integrare, observabilitate, securitate, document storage, backup/restore și suport.

Pentru componentele critice, Furnizorul va organiza sesiuni de shadowing în care specialiștii CNAS urmăresc și execută, sub ghidaj, operațiuni controlate. Scopul este ca transferul să nu rămână teoretic; echipa CNAS trebuie să vadă cum se investighează, cum se verifică și cum se operează sistemul.

- parcurgerea runbook-ului operațional cu exemple concrete;
- **demonstrarea unui deployment controlat și a unui rollback/forward-fix când scenariul o cere;**
- investigarea unui incident simulat folosind loguri, metrici și traces;
- execuția unui backup/restore test, în limitele mediilor disponibile;
- rularea unui proces batch și analiza checkpoint-urilor/erorilor;
- parcurgerea unei solicitări de suport de la ticket la închidere.

Transferul de cunoștințe

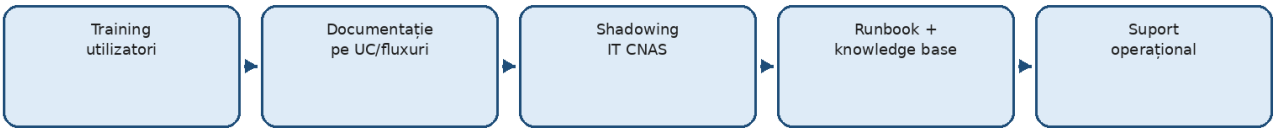


Figura Transferul de cunoștințe: documente, sesiuni și shadowing

Handover checklist și criterii de finalizare

Categorie	Ce se predă	Criteriu de finalizare
Instruire	plan, sesiuni, materiale, evaluări, feedback	participanți instruiți și evidențe acceptabile
Documentație funcțională	SRS, ghiduri, fluxuri, catalog UC/scenarii	aliniată cu versiunea acceptată
Documentație tehnică	SDD, API, DB model, integrare, deployment, security	suficientă pentru mentenanță și transfer
Cod și build	repository/export, instrucțiuni build, dependințe, scripturi DB	build reproductibil pe baza instrucțiunilor
Operare	runbook, monitoring, backup/restore, release notes, known issues	echipa CNAS/suport poate urmări procedurile
Suport	knowledge base, matrice escaladare, registru solicitări, SLA	service transition pregătit

Rezultatul livrat către CNAS

Prin această abordare, Furnizorul va preda CNAS nu doar un sistem funcțional, ci o capacitate documentată de utilizare și operare. Utilizatorii vor primi instruire pe scenarii reale; administratorii vor primi mecanisme pentru configurare și control; echipa IT și suportul vor primi cod, artefacte, runbook-uri și proceduri; iar CNAS va putea verifica, susține și transfera sistemul pe baza unor evidențe, nu pe baza memoriei echipei de implementare.

14. Suport, garanție, mentenanță și service management

14.1 Poziționarea serviciilor de suport

Furnizorul va trata suportul post-implementare ca serviciu operațional măsurabil, nu ca disponibilitate informală a echipei de dezvoltare. Pentru SI „Protecția Socială”, perioada de garanție, mentenanță și suport este mecanismul prin care CNAS păstrează continuitatea după stabilizare, gestionează incidentele, primește remedieri controlate și menține capacitatea de exploatare a sistemului în condiții sigure.

Serviciile vor fi organizate pe principii de service management, cu registru unic al solicitărilor, clasificare, SLA, escaladare, analiză de cauză-rădăcină, release control, raportare periodică și evidențe de închidere. Garanția este prezentată ca serviciu cu reguli, responsabilități, termene și rezultate verificabile.

Perioada de suport și garanție va începe după finalizarea stabilizării și după support readiness review. Astfel, sistemul nu trece brusc din proiect în exploatare; cunoștințele acumulate în analiză, dezvoltare, migrare, go-live și stabilizare sunt transformate în runbook-uri, proceduri, dashboarduri, registre și responsabilități operaționale.

În această secțiune, termenul „suport” include activități de service desk, garanție, mentenanță corectivă/preventivă/adaptivă, asistență operațională, release-uri de remediere, raportare și transfer de cunoștințe. Dezvoltarea funcționalităților noi care depășesc sistemul acceptat rămâne sub controlul procedurii de schimbare.
Conceptul de mentenanță adaptivă și suport se aplică exclusiv pentru menținerea sistemului în conformitate cu specificațiile tehnice inițiale și modificările legislative obligatorii. Orice modificare de flux, ecran nou sau funcționalitate suplimentară solicitată de beneficiar va fi tratată separat ca cerere de schimbare (Change Request), pentru a preveni degradarea performanței serviciului de suport de bază.”
Calculul indicatorilor de performanță (SLA) vizează exclusiv disponibilitatea codului aplicativ și timpul de reacție al echipei Furnizorului. Timpul de indisponibilitate cauzat de probleme de rețea, infrastructură MCloud, servicii guvernamentale externe (MConnect, MPass etc.) sau întârzieri în aprobările administrative ale CNAS va fi extras automat din calculul penalităților.”

14.2 Obiectivul perioadei de garanție și suport

Furnizorul va presta servicii de garanție, mentenanță și suport tehnic timp de 12 luni după finalizarea perioadei de stabilizare, conform cerințelor proiectului. Obiectivul este menținerea sistemului în parametrii acceptați, remedierea defectelor de funcționare ale soluției livrate, suportul tehnic pentru exploatare și păstrarea trasabilității tuturor intervențiilor.

Defectele de funcționare ale sistemului livrat vor fi remediate din contul Furnizorului în limitele garanției și ale SLA. Funcționalitățile noi, extinderile de scope, integrările noi semnificative sau modificările majore care nu derivă din cerințele acceptate vor fi tratate prin managementul schimbărilor, cu analiză de impact, estimare, aprobare, planificare, testare și release control.

Suportul va acoperi nu doar incidente tehnice, ci și asistență pentru utilizarea corectă a platformei, clarificări operaționale, diagnostic, verificarea unor comportamente raportate, consultanță pentru administrare, mentenanță preventivă și actualizarea documentației aferente remedierilor livrate.

Categorie de serviciu	Ce acoperă	Ce nu acoperă automat	Evidență
Garanție	Defecte ale sistemului livrat față de cerințe, SRS/SDD, scenarii acceptate sau comportament demonstrat.	Funcționalități noi, extinderi de domeniu, schimbări legislative majore neincluse.	ticket, analiză, remediere, test, release notes, confirmare închidere
Suport tehnic	Asistență pentru operare, diagnostic, întrebări tehnice, verificări de comportament, ghidare administrativă.	Activități de dezvoltare care modifică obiectul sistemului acceptat.	ticket, răspuns, recomandare, material suport/FAQ dacă este cazul

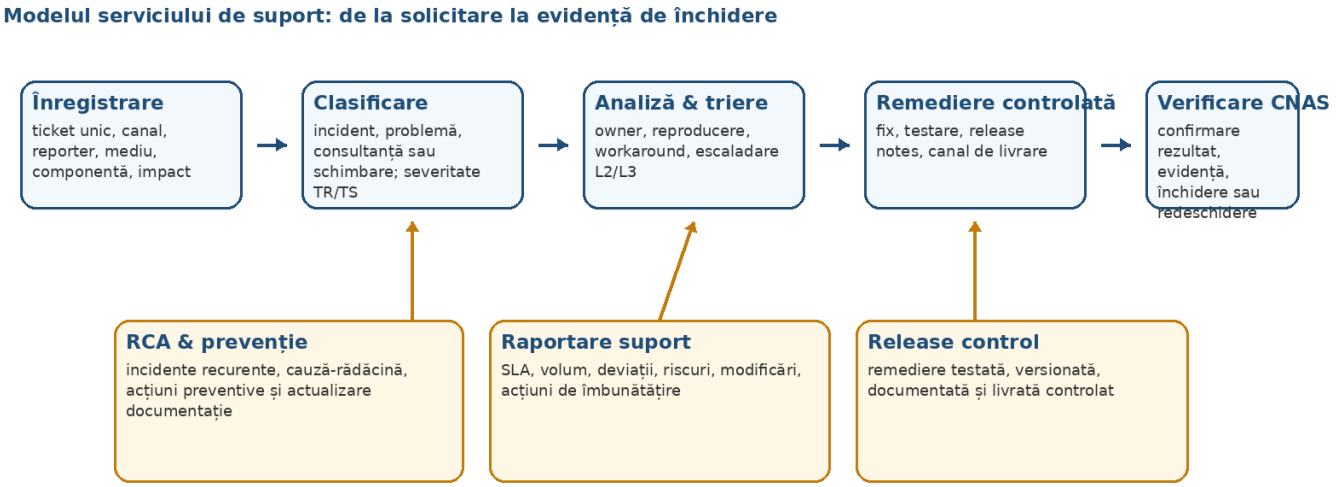
Categorie de serviciu	Ce acoperă	Ce nu acoperă automat	Evidență
Mentenanță corectivă	Remedieri ale erorilor confirmate și ale comportamentelor neconforme.	Schimbări de proces sau reguli noi fără change control.	defect log, fix version, test evidence
Mentenanță preventivă	Analiză loguri, riscuri recurente, patchuri de securitate, optimizări minore și acțiuni preventive.	Rescrieri arhitecturale sau dezvoltări funcționale noi.	raport suport, RCA, acțiuni preventive
Mentenanță adaptivă	Ajustări necesare pentru mediu, integrări, configurări sau parametri aprobați, în limitele sistemului acceptat.	Extinderi majore de integrare sau capabilități noi.	impact analysis, aprobare, release control

14.3 Model service desk, registru solicitări și SLA

Furnizorul va opera un model service desk bazat pe un punct unic de evidență. CNAS poate utiliza canalele agreate pentru comunicare, dar fiecare incident, problemă, solicitare de consultanță, cerere de schimbare sau solicitare de mentenanță trebuie să ajungă în registrul oficial al suportului.

Registrul unic permite urmărirea completă a solicitării: cine a raportat, când a fost raportată, ce componentă este afectată, ce mediu este afectat, ce impact operațional există, cine este responsabil, ce acțiuni au fost efectuate, ce versiune a fost afectată, ce remediere a fost livrată și ce evidență confirmă închiderea.

Această regulă reduce suportul informal și protejează ambele părți. CNAS poate verifica starea solicitărilor, iar Furnizorul poate demonstra respectarea SLA, cauzele întârzierilor, acțiunile efectuate și diferența dintre defect, consultanță, mentenanță și schimbare.



Fgura Modelul serviciului de suport: solicitare, remediere, evidență

Conținutul minim al solicitării

Câmp / informație	Rol în tratarea solicitării	Observație de control
ID unic, dată/oră, canal	Permite urmărirea SLA și auditul serviciului.	Fără ID unic nu există evidență oficială de suport.
Tip solicitare	Incident, problemă, consultanță, schimbare, mentenanță, administrare.	Tipul stabilește fluxul de tratare și raportarea.
Severitate / prioritate	Determină TR/TS și escaladarea.	Severitatea poate fi reclasificată motivat.
Mediu și componentă afectată	Separă producție, UAT, test, integrare, raportare, batch, DB, UI.	Evită diagnostic generic și intervenții greșite.
Descriere și pași de reproducere	Permite confirmarea defectului și testarea remedierii.	Pentru incidente critice se acceptă descriere inițială redusă, completată ulterior.
Impact operațional	Arată efect asupra utilizatorilor, plăților, deciziilor, raportării, integrărilor.	Impactul poate justifica escaladarea.
Atașamente / loguri / capturi	Susțin analiza tehnică și funcțională.	Datele personale se transmit controlat, conform regulilor agreate.
Acțiuni, workaround, versiune de remediere	Păstrează istoria intervenției.	Închiderea se face cu evidență și confirmare.

Clasificarea solicitărilor și nivelurile SLA

Furnizorul va respecta clasificarea solicitărilor și timpii TR/TS solicitați. Programul de suport este în zilele lucrătoare ale Republicii Moldova, în intervalul 08:00–18:00, cu tratamentul special al solicitărilor critice conform SLA agreat. Timpul de răspuns înseamnă confirmarea preluării și inițierea tratării, iar timpul de soluționare înseamnă livrarea remedierii, workaround-ului acceptabil sau rezolvarea operațională conform naturii solicitării.

Clasificarea va fi vizibilă în registrul de suport și în rapoartele periodice. Dacă o solicitare este reclasificată după analiza impactului, reclasificarea va păstra motivul, data, persoana responsabilă și efectul asupra termenelor. Această regulă previne atât supraîncadrarea nejustificată, cât și subestimarea problemelor care afectează procese critice CNAS.

Categorie	Exemplu de impact	TR	TS	Regulă de control
Critică	Sistem indisponibil, proces critic blocat, defect cu impact major asupra plăților/deciziilor sau imposibilitate de lucru pentru mai multe unități.	5 minute	60 minute	Escaladare imediată, comunicare continuă, evidență post-incident.
Înaltă	Funcție importantă indisponibilă, integrare critică afectată, raportare obligatorie blocată, dar există workaround temporar.	60 minute	Până la finele zilei	Analiză prioritară, workaround unde este posibil, plan de remediere.
Ordinară	Defect sau solicitare care afectează lucru curent, dar nu	24 ore	3 zile	Tratare conform backlog suport și release control.

Categorie	Exemplu de impact	TR	TS	Regulă de control
	blochează procesul critic.			
Joasă	Întrebare, solicitare minoră, clarificare, ajustare fără impact operațional semnificativ.	3 zile	Best effort / termen comunicat	Termenul se comunică și se acceptă cu CNAS.

Separarea defectelor, problemelor, consultanței și schimbărilor

Furnizorul va separa clar defectele de garanție, problemele recurente, solicitările de consultanță și schimbările de scope. Această separare este necesară pentru a proteja garanția și pentru a evita transformarea suportului într-un flux nelimitat de dezvoltare nouă sau, invers, clasificarea unor defecte reale ca schimbări.

Un defect reprezintă abatere de la cerință, SRS/SDD, criteriu de acceptanță sau comportament demonstrat. O problemă reprezintă cauză comună sau recurentă care poate genera incidente multiple. O solicitare de consultanță sprijină utilizarea sau administrarea corectă a sistemului. O schimbare de scope introduce funcționalitate, regulă, integrare sau livrabil nou și necesită control al schimbării.

Reclasificarea unei solicitări va fi documentată. Dacă analiza arată că o solicitare inițial raportată ca defect reprezintă schimbare de scope, Furnizorul va prezenta argumentul, impactul și recomandarea. CNAS va decide asupra schimbărilor care afectează obiectul sistemului, prioritatea sau acceptanța.

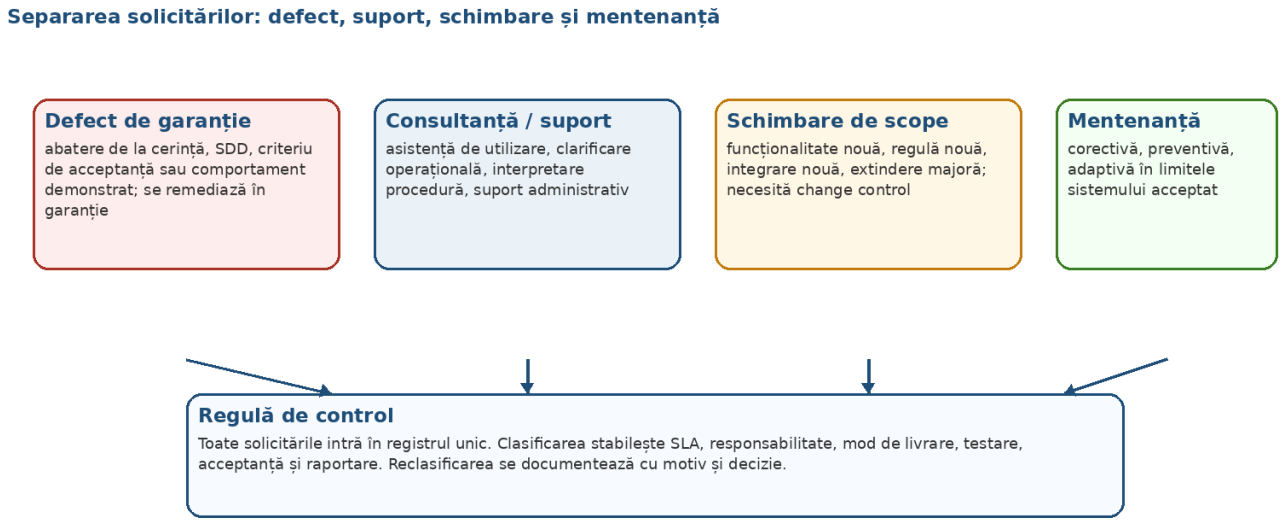


Figura Separarea solicitărilor în service management

Fluxul de tratare a solicitărilor

Fluxul standard de suport va include înregistrare, confirmare, clasificare, triere, analiză, reproducere, workaround unde este posibil, remediere, testare, livrare controlată, verificare de către CNAS și închidere. Pentru incidente critice, pașii se comprimă ca timp, dar nu se elimină evidența.

Furnizorul va păstra diferența între restabilirea serviciului și rezolvarea cauzei. Pentru un incident critic, prioritatea inițială este restabilirea funcționării sau aplicarea unui workaround acceptabil. Ulterior, incidentul poate trece în problem management, cu analiză de cauză-rădăcină și acțiuni preventive.

Remedierile care afectează codul, baza de date, configurările, integrarea, șabloanele, raportarea sau drepturile de acces vor urma release control. Un fix nu se aplică informal în producție. El este pregătit, testat, documentat, versionat și livrat prin canalul agreat, proporțional cu severitatea și urgența.

Escaladare și responsabilități pe niveluri de suport

Furnizorul va organiza suportul pe niveluri operaționale, astfel încât solicitările să ajungă rapid la persoanele capabile să le rezolve. Nivelul de suport nu trebuie confundat cu ierarhia administrativă; el indică tipul de competență necesară pentru remediere sau diagnostic.

CNAS va avea vizibilitate asupra escaladărilor prin registrul solicitărilor și prin raportarea periodică. Escaladarea nu suspendă SLA; ea este mecanismul prin care Furnizorul mobilizează resursa corectă pentru respectarea SLA.

Nivel	Rol principal	Exemple de activități	Evidență
L1 / service desk	Preluare, înregistrare, verificare inițială, comunicare, triere.	ticket, verificare date minime, status, informare CNAS.	registru solicitări, comunicări
L2 / suport aplicație	Diagnostic funcțional și tehnic, configurări, workaround, verificare fluxuri.	analiză UI/API, roluri, rapoarte, batch, integrare, configurări.	acțiuni, recomandări, workaround
L3 / echipă dezvoltare/arhitectură	Remediere cod, DB, integrare, batch, performanță, securitate.	fix, test, release package, release notes.	branch/commit, test evidence, versiune remediere
Escaladare management	Blocaje SLA, risc operațional, dependențe CNAS/STISC, decizii de schimbare.	prioritizare, decizie, plan de acțiune.	minute, decizie, plan

14.4 Hypercare, garanție și mentenanță controlată

Primele săptămâni după go-live vor fi tratate ca perioadă de hypercare, conectată cu stabilizarea operațională. În această perioadă, capacitatea de răspuns crește: comunicare accelerată, triere rapidă a observațiilor și prezență funcțională/tehnică proporțională cu riscul proceselor lansate.

Hypercare nu înlocuiește SLA-ul de suport. El reduce anxietatea operațională și permite colectarea rapidă a problemelor reale din exploatare. Observațiile recurente pot fi transformate în FAQ, ghiduri scurte, corecții de configurare, îmbunătățiri minore sau acțiuni de instruire suplimentară.

Dacă lansarea se face pe domenii sau pe CTAS-uri prioritare, Furnizorul va ajusta prezența și suportul conform planului de phase-in. Pentru CNAS central și pentru unitățile teritoriale cu volum ridicat, suportul în hypercare poate include sesiuni de asistență directă, puncte de contact dedicate și raportare zilnică a situației.

Mentenanță corectivă, preventivă și adaptivă

Mentenanța corectivă va remedia defectele confirmate ale sistemului livrat. Mentenanța preventivă va urmări reducerea riscurilor operaționale: analiză incidente recurente, verificări loguri, actualizări de securitate, optimizări minore, verificări de performanță și actualizarea documentației. Mentenanța adaptivă

va acoperi ajustări necesare pentru menținerea funcționării în raport cu schimbări ale mediului, integrărilor, parametrilor aprobați sau condițiilor de operare.

Actualizările la nivel de aplicație vor fi minimizate și grupate astfel încât CNAS să poată planifica aplicarea lor, inclusiv pe bază lunară, cu excepții pentru probleme critice sau vulnerabilități de securitate. Versiunile noi nu vor fi impuse automat în producție; ele vor fi planificate, documentate, testate și acceptate conform canalului de release.

Furnizorul va păstra trasabilitatea dintre solicitare, modificare, versiune, testare și deployment. Această regulă este esențială pentru un sistem în care remedierile pot afecta decizii, plăți, rapoarte, integrări sau date personale.

Administrarea fondului de dezvoltare neplanificată

În perioada de garanție se va administra distinct fondul de 50 om/zile pentru dezvoltare neplanificată, conform cerințelor documentației. Acest fond nu se confundă cu remedierea defectelor de garanție. Defectele confirmate ale sistemului livrat se remediază conform garanției; dezvoltarea neplanificată acoperă solicitări aprobate de CNAS care nu reprezintă defecte ale sistemului acceptat.

Utilizarea fondului va urma un mecanism transparent: solicitare CNAS, descriere, analiză de impact, estimare efort, aprobare, implementare, testare, livrare, evidență de consum și confirmare rezultat. Registrul de suport va păstra separat consumul acestui fond, astfel încât CNAS să poată urmări disponibilul, rezultatele livrate și deciziile aprobate.

Exemplele de utilizare pot include ajustări operaționale, completări minore de șabloane, rafinări de rapoarte, optimizări mici, adaptări compatibile cu sistemul acceptat sau mici îmbunătățiri solicitate după exploatarea reală. Funcționalitățile majore noi, integrările noi semnificative sau schimbările de domeniu vor fi tratate prin procedura formală de schimbare.

Knowledge base, FAQ și materiale de suport reutilizabile

Furnizorul va transforma întrebările recurente și incidentele repetitive în materiale de suport reutilizabile. Pe durata stabilizării și suportului, observațiile utilizatorilor CNAS/CTAS pot genera completări la ghiduri, FAQ, instrucțiuni scurte, materiale video sau proceduri interne de lucru.

Această abordare reduce presiunea pe service desk și crește autonomia utilizatorilor. Suportul nu va rămâne doar reactiv; el va produce cunoaștere operațională pentru CNAS și va ajuta la maturizarea modului de exploatare a sistemului.

Materialele actualizate vor fi versionate și predate CNAS. Dacă o remediere schimbă comportamentul unei funcții, documentația afectată va fi actualizată împreună cu release notes, astfel încât utilizatorii și administratorii să nu primească un sistem schimbat fără explicație.

Monitorizare, observabilitate și suport proactiv

Suportul pentru SI „Protecția Socială” va utiliza informațiile de observabilitate livrate în arhitectură: loguri, metrici, alerte, starea integrărilor, starea proceselor batch, timpi de răspuns, erori recurente și indicatori de sănătate. Furnizorul va folosi aceste date pentru diagnostic și pentru prevenirea incidentelor, nu doar pentru analiză post-factum.

Pentru procesele critice — integrare, batch, raportare voluminoasă, joburi de plată, refresh de data marts, notificări sau sincronizări — suportul va urmări starea execuției, durata, volumul procesat, rezultatul, erorile,

retry-urile și posibilitatea de reluare. O problemă de batch sau integrare nu trebuie descoperită doar prin reclamația utilizatorului; ea trebuie să devină vizibilă prin monitorizare și alerte.

Dacă infrastructura MCloud/STISC limitează anumite mecanisme de observabilitate, Furnizorul va documenta cerințele, alternativele și impactul asupra suportului. CNAS va primi recomandări pentru menținerea vizibilității operaționale necesare unui sistem critic.

14.5 Raportarea serviciilor de suport

Furnizorul va prezenta rapoarte periodice de suport, în format agreat cu CNAS. Raportul va arăta calitatea serviciului și starea operațională a sistemului, nu doar lista tichetelelor închise.

Raportarea va include volumul solicitărilor pe tip și severitate, respectarea TR/TS, solicitări deschise, incidente critice/înalte, probleme recurente, cauză-rădăcină, acțiuni preventive, modificări livrate, release notes, documentație actualizată, consumul fondului de dezvoltare neplanificată, riscuri operaționale și recomandări pentru perioada următoare.

Rapoartele de suport vor susține service review-uri periodice cu CNAS. Aceste întâlniri permit verificarea calității suportului, prioritizarea problemelor recurente, validarea acțiunilor preventive și pregătirea eventualelor schimbări controlate.

Indicator / evidență	Ce arată	Utilitate pentru CNAS
Solicitări pe categorie/severitate	Volumul și profilul suportului.	Identifică zonele cu presiune operațională.
Respectarea TR/TS	Calitatea răspunsului și soluționării.	Verifică respectarea SLA.
Incidente majore și RCA	Cauzele problemelor importante.	Permite prevenție și decizii de operare.
Probleme recurente	Defecte sau procese care produc solicitări repetate.	Reduce costul operațional prin acțiuni preventive.
Release-uri livrate	Ce remedieri/modificări au intrat în sistem.	Leagă suportul de controlul versiunilor.
Documentație actualizată	Ghiduri, runbook, FAQ, proceduri modificate.	Păstrează cunoașterea instituțională.
Consum 50 om/zile	Solicitări aprobate, efort consumat, rezultat.	Separă dezvoltarea neplanificată de garanție.
Riscuri și recomandări	Probleme care pot afecta operarea viitoare.	Permite acțiuni înainte de incident.

Support readiness review și începutul garanției

Înainte de intrarea deplină în perioada de garanție și suport, Furnizorul va executa un support readiness review. Acesta confirmă că sistemul poate trece din regim de proiect în regim de serviciu operațional.

Review-ul va verifica cel puțin existența runbook-ului operațional, canalele de suport, registrul solicitărilor, regulile de clasificare, SLA-ul, matricea de escaladare, accesul echipei de suport, lista problemelor cunoscute, documentația tehnică și de utilizare, procedura de release pentru remedieri, dashboardurile și alertele operaționale.

Dacă anumite elemente nu sunt pregătite, trecerea în suport va fi documentată cu acțiuni deschise, responsabilități și termene. Garanția nu trebuie să înceapă ca perioadă ambiguă în care echipa de proiect intervine informal, iar echipa de suport nu are context.

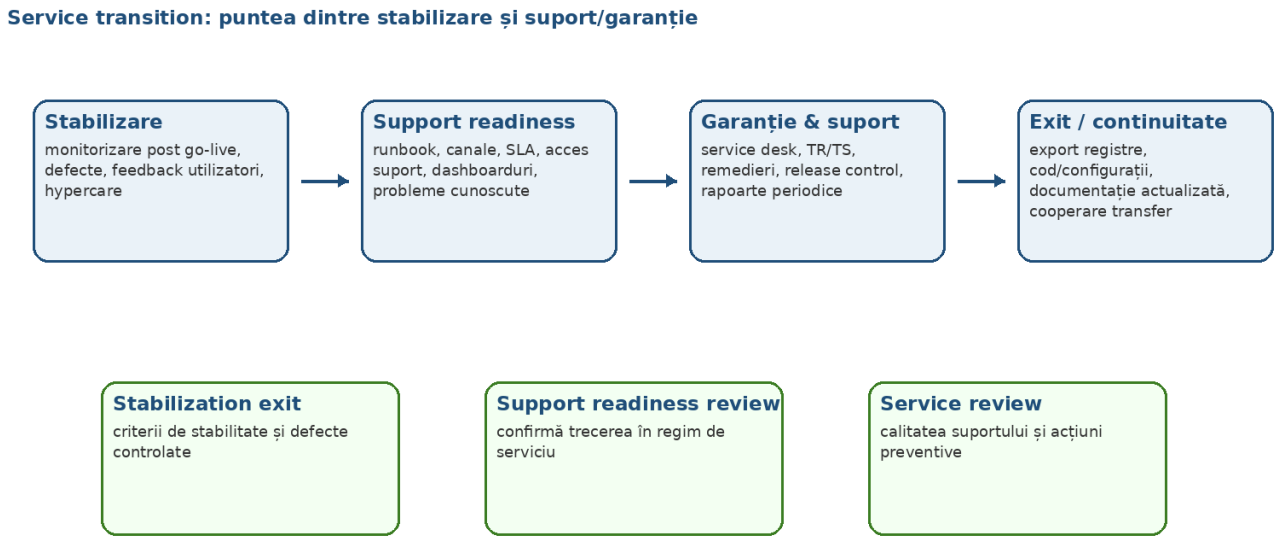


Figura Service transition: stabilizare, readiness, suport și exit

Calitatea suportului, RCA și îmbunătățire continuă

Pentru incidente critice, incidente recurente sau probleme cu impact asupra proceselor CNAS, Furnizorul va realiza analiză de cauză-rădăcină. RCA nu va urmări doar identificarea erorii tehnice, ci și mecanismul de prevenire: test suplimentar, alertă nouă, modificare de documentație, ajustare de configurare, îmbunătățire de monitoring sau acțiune de instruire.

Acțiunile preventive vor fi incluse în raportarea de suport și urmărite până la închidere. Această abordare transformă suportul din reacție la incidente în mecanism de îmbunătățire a exploatării sistemului.

Furnizorul va organiza service review-uri periodice cu CNAS pentru discutarea calității suportului, SLA, incidentelor majore, riscurilor, problemelor recurente, documentației și eventualelor propuneri de îmbunătățire.

Politica de release pentru remedieri și actualizări

Remedierile și actualizările livrate în perioada de suport vor fi gestionate prin release control. Pentru fiecare release se vor pregăti note de versiune, lista solicitărilor incluse, impactul, instrucțiunile de deployment, testele executate, eventualele acțiuni post-deployment și documentația afectată.

Furnizorul va evita intervențiile directe necontrolate în producție. Pentru incidente critice poate fi necesară livrare accelerată, dar chiar și în acest caz se păstrează evidența: ticket, aprobare de urgență, modificare, test minim, deployment, verificare și documentare post-factum.

Actualizările ordinare vor fi grupate pentru a reduce perturbarea operării. Actualizările de securitate sau incidentele critice pot avea traseu accelerat, cu informarea și acordul CNAS conform procedurii agreate.

Exit, transfer și continuitate după suport

La finalul perioadei de suport, CNAS trebuie să poată continua exploatarea sistemului, fie prin prelungirea suportului, fie prin preluare internă, fie prin transfer către un alt regim de mentenanță. Furnizorul va pregăti pachetul de exit astfel încât istoricul suportului, documentația, codul, configurările și versiunile livrate să rămână utilizabile.

Pachetul de exit va include documentația actualizată, exportul registrului solicitărilor, lista incidentelor și problemelor recurente, acțiunile preventive, release notes, codul/configurările aferente modificărilor livrate, instrucțiunile de build/deploy, runbook-ul operațional și recomandările pentru perioada următoare.

Furnizorul va coopera cu CNAS și, dacă este cazul, cu o terță parte autorizată pentru transferul cunoștințelor necesare continuității. Această regulă susține independența instituțională a CNAS și reduce dependența de cunoștințe tacite.

Livrabil / evidență M7	Conținut minim	Rol în acceptanță / continuitate
SLA / model suport	Canale, program, clasificări, TR/TS, escaladare, responsabilități.	Confirmă modul de prestare a suportului.
Registru solicitări / export	Solicitări, status, severitate, acțiuni, termene, închidere.	Demonstrează trasabilitatea serviciilor.
Raport periodic suport	Volum, SLA, incidente majore, riscuri, acțiuni preventive.	Permite monitorizarea calității suportului.
Registru modificări	Modificări, aprobări, versiuni, teste, release notes.	Asigură controlul schimbărilor.
Plan calitate suport	Indicatori, riscuri, prevenție, responsabilități, calendar review.	Acoperă calitatea serviciului.
Pachet handover/exit	Cod, configurări, documentație, export solicitări, cooperare transfer.	Asigură continuitatea dacă suportul nu se prelungește.

Rezultatul livrat către CNAS

Prin modelul propus, CNAS primește un serviciu de suport verificabil: solicitările sunt înregistrate, clasificate, tratate conform SLA, remediate controlat, raportate periodic și închise cu evidențe. Garanția nu rămâne o promisiune; ea este serviciu gestionat, măsurabil și auditat.

Suportul păstrează legătura cu arhitectura, securitatea, migrarea, raportarea, observabilitatea, release control și handover-ul. Fiecare remediere relevantă se leagă de ticket, test, versiune, documentație și confirmare. Fiecare incident major produce lecții operaționale. Fiecare perioadă de raportare arată CNAS calitatea serviciului și zonele care necesită atenție.

Rezultatul final este capacitatea CNAS de a exploata SI „Protecția Socială” fără suport informal, fără remedieri opace și fără dependență de cunoștințe nedeclarate. Furnizorul livrează nu doar un sistem acceptat, ci și mecanismul prin care sistemul rămâne susținut, documentat, transferabil și controlabil pe durata garanției și după aceasta.

15. Proprietate, licențiere, transferabilitate și evitarea dependenței de furnizor

15.1 Rolul secțiunii

Această secțiune stabilește modul în care soluția livrată rămâne controlabilă de CNAS pe termen lung. Pentru un sistem informațional de stat, proprietatea asupra livrabilelor, accesul la cod/configurări, documentația, licențierea componentelor și portabilitatea datelor nu sunt detalii juridice secundare; ele determină capacitatea instituției de a opera, audita, extinde și transfera sistemul după finalizarea proiectului.

Furnizorul va livra sistemul astfel încât CNAS să poată utiliza, verifica, reconstrui, opera, audita, extinde și transfera soluția către echipa proprie sau către alt furnizor autorizat, în limitele contractului și ale regimului de licențiere aplicabil. Această transferabilitate va fi legată de cerințe, UC-uri, shared services, date, documentație, artefacte de deployment și evidențe de acceptanță.

Transferabilitate controlată

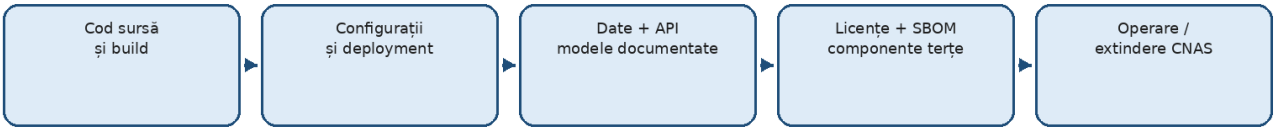


Figura Transferabilitate: sistem predat ca pachet complet, nu ca dependență informală

15.2 Ancorarea transferabilității în cerințe, UC-uri și livrabile

Transferabilitatea nu se rezumă la predarea codului sursă. CNAS trebuie să poată înțelege cum fiecare UC, flux operațional și cerință critică este implementată, testată, documentată și operată. De aceea, pachetul de proprietate și handover va păstra legătura între cerințe/UC-uri, SRS/SDD, cod, API-uri, modele de date, teste, documentație și artefacte de deployment.

Această legătură este esențială pentru mentenanță ulterioară. Dacă un viitor furnizor trebuie să modifice un flux de pensie, un raport statistic, un șablon de decizie sau o integrare, el trebuie să poată identifica cerința, obiectul funcțional, componenta tehnică, contractul API, modelul de date, testele asociate și impactul asupra shared services.

Zonă cerință / UC	Artefacte de transferabilitate	De ce contează pentru CNAS
UC01-UC05: public, dashboard, sarcini	UI shell, componente frontend, API contracts, ghiduri utilizator, teste roluri	permite modificări de interfață/navigare fără rescriere haotică
UC06-UC11, UC21: cereri, dosare, decizii, documente	modele cerere/dosar/decizie, workflow, șabloane, teste UAT, audit trail	permite extinderea serviciilor și păstrarea coerenței deciziilor
Registre, contribuții, cont individual	model date, mapping, reguli, proceduri migrare/reconciliere, teste date	protejează continuitatea evidenței istorice și a calculului drepturilor
UC09/UC19: raportare	catalog rapoarte, catalog indicatori, data marts, snapshot-uri, teste valori control	asigură regenerare și mentenanță raportare fără SQL informal
UC14: interoperabilitate	catalog integrare, OpenAPI/contracte, payload-uri, erori, certificate/acces	permite schimbarea/adaptarea integrărilor fără pierderea trasabilității

Zonă cerință / UC	Artefacte de transferabilitate	De ce contează pentru CNAS
UC15-UC18, UC20-UC23: administrare, workflow, audit	matrice roluri, modele permisiuni, shared services, audit model, runbook	asigură operare sigură și controlată după predare

15.3 Proprietate, licențiere și controlul componentelor terțe

Furnizorul va organiza livrabilele astfel încât acestea să poată fi inventariate, verificate și reutilizate. Proprietatea și drepturile de utilizare asupra livrabilelor vor fi exercitate conform contractului, iar documentul tehnic va distinge clar între componente custom dezvoltate pentru CNAS, componente open-source, biblioteci terțe și eventuale produse comerciale autonome.

Pentru componentele dezvoltate custom, Furnizorul va preda codul sursă, configurările, scripturile, modelele de date, documentația și instrucțiunile necesare pentru build, testare, deployment și mentenanță. Pentru componentele terțe open-source se va preda inventarul componentelor și regimul lor de licențiere. Pentru datele CNAS, controlul instituției va fi păstrat prin modele documentate, exporturi controlate, backup/restore, audit și mecanisme de acces conforme politicilor aprobate.

Stivă standardizată și reducerea lock-in-ului tehnic

Stack-ul asumat utilizează tehnologii open-source, standardizate, larg utilizate și documentate: Java 25 LTS / Spring, React, PostgreSQL, OpenAPI, containerizare, Kubernetes/Helm, CI/CD, instrumente de observabilitate și mecanisme de build/deployment versionate. Această alegere reduce dependența de runtime-uri proprietare obscure, de licențe greu de controlat sau de cunoștințe tacite disponibile doar la Furnizor.

Această poziționare nu elimină responsabilitatea Furnizorului pe durata implementării, garanției și suportului. Ea oferă CNAS o bază tehnică transferabilă: o echipă IT calificată sau un furnizor ulterior poate înțelege, reconstrui și continua sistemul pe baza codului, documentației, testelor, contractelor API, runbook-urilor și artefactelor predate.

Licențiere și controlul componentelor terțe

Furnizorul va menține, în documentația tehnică a soluției, inventarul componentelor terțe open-source utilizate: biblioteci, framework-uri, servicii, instrumente de build/deployment, componente de raportare, pachete frontend/backend și alte dependințe relevante. Inventarul va indica rolul componentei, versiunea, licența, restricțiile și obligațiile asociate, în măsura aplicabilă.

Pentru componentele open-source, Furnizorul va urmări compatibilitatea licențelor cu utilizarea instituțională și cu livrarea codului/documentației către CNAS. Oferta tehnică nu introduce componente comerciale obligatorii și nu presupune costuri de licențiere ascunse pentru stack-ul aplicativ propus.

Tip componentă	Regim de control	Evidență predată
Cod custom CNAS	predare cod sursă, documentație, instrucțiuni build/deploy	repository/export, release tags, build guide
Componente open-source	inventar tehnic al componentelor, versiuni, obligații de licențiere open-source, compatibilitate	SBOM / inventar tehnic al componentelor open-source și al dependențelor
Componente comerciale obligatorii	nu sunt prevăzute în stack-ul aplicativ propus; orice cerință comercială impusă de mediul de exploatare se tratează separat de stack-ul aplicativ	nu se aplică pentru stack-ul aplicativ ofertat; documentare separată doar dacă platforma de exploatare impune componente externe

Tip componentă	Regim de control	Evidență predată
Artefacte deployment	configurații versionate, scripturi, Helm/charts, release notes	deployment package, runbook
Date și documente	modele, exporturi controlate, storage, audit, backup/restore	model date, proceduri export/restaurare

15.4 Proprietate, licențiere, transferabilitate și evitarea dependenței de Furnizor

Arhitectura va fi proiectată astfel încât CNAS să poată deține, opera, reconstrui și întreține sistemul în condițiile contractuale agreate. Codul custom, configurările, scripturile, contractele API, modelele de date, șabloanele, documentația, pipeline-urile și runbook-urile vor fi livrate ca artefacte transferabile, nu ca rezultat dependent de mediul intern al Furnizorului.

Pentru componentele terțe open-source se va menține inventar tehnic de componente, versiuni, licențe, dependențe, limitări și responsabilități de actualizare. Stack-ul aplicației este formulat pe tehnologii open-source, fără licențe comerciale obligatorii, cu documentație disponibilă și competențe pe piață. Componentele utilizate vor fi evidențiate în documentația tehnică și în inventarul de componente al soluției, fără constituirea unui registru separat de licențe în pachetul de ofertă.

Handover-ul nu va însemna transmiterea unei arhive de cod. CNAS va primi repository-uri, istoric, instrucțiuni de build/rebuild, configurații, proceduri de deployment, runbook, catalog de integrare, model de date, catalog rapoarte, ghid de administrare, ghid de dezvoltator și mecanisme de suport pentru transferul de competențe tehnice.

Transfer de competențe tehnice și shadowing pentru echipa IT CNAS

Transferul de proprietate operațională va include sesiuni practice pentru echipa IT CNAS. Furnizorul va organiza parcurgerea arhitecturii, shared services, pipeline-urilor CI/CD, deployment-ului, monitorizării, logurilor, reluării joburilor, backup/restore, catalogului de integrare și mecanismelor de raportare. Echipa CNAS va putea urmări, împreună cu Furnizorul, scenarii reale de operare: aplicarea unui release, investigarea unei erori, reluarea unui job, verificarea unei integrări și restaurarea controlată a unui backup.

Această abordare reduce dependența informală de Furnizor. CNAS nu primește doar cod și documentație, ci înțelegerea practică a modului în care sistemul se operează, se diagnostichează și se dezvoltă în continuare.

15.5 Transfer artefacte, portabilitatea datelor și continuitate

Categorie	Ce se predă / documentează	Conexiune cu cerințele
Cod sursă	repository, versiuni, branch/tag release, instrucțiuni build	UC-uri implementate, defecte remediate, release-uri acceptate
Configurări	parametri, Helm charts, configurări medii, fără secrete în cod	operare MCloud, administrare, CI/CD, security readiness
Baza de date	scripturi migrare, model date, dicționar câmpuri	registre, migrare, reporting, audit
API și integrare	OpenAPI, contracte interne/externe, payload-uri, erori	UC14, integrări guvernamentale, contract tests
Raportare	data marts, snapshot-uri, catalog rapoarte/indicatori, șabloane	UC09/UC19, rapoarte, exporturi
Documentație	SRS, SDD, ghiduri, runbook, proceduri suport	UAT, suport, handover, transferabilitate

Portabilitatea datelor și continuitatea informațională

Datele CNAS vor rămâne accesibile și transferabile prin modele documentate, exporturi controlate și scheme cunoscute. Pentru datele operaționale, istorice și de raportare, Furnizorul va documenta structurile relevante, sursele, indicatorii, snapshot-urile și regulile de generare. Portabilitatea datelor nu înseamnă doar export brut; înseamnă posibilitatea de a înțelege și reconstrui informația într-un mod controlat.

- model de date și dicționar de câmpuri pentru zonele principale;
- documentarea surselor pentru rapoarte, indicatori și snapshot-uri;
- mecanisme de export pentru date și documente, acolo unde sunt agreate;
- audit al generării/transferului datelor;
- proceduri pentru transfer către CNAS sau alt furnizor autorizat.

Exit, transfer către alt furnizor și continuitate post-suport

La încheierea perioadei de suport/garanție sau în cazul transferului către CNAS/un alt furnizor autorizat, Furnizorul va preda pachetul de exit/handover: cod sursă și configurări actualizate, documentație curentă, registru solicitări/incidente/modificări, release notes, situația licențelor, lista problemelor cunoscute, proceduri operaționale și recomandări privind continuitatea suportului.

Transferul va include cooperare rezonabilă pentru clarificarea artefactelor predate, fără a transforma exit-ul într-un nou proiect de dezvoltare. Scopul este ca CNAS să poată continua operarea și mentenanța pe baza pachetului predat, a documentației și a cunoștințelor transferate.

Rezultatul livrat către CNAS

Prin această abordare, CNAS primește mai mult decât dreptul de utilizare a unui sistem. CNAS primește capacitatea documentată de a controla sistemul: cod, configurări, documentație, licențe, date, API-uri, teste, runbook-uri și artefacte de deployment. Evitarea dependenței de furnizor nu este declarată ca principiu abstract; ea este susținută prin livrabile concrete, legate de cerințe, UC-uri și versiuni acceptate.

16. Managementul implementării, metodologie și plan de execuție

Capitolul explică modelul de delivery assurance, functional backbone, shared services și rolul activ al CNAS în implementare.

16.1 Sumar metodologic și principiu de livrare

Furnizorul va aplica pentru SI „Protecția Socială” o metodologie de implementare construită pentru un sistem public critic, cu control formal pe milestone-uri, execuție incrementală în etapa de proiectare și dezvoltare, reutilizare obligatorie a mecanismelor comune și acceptanță pe evidențe. Abordarea respectă structura de implementare cerută pentru CNAS și adaugă mecanisme practice pentru reducerea riscului: incrementuri lunare, CI/CD, design authority, feedback funcțional, data & migration assurance, readiness gates și service transition.

Metodologia este orientată spre progres verificabil. Fiecare increment va produce funcționalitate demonstrabilă, teste executate, documentație actualizată, decizii urmărite, date sau configurări validate și evidențe care pot fi examinate de CNAS. Astfel, progresul proiectului nu va fi raportat doar prin activități efectuate, ci prin rezultate care pot fi verificate în scenarii reale de lucru.

CNAS va exercita rolul de autoritate funcțională și beneficiar operațional al sistemului. Furnizorul va organiza mecanismele de lucru astfel încât CNAS să poată verifica, comenta, solicita clarificări, cere ajustări în limitele contractului, aproba decizii funcționale și confirma readiness-ul etapelor. Această implicare nu este un element opțional al proiectului; este parte a metodei de livrare, deoarece regulile, prioritățile, datele, procesele și acceptanța aparțin autorității contractante.

Element metodologic	Cum funcționează în ofertă	Ce primește CNAS
Waterfall guvernat pe milestone-uri	Etapele, livrabilele, criteriile și acceptanța rămân controlate formal.	Predictibilitate contractuală, gates, documente și procese-verbale de acceptanță.
Execuție incrementală în M2	Proiectarea și dezvoltarea se livrează prin pachete lunare demonstrabile.	Vizibilitate continuă, feedback timpuriu, reducerea acumulării de risc.
Functional Backbone	UC-urile sunt legate prin obiecte comune: cerere, dosar, workflow, decizie, document, audit.	Sistem coerent, nu module izolate care duplică aceleași mecanisme.
Shared Services / Shared Artefacts	Serviciile și artefactele comune sunt livrate ca foundation baseline și extinse prin reutilizare.	Unitate funcțională între contribuții, pensii și beneficii.
Delivery Assurance	Fiecare increment produce evidențe: teste, release, documentație, date, decizii, feedback.	Control real al progresului și suport pentru acceptanță.
Rol activ CNAS	CNAS verifică, comentează, aprobă, prioritizează și confirmă readiness-ul etapelor.	Autoritate funcțională exercitată în proiect, nu așteptare pasivă a rezultatului.

Figura Modelul general al metodologiei propuse

Filozofia de livrare pentru un sistem public critic

Furnizorul va trata SI „Protecția Socială” ca sistem public critic cu efect direct asupra proceselor instituționale ale CNAS, nu ca produs software livrat exclusiv prin componente tehnice. Metodologia de implementare va porni de la faptul că sistemul susține evidența contribuțiilor, persoane asigurate, cont individual, pensii, prestații, decizii, plăți, raportare, interoperabilitate, audit și suport operațional. În consecință, finalizarea unei funcționalități nu va fi considerată suficientă doar prin existența codului sau a ecranului aferent; ea va fi demonstrată prin comportament funcțional, date, documente, audit, testare și capacitate de operare.

Furnizorul va transforma cerințele caietului de sarcini, cazurile de utilizare, anexele funcționale, cerințele de migrare, cerințele de interoperabilitate și cerințele de suport într-un sistem verificabil. Această transformare va fi controlată prin livrabile formale, decizii documentate, registre operaționale, incrementuri lunare în M2 și evidențe pregătite pentru verificarea CNAS. Obiectivul metodologic este ca fiecare etapă să reducă ambiguitatea și să crească nivelul de certitudine asupra sistemului livrat.

Metodologia nu promite eliminarea tuturor clarificărilor înainte de dezvoltare, deoarece într-un sistem CNAS de această dimensiune unele detalii funcționale, de date sau de integrare se confirmă prin analiză, prototipare, testare și feedback instituțional. În schimb, Furnizorul va controla clarificările printr-o disciplină de decizie: fiecare interpretare relevantă va fi legată de cerință, impact, opțiune recomandată, decizie CNAS, implementare și testare. Astfel, flexibilitatea necesară proiectului nu se transformă în schimbare necontrolată.

Principiul metodologic asumat

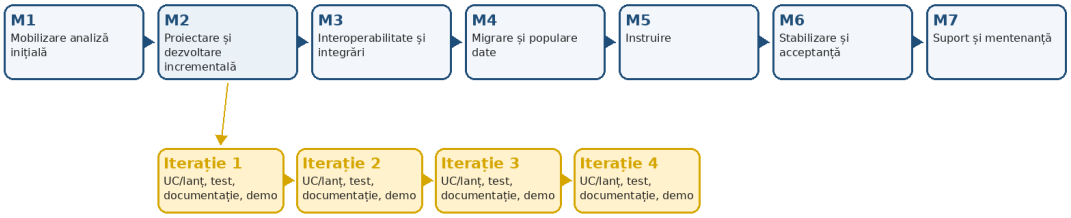
Furnizorul va guverna proiectul prin milestone-uri, livrabile formale, criterii de acceptanță și decizii documentate. Această structură asigură controlul cerut pentru un sistem public critic și permite CNAS să urmărească fiecare etapă prin documente, demonstrații, teste, rapoarte și evidențe.

În Milestone 2, proiectarea și dezvoltarea vor fi executate incremental, prin pachete lunare de lucru. Fiecare pachet va include clarificarea cerințelor, dezvoltarea componentelor, testare internă, actualizarea documentației tehnice, pregătirea artefactelor de release și prezentarea incrementului. Incrementurile lunare nu înlocuiesc acceptanța formală a milestone-urilor; ele creează vizibilitate, reduc riscul și permit intervenția timpurie a CNAS asupra direcției funcționale.

Prin această formulă, Furnizorul păstrează controlul Waterfall la nivel de guvernanță și acceptanță, iar în interiorul etapei de dezvoltare livrează incremental, cu CI/CD, feedback funcțional și readiness gates. Abordarea evită atât dezvoltarea opacă până la final, cât și schimbarea necontrolată a metodologiei contractuale.

În această ofertă, „readiness gate” înseamnă un punct formal de trecere între etape sau subetape. Trecerea se face numai când există evidențe suficiente: documente aprobate, componente dezvoltate, teste executate, defecte controlate, date validate, utilizatori pregătiți sau suport operațional activat, după caz.

Waterfall guvernat pe milestone-uri, cu execuție incrementală în M2



Pentru a face vizibilă relația dintre controlul contractual și livrarea incrementală, Furnizorul va utiliza o planificare în două niveluri. Primul nivel este cel al milestone-urilor contractuale, prin care se păstrează guvernanța formală a proiectului, livrabilele, criteriile de acceptanță și procesele-verbale aferente. Al doilea nivel este cel al incrementurilor lunare din Milestone 2, prin care proiectarea și dezvoltarea produc rezultate verificabile înainte de acceptanța finală a etapelor.

Această separare permite CNAS să urmărească progresul real fără a pierde controlul formal al contractului. Incrementurile lunare nu înlocuiesc acceptanța contractuală și nu fragmentează responsabilitatea Furnizorului. Ele oferă vizibilitate timpurie asupra funcționalităților, shared services, documentației, testelor și observațiilor CNAS, astfel încât riscurile să fie identificate și tratate înainte de acumularea lor în etapele finale.

Figura următoare prezintă modul în care milestone-urile, incrementurile M2, mecanismele Shared Services/Foundation, feedback-ul CNAS și evidențele de control funcționează împreună în cadrul aceleiași metode de livrare.

Etapă / mecanism	M1 Mobilizare	M2 Incrementuri lunare	M3 Integrare	M4 Migrare	M5 Instruire	M6 Stabilizare	M7 Suport
Waterfall - control contractual	Gate inițial	Livrabile intermediare	Acceptanță integrare	Acceptanță date	Acceptanță instruire	Acceptanță finală	SLA / rapoarte
Incrementuri M2		M2.1 | M2.2 | M2.3 | ... | M2.n					
Shared Services / Foundation	setup	baseline + extindere	stabilizare contracte	utilizare migrare	suport training	operare	mentenanță
Feedback CNAS	guvernanță	review lunar / Model Office	validare efect funcțional	decizii excepții	validare utilizatori	readiness	suport
Evidențe	registre	release, teste, SRS/SDD	loguri, contracte	reconciliere	training evidence	checklist	service reports

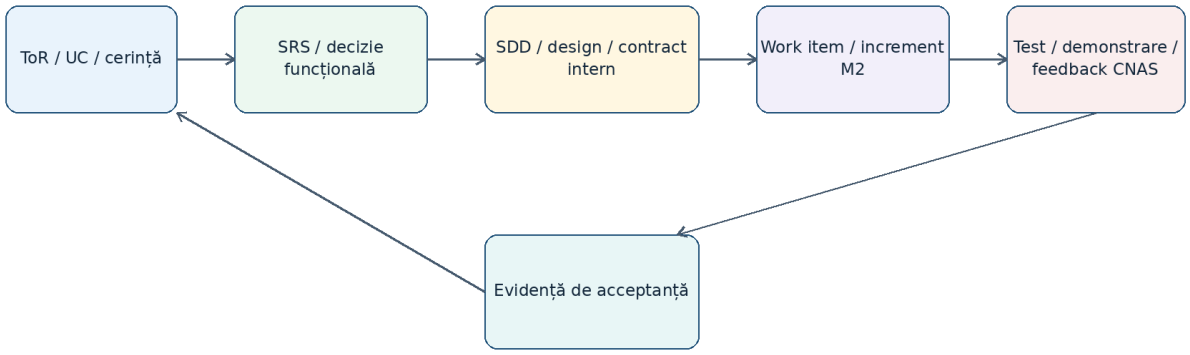
Cadrul conceptual al metodologiei

Metodologia propusă va funcționa pe mai multe straturi active pe toată durata proiectului. Aceste straturi nu sunt capitole teoretice, ci mecanisme de lucru prin care Furnizorul va organiza execuția, va gestiona dependențele și va pregăti acceptanța. Ele permit menținerea controlului Waterfall pe milestone-uri, fără a bloca livrarea incrementală din M2.

Strat metodologic	Rol în implementare	Evidență produsă
Stratul funcțional	Transformă UC-urile și anexele CNAS în lanțuri operaționale: cerere, dosar, decizie, plată, raportare și audit.	scenarii funcționale, backlog de increment, mapping UC-lanțuri, demonstrații
Stratul de trasabilitate	Leagă cerințele de SRS/SDD, work items, teste, defecte, decizii și acceptanță.	matrice de conformitate, registru cerințe, test cases, evidence log
Stratul de guvernanță	Separă responsabilitățile CNAS și ale Furnizorului și păstrează deciziile importante vizibile.	decision log, minute, issue/risk register, dependency board
Stratul shared services	Asigură reutilizarea obiectelor comune: cereri, decizii, workflow, documente, audit, notificări, interop.	catalog shared artefacts, contracte interne, API standards, componente comune
Stratul de date și migrare	Controlează calitatea datelor, mapping-ul, rulările de migrare și reconcilierea.	profilare date, mapping, rapoarte de reconciliere, error bucket, sign-off
Stratul de calitate și securitate	Integrează testarea, review-ul, autorizarea, auditul și privacy by design în fiecare increment.	rapoarte QA, test results, defect log, security checks
Stratul de operare și handover	Pregătește sistemul pentru utilizare, suport, mentenanță și transfer către CNAS.	runbook, ghiduri, training evidence, service desk setup, release notes

Prin această structură, proiectul rămâne controlabil fără a deveni rigid. Furnizorul va putea livra incremental și va putea integra feedback-ul CNAS, dar fiecare ajustare relevantă va rămâne legată de cerință, impact, decizie, testare și evidență.

Cerință → implementare → evidență → acceptanță



Registrul de trasabilitate leagă fiecare element de cerință, design, implementare, test, defect și decizie CNAS.

16.2 Guvernanță, rol CNAS, RACI și mecanisme de decizie

CNAS va fi tratată în cadrul implementării ca autoritate funcțională asupra proceselor, datelor și regulilor instituționale. Furnizorul va livra analiza, soluția tehnică, implementarea și evidențele; CNAS va valida sensul business, prioritățile, regulile, scenariile, datele, excepțiile și acceptanța. Această separare este esențială: Furnizorul nu va presupune unilateral reguli instituționale acolo unde este necesară decizia autorității contractante.

Metoda de lucru va include ferestre formale de review, ședințe de clarificare, decision log, registru de observații, mecanism de răspuns la comentarii, prioritizare a defectelor și confirmarea readiness-ului pe etape. În acest mod, CNAS poate cere clarificări, insista asupra corectării deviațiilor, solicita ajustări în limitele contractului, valida excepții de date și aproba interpretări funcționale.

Implicarea CNAS va fi planificată astfel încât să nu devină blocaj informal. Furnizorul va pregăti materialele de decizie, variantele de flux, impactul schimbărilor, evidențele de testare și recomandările tehnice. CNAS va putea decide informat, pe baza efectului asupra proceselor instituționale, datelor, utilizatorilor și acceptanței.

Mecanism	Rolul Furnizorului	Rolul CNAS
Review SRS/SDD	Pregătește documentele, explică opțiunile, urmărește observațiile.	Validează fluxurile, regulile, datele, rolurile și scenariile relevante.
Model Office / demonstrații	Prezintă incrementuri pe scenarii reprezentative și date controlate.	Testează, comentează, confirmă utilitatea operațională sau solicită ajustări.
Decision log	Documentează decizii, alternative, impact și responsabilități.	Aprobă interpretările funcționale și prioritățile care aparțin autorității.
Readiness gates	Pregătește evidențe și checklisturi pentru trecerea între etape.	Confirmă că sunt îndeplinite condițiile funcționale, operaționale și de acceptanță.
Gestionarea schimbărilor	Evaluează impactul tehnic, calendaristic și de testare.	Decide asupra schimbărilor de scop, priorității și acceptabilității operaționale.

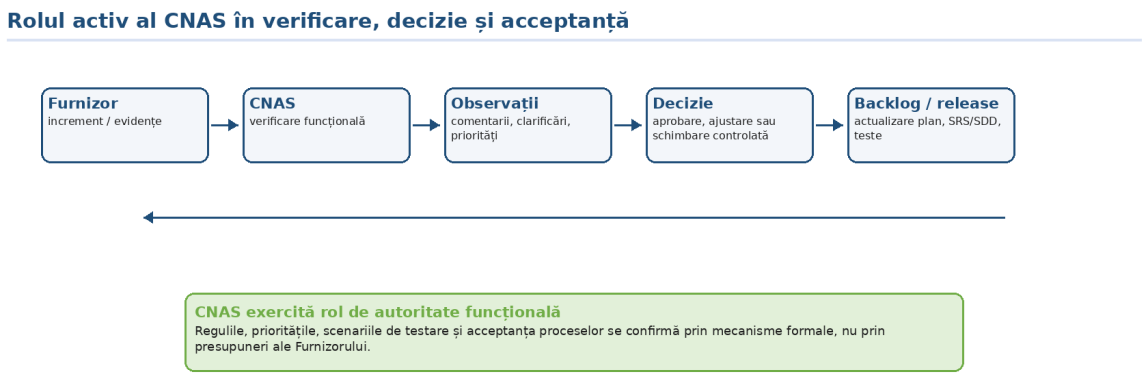


Figura CNAS ca autoritate funcțională activă în verificare, decizie și acceptanță

RACI operațional și efort CNAS

Furnizorul va organiza implicarea CNAS ca activitate planificată și gestionată, nu ca solicitare ad-hoc de disponibilitate. Pentru fiecare etapă relevantă, Furnizorul va indica tipul de participare necesară, materialele de intrare, termenul de review, deciziile așteptate și impactul întârzierii. Această abordare permite CNAS să

își aloce experții funcționali, tehnici și decizionali fără a transforma validarea într-un blocaj informal al proiectului.

RACI-ul operațional va fi utilizat pentru activitățile cu impact asupra cerințelor, datelor, fluxurilor, migrației, UAT-ului, go-live-ului și acceptanței. Furnizorul rămâne responsabil pentru pregătirea materialelor, analiza impactului, implementare, testare și evidențe. CNAS exercită rolul de autoritate funcțională asupra proceselor, datelor, priorităților și acceptanței. Acolo unde o decizie aparține CNAS, Furnizorul va prezenta opțiuni clare, recomandare, impact și termen de răspuns.

Pentru planificarea realistă a proiectului, Furnizorul va propune o estimare de efort CNAS pe tipuri de activități. Estimarea va fi confirmată în etapa de mobilizare și ajustată în funcție de calendarul aprobat, disponibilitatea experților și criticitatea fluxurilor.

Activitate	Rol Furnizor	Rol CNAS	Efort orientativ CNAS
Review SRS/SDD	Pregătește documente, matrice, variante și impact.	Validează procese, date, roluri, reguli și observații.	2-4 ore/săptămână per expert de domeniu în perioadele active de review.
Workshop UC / fluxuri	Moderează, documentează decizii, actualizează artefacte.	Explică regulile, excepțiile și practica operațională.	Sesiuni de 1.5-2 ore, planificate pe domenii.
Model Office / demo lunar	Prezintă scenarii, build, release notes și test evidence.	Testează utilitatea operațională și formulează observații.	1 sesiune lunară per flux activ, plus timp pentru observații.
Migrare și data quality	Prezintă profiling, mapping, erori, reconciliere.	Decide asupra interpretării datelor și excepțiilor.	Efort variabil; intens în profiling, mapping și dress rehearsal.
UAT	Pregătește mediu, scenarii, date, suport și defect log.	Execută/confirmă scenarii și semnează rezultatele.	Efort concentrat pe ferestre UAT aprobate.
Readiness / go-live	Pregătește checklist, runbook, training și support readiness.	Confirmă condițiile de lansare și observațiile finale.	Sesiuni formale de readiness, cu decidenți desemnați.

Valorile de efort sunt orientative și nu introduc obligații suplimentare față de contract. Ele ajută la planificarea realistă a implicării instituționale și la prevenirea blocajelor de validare.

Furnizorul va organiza procesul de review și decizie astfel încât implicarea activă a CNAS să susțină proiectul fără a deveni blocaj informal. Pentru documente, incrementuri, decizii de design, excepții de date și readiness gates vor fi propuse ferestre de review agreate în planul de lucru. Aceste ferestre nu limitează autoritatea CNAS, ci fac vizibil impactul timpului de răspuns asupra calendarului, dependențelor și acceptanței.

Dacă o observație, decizie sau validare nu poate fi obținută în termenul agreat, Furnizorul va marca subiectul ca dependență deschisă, va propune opțiuni de continuare și va escalada decizia către nivelul de guvernanță corespunzător. Echipele vor continua activitățile neafectate, iar activitățile dependente vor fi replanificate sau executate pe ipoteze documentate numai dacă acest mecanism este acceptat de CNAS și nu afectează drepturile, datele, securitatea, migrarea sau acceptanța.

Aprobarea tacită nu va fi utilizată ca substitut pentru deciziile funcționale critice. Pentru reguli instituționale, fluxuri, date, excepții, securitate, migrare, UAT și go-live, decizia CNAS va rămâne explicită. Pentru elementele administrative sau tehnice fără impact funcțional major, procedura de lucru poate prevedea termene de review și mecanisme de escaladare, astfel încât proiectul să nu fie blocat de lipsa unui răspuns punctual.

Tip subiect	Fereastră de review recomandată	Dacă nu există răspuns	Ce nu se aprobă tacit
Document SRS/SDD sau capitol major	termen agreat în planul de lucru	open point + escaladare + replanificare impact	fluxuri, reguli, roluri, date critice
Increment lunar / Model Office	review în fereastra incrementului	feedback log deschis + continuare pe elemente neafectate	acceptanță funcțională finală
Excepție de date / migrare	înainte de rularea următoare relevantă	marcare ca risc și blocaj de migrare	corecții cu efect juridic/financiar
Decizie tehnică fără impact funcțional major	termen scurt agreat	continuare pe ipoteză documentată, dacă procedura permite	securitate, acces, date personale, go-live
Readiness gate	în ședință formală de readiness	gate rămâne deschis până la clarificare	trecerea între etape critice

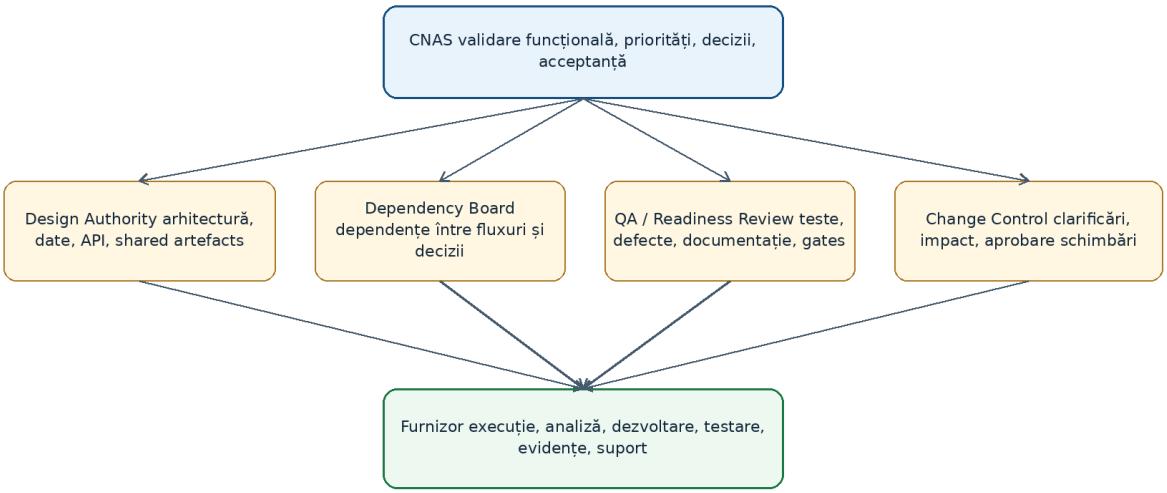
Model de guvernanță și responsabilități operaționale

Furnizorul va opera proiectul printr-un model de guvernanță care păstrează CNAS în poziția de autoritate funcțională asupra proceselor, datelor, priorităților și acceptanței, iar Furnizorul în poziția de responsabil pentru analiză, proiectare, implementare, testare, documentare, evidențe și pregătirea livrabilelor. Această separare protejează proiectul de două riscuri: decizii tehnice luate fără sens instituțional și decizii funcționale luate fără înțelegerea impactului tehnic.

Furnizorul va pregăti pentru CNAS opțiuni de implementare, explicații privind impactul, variante de flux, consecințe asupra datelor, dependențe, riscuri și recomandări tehnice. CNAS va putea valida sensul funcțional, confirma priorități, cere ajustări în limitele contractuale, decide asupra excepțiilor de date și aproba readiness-ul etapelor. Această colaborare nu va fi tratată ca interacțiune informală, ci ca mecanism de control al livrării.

Componentă de guvernanță	Rol principal	Participare CNAS	Evidență / rezultat
Steering / coordonare de proiect	urmărește milestone-uri, riscuri majore, blocaje, dependențe și acceptanță	confirmă priorități, escaladează decizii, aprobă direcții majore	minute, decizii, status report, risk register
Design Authority	controlează arhitectura funcțională/tehnică, shared artefacts și standardele comune	validează opțiuni cu impact funcțional și efect asupra operării CNAS	decision log, design notes, impact assessment
Dependency Board	urmărește dependențele între contribuții, pensii, beneficii, interop, migrare și raportare	prioritizează blocajele funcționale și confirmă secvențierea livrării	dependency board, action log
QA / Readiness Review	verifică dacă incrementul/livrabilul are teste, documentație, defecte controlate și evidențe	verifică demonstrarea funcțională și formulează observații	readiness checklist, test report, feedback log
Change Control	separă clarificările de schimbările de scope și evaluează impactul	decide asupra schimbărilor cu impact pe obiect, prioritate sau acceptanță	change request, impact analysis, approval record

Guvernanță și control: CNAS ca autoritate funcțională activă



Furnizorul pregătește opțiuni, impact și evidențe; CNAS decide asupra sensului funcțional, priorităților și acceptanței.

16.3 Delivery Assurance: cerințe, trasabilitate, incrementuri și Model Office

Furnizorul va aplica un model de asigurare a livrării prin care fiecare increment, milestone și tranziție operațională produce evidențe verificabile. Progresul va fi prezentat ca rezultat controlabil: UC-uri sau părți de lanț funcțional implementate, teste executate, defecte închise sau justificate, documentație actualizată, date validate, configurări aplicate, release package pregătit și feedback CNAS tratat.

Acest model permite CNAS să urmărească starea proiectului pe mai multe axe: cerințe, UC-uri, lanțuri operaționale, shared services, migrare, integrare, securitate, documentație, instruire și suport. Astfel, raportarea de progres nu se reduce la procent estimativ de dezvoltare, ci arată ce poate fi demonstrat, verificat și acceptat.

Furnizorul va menține registre operaționale pentru cerințe/UC-uri, decizii, riscuri, dependențe, defecte, schimbări, date/migrare, release-uri și observații CNAS. Aceste registre vor susține trasabilitatea între cerință, implementare, testare, demonstrare și acceptanță.

„Delivery Assurance Model” este denumirea folosită în această ofertă pentru ansamblul mecanismelor prin care Furnizorul dovedește progresul: registre, teste, release-uri, documentație, demonstrații, feedback CNAS și gates. Termenul nu introduce o metodologie separată, ci descrie controlul livrării.

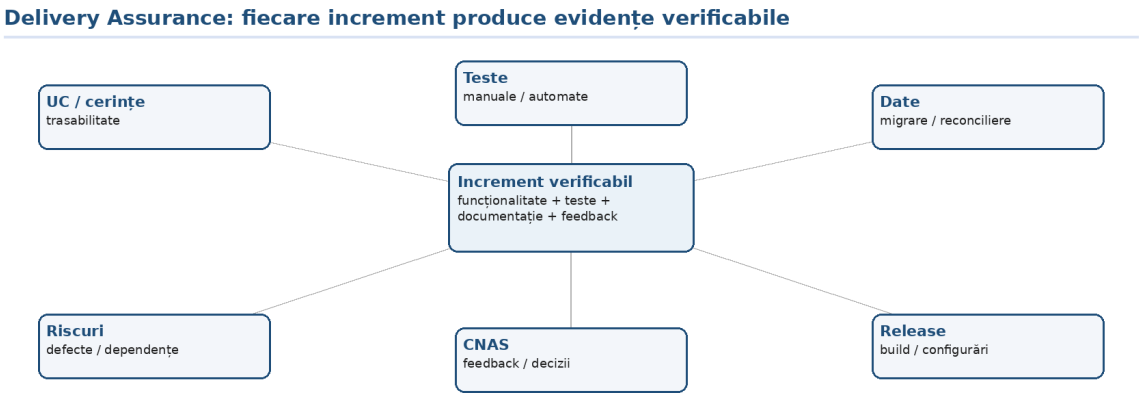


Figura Delivery Assurance: fiecare increment produce evidențe verificabile

Furnizorul va include anexele funcționale ale Caietului de sarcini în modelul de Delivery Assurance. Procesele și scenariile descrise în anexele ToR vor fi tratate ca input activ pentru SRS, SDD, modelul de date, catalogul de API-uri, catalogul de rapoarte, catalogul de șabloane, registrul de migrare, scenariile de testare și UAT pack-ul. Ele nu vor fi procesate doar la nivel de confirmare generală în matricea de conformitate.

Pentru fiecare proces relevant, Furnizorul va urmări minimum următoarele elemente: domeniul operațional, actorii, obiectele informaționale, regulile principale, datele de intrare, rezultatul operațional, documentele generate, integrările implicate, auditul necesar, scenariile de testare și evidența de acceptanță. Această structură permite CNAS să verifice că anexele au fost transformate în soluție implementabilă, nu doar citate în ofertă.

Pe parcursul proiectului, registrul proceselor/scenariilor va deveni instrument de lucru pentru clarificări, proiectare și acceptanță. Atunci când un proces din anexă ridică o ambiguitate, aceasta va fi înregistrată ca open point sau decizie funcțională, cu impact asupra SRS/SDD, datelor, workflow-ului, testării și acceptanței. Astfel, procesele complexe din anexele caietului nu se pierd în documente descriptive, ci intră în mecanismul controlat de livrare.

Metodologia de livrare ca task narative

Furnizorul va trata planul de lucru ca o succesiune de activități care pregătesc una pe alta, nu ca listă de sarcini tehnice independente. Fiecare activitate va reduce o incertitudine și va produce o evidență utilizabilă în activitatea următoare. Această logică este importantă pentru SI „Protecția Socială”, deoarece dezvoltarea funcțională depinde de decizii asupra datelor, workflow-urilor, integrărilor, migrației, rapoartelor și modului de operare.

Mobilizarea va stabili guvernanța, canalele de comunicare, registrele de lucru, calendarul de review, modelul de raportare și modul de escaladare. Analiza va transforma cerințele și UC-urile în fluxuri, reguli, date, obiecte comune și scenarii de testare. Proiectarea va produce SRS/SDD, model de date, model de securitate, design de integrare, design de migrare, shared artefacts și regulile de release. Dezvoltarea va livra incremental funcționalități demonstrabile, pe același nucleu comun. Testarea va produce evidențe înainte de demonstrare, nu după feedback-ul CNAS. UAT-ul va confirma scenarii complete, nu doar ecrane. Go-live-ul va fi pregătit prin readiness gates, nu prin decizie tehnică de instalare.

Pentru fiecare pachet de lucru lunar din M2, Furnizorul va aplica un ciclu repetabil: selectarea pachetului, confirmarea cerinței și a dependențelor, proiectare detaliată, implementare, testare internă, actualizarea

documentației, generarea artefactelor de release, demonstrarea pe scenarii, înregistrarea feedback-ului CNAS și includerea observațiilor în backlog/registru de clarificări. Acest ciclu asigură progres real fără a transforma incrementurile în acceptanță formală prematură.

Trasabilitatea cerințelor și răspunsul la UC-uri

Furnizorul va utiliza matricea de conformitate ca instrument activ de execuție, nu doar ca anexă de ofertă. Fiecare cerință funcțională, UC, cerință non-funcțională, cerință de migrare, cerință de integrare, livrabil și condiție de suport va fi legată de artefacte de proiectare, pachete de lucru, teste și evidențe. Această trasabilitate permite CNAS să verifice unde se află fiecare cerință în ciclul de implementare și ce probă susține conformitatea.

Pentru UC-uri, Furnizorul va menține două niveluri de trasabilitate. Primul nivel va arăta acoperirea formală a fiecărui UC: ecran, API, workflow, roluri, date, documente și teste. Al doilea nivel va arăta cum UC-ul funcționează în lanțuri operaționale: de exemplu, dashboardul conduce la sarcină, sarcina la cerere/dosar, dosarul la verificare, verificarea la decizie, decizia la document/notificare/plată/raportare și audit. Astfel, UC-ul rămâne verificabil contractual, iar sistemul rămâne demonstrat ca mecanism operațional.

Element sursă	Artefact de proiectare	Execuție	Verificare	Acceptanță / evidență
ToR / UC / anexă	SRS, flux, wireframe, model date, reguli	work item, componentă, configurare	test funcțional, test rol, test regresie	test report, demo, feedback CNAS, sign-off
Integrare externă	catalog integrare, contract, mapping, erori	adaptor, gateway, snapshot, log	contract test, timeout/retry, scenariu negativ	raport integrare, log audit, evidență schimb date
Migrare date	mapping, reguli transformare, reconciliere	staging, import, error bucket	rulare pilot, comparație, excepții	raport reconciliere, decizie CNAS asupra excepțiilor
Raport / document	dataset, șablon, drepturi, output	Jasper/template, export, audit	generare, verificare valori, acces	catalog rapoarte, output validat, audit export
Security / privacy	model roluri, permisiuni, segregare	backend authorization, log minimizat	test acces, test caz negativ	security readiness evidence, audit trail

Requirements Traceability Management în instrument de lucru

Furnizorul va menține trasabilitatea cerințelor într-un instrument de lucru utilizat pe durata implementării, de tip Jira, Azure DevOps sau echivalent agreat cu CNAS. Matricea de conformitate va rămâne documentul formal de ofertă și acceptanță, iar instrumentul operațional va permite urmărirea zilnică a fiecărei cerințe, UC, defect, decizie, test și release.

Fiecare cerință relevantă va avea identificator, sursă, status, owner, legătură către SRS/SDD, work items, componente, teste, defecte, release și evidență de acceptanță. Astfel, CNAS poate verifica nu doar dacă o cerință a fost declarată conformă, ci unde se află în execuție, ce test o acoperă, ce defecte o afectează și în ce versiune a fost livrată.

Cerință / UC	Artefact proiectare	Work item	Cod / Configurare	Test	Evidență / Acceptanță
ToR / anexă / UC	SRS / SDD / flux / model date	ticket în tool	commit / PR / release	test case / rezultat	demo / report / sign-off

Element urmărit	Conținut minim în instrument
Cerință / UC	ID unic, sursă ToR, status, prioritate, legătură cu SRS/SDD.
Work item	activitate de analiză, proiectare, dezvoltare, testare sau documentare.
Test case	scenariu care confirmă comportamentul cerut, inclusiv cazuri negative.
Defect / issue	abatere de la cerință, design, criteriu de acceptanță sau rezultat așteptat.
Release	versiunea în care cerința este livrată, testată și demonstrată.
Evidence item	raport de test, demo script, output, log, decizie CNAS sau sign-off.

16.4 Execuție pe fluxuri: Functional Backbone, Shared Services, migrare, integrare, testare

Furnizorul va construi funcționalitatea în jurul unui backbone funcțional comun. Acesta leagă cazurile de utilizare din Caietul de sarcini într-un comportament operațional coerent și permite ca obiectele recurente ale CNAS să fie implementate unitar: cerere, dosar/caz, sarcină, workflow, verificare, integrare, calcul sau regulă de domeniu, decizie, drept sau efect operațional, document, notificare, plată când documentul sau procesul o solicită, raportare și audit.

Backbone-ul nu înlocuiește UC-urile. UC-urile rămân unitățile formale de verificare funcțională. Backbone-ul arată cum aceste UC-uri lucrează împreună în exploatare. O cerere de pensie și o cerere de beneficiu pot avea reguli și formulare diferite, dar folosesc aceleași mecanisme comune pentru solicitant, documente, sarcini, statusuri, decizie, notificare și audit. Această abordare reduce duplicarea și crește coerența sistemului.

Furnizorul va utiliza backbone-ul pentru proiectarea scenariilor de demonstrare și UAT. Testarea nu se va limita la confirmarea fiecărui UC izolat, ci va verifica lanțurile instituționale: date intrate în sistem, verificare, calcul, decizie, document, notificare, efect asupra plății sau raportării și audit.

„Functional Backbone” este axa funcțională comună a sistemului: setul de obiecte și mecanisme care apar în mai multe domenii CNAS. Termenul este folosit pentru claritate metodologică; în implementare el se va concretiza în modele de date, servicii, workflow-uri, API-uri, șabloane și scenarii de testare.

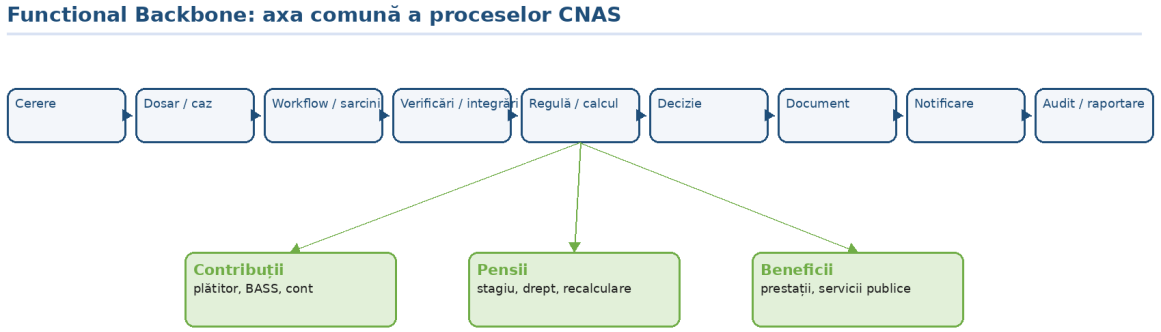


Figura Functional Backbone: obiecte comune și reguli specifice de domeniu

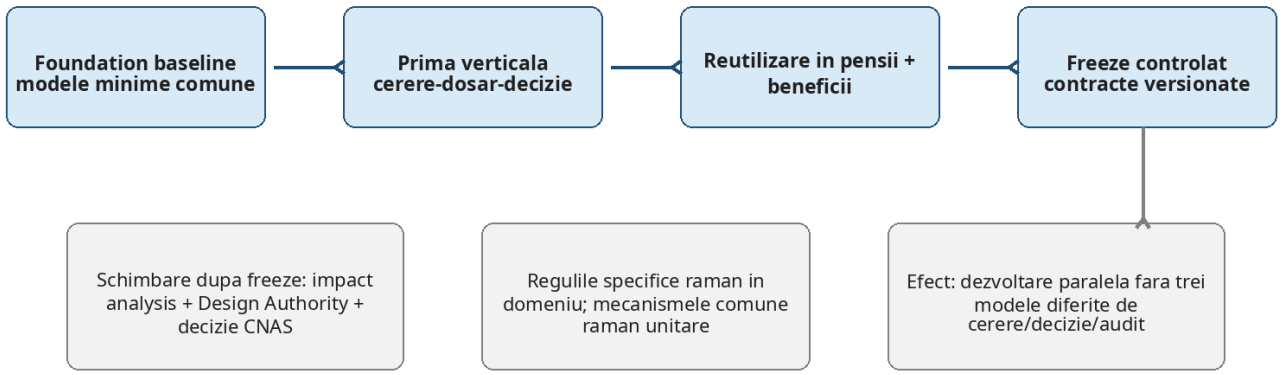
Furnizorul va stabiliza devreme nucleul funcțional comun al sistemului, astfel încât fluxurile dezvoltate ulterior pentru contribuții, pensii și beneficii să nu creeze variante paralele ale aceloraşi obiecte. Cererea, dosarul, decizia, sarcina, workflow-ul, documentul, notificarea, auditul și raportarea vor avea modele comune inițiale, validate printr-o primă verticală funcțională și extinse apoi prin reutilizare controlată în domenii.

Această stabilizare nu va bloca dezvoltarea funcțională prin proiectarea excesivă a unei platforme abstracte. Furnizorul va livra un foundation baseline suficient pentru primele fluxuri verticale, apoi va maturiza backbone-ul pe baza utilizării reale în domenii. După validarea inițială, modificările asupra obiectelor comune vor fi gestionate prin Design Authority, impact analysis, versionare și decizie CNAS atunci când schimbarea afectează procesul, datele sau acceptanța.

Prin acest mecanism, proiectul evită două riscuri opuse: un nucleu comun definit prea târziu, care permite fragmentarea modulelor, și un nucleu comun proiectat prea amplu înainte de a fi testat funcțional. CNAS primește astfel un sistem unitar, dar nu rigid: componentele comune rămân controlate, iar regulile specifice contribuțiilor, pensiilor și beneficiilor rămân implementate în domeniile lor.

Element al backbone-ului	Moment de stabilizare	Cum evoluează ulterior	Control necesar
Cerere / dosar / decizie	Foundation baseline + prima verticală demonstrativă	Extindere pe tipuri de servicii și reguli specifice	Design Authority + validare CNAS pentru impact funcțional
Workflow / sarcini / dashboard	După demonstrarea primului flux end-to-end	Adăugare de stări, tranziții, termene și cozi specifice	Teste de regresie pe lanțuri și verificare roluri
Documente / șabloane / notificări	Înainte de decizii oficiale și comunicări către utilizatori	Versionare șabloane și adaptare pe tip de drept/serviciu	Guvernanță șabloane + audit export/generare
Audit / jurnal evenimente	Din primul increment funcțional	Extindere cu evenimente business specifice domeniului	Reguli comune de audit și acces la jurnal
API-uri interne / contracte shared	Înainte de dezvoltarea paralelă extinsă	Versionare și compatibilitate controlată	Contract review + impact analysis

Stabilizarea Functional Backbone fara blocarea dezvoltarii



Organizarea execuției pe fluxuri funcționale paralele

Furnizorul va organiza execuția pe fluxuri funcționale paralele pentru a permite progres real în Milestone 2 fără a transforma sistemul într-o colecție de module izolate. Fluxurile vor reflecta domeniile naturale ale SI „Protecția Socială”: contribuții, plătitori, persoane asigurate și cont individual; pensii, drepturi, calcul și decizii; beneficii/prestații, cereri, examinare, decizii și plăți specifice.

Fluxurile de domeniu vor utiliza același nucleu comun pentru identitate, roluri, workflow, sarcini, documente, șabloane, notificări, audit, integrare, raportare și CI/CD. În acest mod, dezvoltarea poate avansa în paralel, dar sistemul rămâne unitar pentru utilizator, administrator, auditor și echipa de suport.

Furnizorul va coordona dependențele dintre fluxuri prin guvernanță funcțională și tehnică. Fluxul de pensii depinde de contul individual și datele contributive; beneficiile pot utiliza aceleași mecanisme de cerere, dosar, decizie și notificare; raportarea poate traversa mai multe domenii. Aceste dependențe vor fi vizibile în dependency board și tratate înainte de a afecta calendarul sau acceptanța.

Flux de lucru	Responsabilitate principală	Dependențe controlate prin platformă
Contribuții, plătitori, persoane asigurate și cont individual	Date contributive, relația plătitor-persoană, contribuții BASS, cont individual, surse externe relevante.	Model comun de persoană, audit, Integration Gateway, raportare, CI/CD, date istorice.
Pensii, drepturi, calcul și decizii	Cereri de pensie, dosare, condiții, stagiu, calcul, decizie, drept, recalculare.	Cont individual, workflow, documente, notificări, plăți, audit, șabloane.
Beneficii/prestații și servicii publice	Cereri, verificări, decizii, prestații, documente și plăți specifice.	Workflow comun, șabloane, integrări, notificări, raportare, audit.
Platformă comună și administrare globală	Roluri, permisiuni, workflow framework, nomenclatoare, Jasper, audit, CI/CD, standarde API/UI.	Toate fluxurile de domeniu; controlează reutilizarea și excepțiile.

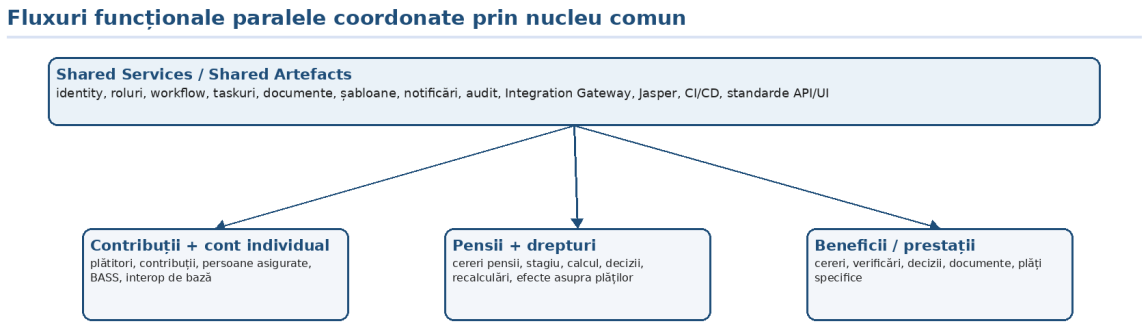


Figura Fluxuri funcționale paralele coordonate prin nucleu comun

Shared Services, Shared Artefacts și reutilizare controlată

Furnizorul va livra un nucleu comun de servicii și artefacte reutilizabile pentru obiectele și mecanismele care trebuie gestionate unitar indiferent de domeniu. Cererile, dosarele, deciziile, sarcinile, workflow-urile, documentele, notificările, șabloanele, auditul, nomenclatoarele, integrările și rapoartele nu vor fi inventate separat în contribuții, pensii și beneficii.

Abordarea este similară cu un design system în frontend, dar aplicată la nivel funcțional și backend. La nivel UI, aceleași componente vizuale asigură consistență. La nivel de sistem CNAS, aceleași obiecte și servicii

comune asigură consistența proceselor: aceeași logică de sarcină, același model de document, același audit, același mod de notificare și aceeași guvernanță a șabloanelor.

Furnizorul va evita două riscuri opuse. Primul risc este blocarea dezvoltării prin proiectarea unei platforme generice complete înainte de funcțional. Al doilea risc este dezvoltarea rapidă, dar fragmentată, în care fiecare flux își creează propriile mecanisme. Răspunsul de implementare este livrarea incrementală a nucleului comun: foundation baseline, prima verticală demonstrativă, reutilizare în mai multe domenii și stabilizare versionată a artefactelor comune.

„Shared Services” sunt servicii runtime comune, de exemplu workflow, documente, notificări, audit sau Integration Gateway. „Shared Artefacts” sunt modele, contracte, șabloane și convenții comune, de exemplu modelul de cerere, decizie, sarcină, document, audit sau API intern. Ambele sunt mecanisme de reutilizare și control, nu simple denumiri tehnice.

Element comun	Ce se gestionează central	Ce rămâne specific domeniului
Cerere	Envelope comun: solicitant, serviciu, canal, status, documente, istoric, responsabil, termene.	Formularul concret, criteriile de eligibilitate și validările specifice.
Dosar / caz	Legarea cererilor, verificărilor, documentelor, deciziilor și evenimentelor.	Regulile de constituire a dosarului pentru pensie, beneficiu sau alt serviciu.
Decizie	Structură oficială: rezultat, temei, aprobare, document generat, notificare, audit.	Calculul, condițiile și temeiurile specifice domeniului.
Workflow	Motor de stare, tranziții, sarcini, responsabilități, termene și audit.	Pașii concreți ai fluxului și regulile de tranziție specifice serviciului.
Documente și șabloane	Generare, versionare, metadate, limbă, export, arhivare și audit.	Conținutul juridic și formatul fiecărui document specific.
Audit	Evenimente comune, utilizator, acțiune, obiect, timp, rezultat și context.	Semnificația business a evenimentului în domeniul respectiv.
Raportare / Jasper	Framework de rapoarte, dataseturi, drepturi, export, jurnalizare.	Indicatorii și structurile de raportare specifice contribuțiilor, pensiilor sau beneficiilor.

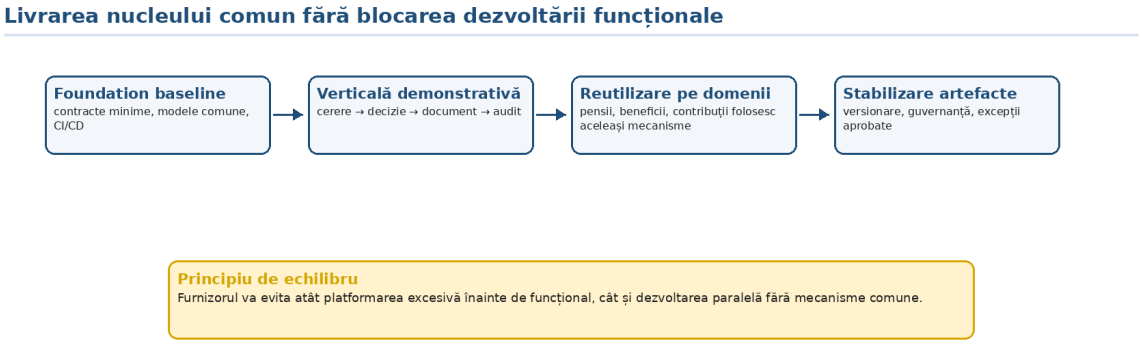


Figura Livrarea nucleului comun fără blocarea dezvoltării funcționale

Design Authority și guvernanța dependențelor

Furnizorul va institui o funcție de Design Authority / guvernanță funcțională și arhitecturală pentru a menține unitatea sistemului în condiții de dezvoltare paralelă. Această funcție va controla modelele comune, contractele API, standardele UI, workflow-urile, shared artefacts, integrarea, raportarea și excepțiile de la reutilizare.

Design Authority nu va înlocui decizia CNAS asupra regulilor instituționale. Rolul ei este să pregătească opțiuni tehnice și funcționale coerente, să arate impactul deciziilor, să prevină duplicarea și să asigure că fiecare echipă de domeniu lucrează pe același cadru comun. Acolo unde decizia privește regulă, proces, prioritate, date sau acceptanță, CNAS va decide ca autoritate funcțională.

Dependențele vor fi urmărite prin dependency board. Orice dependență critică va avea proprietar, termen, impact, decizie necesară și stare. Exemplele principale sunt: cont individual înainte de fluxuri de pensii, model comun de document înainte de decizii oficiale, Integration Gateway înainte de verificări externe, Jasper/reporting framework înainte de rapoarte grele și model comun de roluri înainte de UAT pe profiluri reale.

Tip decizie	Responsabilitate Furnizor	Implicare CNAS
Model comun / shared artefact	Propune model, explică impact, implementează și versionează.	Confirmă că modelul acoperă procesele și datele instituționale.
Excepție de la reutilizare	Justifică tehnic și funcțional excepția, estimează impactul.	Aprobă dacă excepția este acceptabilă operațional și contractual.
Flux / regulă de business	Prezintă opțiuni, efecte în sistem, teste și impact.	Decide interpretarea funcțională și validarea procesului.
Dependență critică	Raportează blocajul, propune soluții sau secvențiere alternativă.	Prioritizează decizii, resurse de validare și clarificări instituționale.

Disciplina clarificărilor, deciziilor și schimbărilor

Furnizorul va separa clar trei categorii de intervenții: clarificare, decizie de proiectare și schimbare de scope. Clarificarea explică o cerință existentă sau confirmă interpretarea ei. Decizia de proiectare stabilește modul de implementare în interiorul scope-ului aprobat. Schimbarea de scope modifică sau extinde cerința, livrabilul, integrarea, calendarul, criteriul de acceptanță sau volumul de lucru. Această separare protejează CNAS de confuzia dintre ajustarea normală a implementării și modificarea obiectului contractual.

Toate clarificările cu impact funcțional, tehnic sau de date vor fi înregistrate într-un decision log. Pentru fiecare decizie relevantă, Furnizorul va indica cerința afectată, contextul, variantele analizate, recomandarea, impactul asupra fluxurilor, datelor, testelor și documentației, decizia CNAS și data aplicării. În acest mod, deciziile nu rămân în e-mailuri sau discuții informale, ci devin parte a trasabilității proiectului.

Schimbările vor fi evaluate prin impact analysis. Evaluarea va acoperi cel puțin: cerințe/UC-uri afectate, componente tehnice, shared services, date/migrare, rapoarte/documente, integrări, securitate, testare, instruire, suport și calendar. CNAS va putea decide informat asupra schimbării, iar Furnizorul va putea integra decizia fără a deteriora controlul asupra livrării.

Mecanica incrementurilor lunare în M2

Fiecare increment lunar va fi planificat ca pachet de livrare verificabil. Pachetul va include UC-uri sau părți de lanțuri operaționale, decizii de analiză, componente dezvoltate, configurări, șabloane, teste, documentație actualizată și demonstrație pe scenarii. Furnizorul va evita incrementuri care livrează doar componente interne fără valoare demonstrabilă pentru CNAS.

Incrementurile vor urmări vertical slices. Un increment valoros poate acoperi, de exemplu, cerere simplă, dosar, workflow, sarcină în dashboard, decizie, document, notificare și audit. Alt increment poate extinde același mecanism către pensii sau beneficii. Astfel, CNAS vede comportamentul sistemului, nu doar acumularea de cod sau ecrane.

Primele incrementuri vor stabili foundation baseline: roluri, utilizatori, workflow minim, taskuri, model de document, audit, CI/CD, standarde API/UI și primele contracte shared. Incrementurile ulterioare vor extinde domeniile, vor confirma reutilizarea și vor transforma shared services din schelet inițial în mecanisme mature folosite în mai multe fluxuri.

Tip increment	Conținut recomandat	Evidență livrată
Foundation baseline	Roluri, workflow minim, taskuri, audit, document skeleton, CI/CD, API/UI standards.	Demo tehnic-funcțional, repository, release package, documentație inițială.
Verticală demonstrativă	Cerere → dosar → workflow → decizie → document → notificare → audit.	Scenariu rulat, teste, feedback CNAS, actualizare SRS/SDD.
Extindere domeniu	Aplicarea mecanismelor comune în pensii, beneficii sau contribuții.	UC-uri implementate, reutilizare dovedită, defecte/observații tratate.
Stabilizare shared artefacts	Versionare, guvernanță, excepții, contracte API, standarde de testare.	Decision log, contracte aprobate, teste de regresie.

CI/CD, release control și deployment traceability

Furnizorul va utiliza CI/CD ca mecanism de trasabilitate și control al release-urilor. Fiecare schimbare relevantă va fi legată de work item, cerință, UC, defect sau decizie. Build-urile, testele, artefactele, scripturile de migrare, configurările, șabloanele Jasper/documente și release notes vor fi gestionate ca pachet coerent de livrare.

Pentru CNAS, release package-ul va include cod aplicație, imagini/container artefacts, migrații de bază de date, configurări, șabloane, versiuni de API, release notes, raport de teste, instrucțiuni de deployment și rollback/forward-fix dacă scenariul tehnic o cere. Această structură permite reproducerea instalărilor și investigarea ulterioară a fiecărei versiuni.

Promovarea între medii se va realiza controlat: development, test, UAT/pre-production și production, conform mediilor disponibile și aprobate. Fiecare promovare va avea condiții minime: build reușit, teste relevante, migrații validate, configurări versionate, defecte critice tratate și documentație actualizată.

CI/CD înseamnă integrare continuă și livrare/deployment controlat. În această ofertă, termenul nu este folosit ca simplu element tehnic, ci ca mecanism de legare între cerință, cod, test, artefact, release, mediu de instalare și evidență de acceptanță.

Model Office, feedback funcțional și UAT

Furnizorul va introduce un mecanism de feedback funcțional înainte de UAT-ul formal. Incrementurile lunare vor fi demonstrate pe scenarii reprezentative CNAS, cu utilizatori funcționali desemnați și cu date controlate. Scopul este verificarea utilității operaționale, nu doar confirmarea că funcția rulează tehnic.

Acest mecanism poate funcționa ca Model Office: un cadru controlat în care fluxurile sunt rulate cu roluri reale, date reprezentative și scenarii concrete. Observațiile CNAS, clarificările, defectele și deciziile rezultate vor fi înregistrate, analizate și integrate în backlog, SRS/SDD, teste și planul de implementare.

UAT-ul formal va fi derivat din UC-uri și din lanțurile funcționale. Pentru fiecare flux critic, scenariile vor acoperi cazul standard, date lipsă, documente incomplete, verificări externe indisponibile, autorizare insuficientă, respingere, corectare, generare document, notificare, audit și raportare. CNAS va confirma scenariile și rezultatele ca autoritate funcțională asupra procesului.

„Model Office” este un mod de validare funcțională controlată, anterior UAT-ului formal. În practică, înseamnă demonstrații pe scenarii reale, cu utilizatori desemnați CNAS, observații înregistrate și decizii urmărite. Nu este o etapă contractuală separată dacă documentația nu o definește astfel; este un mecanism de reducere a riscului.

Prototipare rapidă UI/UX înainte de dezvoltarea extinsă

Furnizorul va utiliza prototiparea rapidă pentru ecranele și fluxurile cu impact operațional ridicat, înainte de dezvoltarea completă a componentelor. Pentru operatorii CNAS/CTAS, diferența dintre un flux utilizabil și unul corect tehnic, dar greu de operat, poate produce timp pierdut, erori de procesare și rezistență la utilizare. De aceea, interfețele critice vor fi validate prin mockup-uri, wireframe-uri sau prototipuri interactive înainte de implementarea extinsă.

Prototipurile vor fi folosite pentru confirmarea structurii ecranelor, ordinii câmpurilor, comportamentului butoanelor, mesajelor de validare, vizibilității sarcinilor, navigării între obiecte și prezentării documentelor/rapoartelor. Validarea va fi făcută cu utilizatori funcționali desemnați de CNAS, pe scenarii concrete și cu respectarea principiilor MUD unde sunt aplicabile.

Această abordare reduce costul schimbărilor. O modificare de flux sau ecran făcută în prototip este mai ieftină și mai rapidă decât modificarea unui modul deja dezvoltat, testat și conectat la servicii backend. Prototiparea nu înlocuiește SRS/SDD sau UAT, ci ajută la maturizarea lor înainte de codarea completă.

Ce se prototipează	Ce validează CNAS	Cum se folosește rezultatul
Dashboard și cozi de sarcini	priorități, filtre, acțiuni disponibile	ajustare UX înainte de dezvoltare
Cerere/dosar/decizie	ordine câmpuri, documente, tranziții, mesaje	actualizare SRS/SDD și scenarii de testare
Rapoarte/documente	structură, parametri, export, citire	confirmare șabloane și date necesare
Administrare/configurare	roluri, șabloane, fluxuri, nomenclatoare	reducerea riscului de configurări greu de folosit

Data & Migration Assurance

Furnizorul va trata datele CNAS ca parte centrală a metodei de livrare. Funcționalitatea nu va fi considerată matură dacă rulează doar pe date noi introduse manual în teste. Sistemul trebuie să funcționeze pe date istorice și operaționale migrate, reconciliate și acceptate pe evidențe.

Furnizorul va trata data cleansing-ul ca activitate distinctă față de migrarea tehnică. Migrarea mută și transformă datele; data cleansing-ul reduce erorile, ambiguitățile și inconsistențele care ar putea afecta funcționalitatea noului sistem. Pentru CNAS, această separare este esențială deoarece datele istorice pot conține duplicate, coduri vechi, valori lipsă, adrese neuniforme, perioade suprapuse, diferențe între registre, clasificatoare depășite sau situații care necesită decizie funcțională.

Furnizorul va propune un mecanism de curățare asistată a datelor, fără a modifica unilateral sensul instituțional al datelor. Regulile tehnice de detectare vor fi pregătite de Furnizor; regulile funcționale, pragurile de acceptare și deciziile asupra excepțiilor vor fi confirmate de CNAS. În acest mod, calitatea datelor este îmbunătățită înainte de migrarea finală, iar responsabilitatea asupra interpretării instituționale rămâne la autoritatea contractantă.

Etapă	Ce se execută	Evidență
Profilare inițială	Identificare volume, câmpuri lipsă, duplicate, anomalii, coduri invalide, valori necorelate.	Raport de profiling și listă de riscuri de date.

Etapă	Ce se execută	Evidență
Reguli de curățare	Definire reguli tehnice și funcționale: normalizare, deduplicare, mapare coduri vechi, completări permise.	Catalog reguli data cleansing, aprobat/confirmat unde este necesar.
Liste de excepții	Separarea cazurilor corectabile automat de cazurile care cer decizie CNAS.	Error bucket, liste de excepții și status de soluționare.
Curățare asistată	Aplicarea regulilor asupra datelor sursă sau staging, conform deciziilor aprobate.	Rulare controlată, log modificări, raport de impact.
Validare post-cleansing	Compararea rezultatelor înainte/după și validarea indicatorilor de calitate.	Raport data quality și decizie privind pregătirea pentru migrare.

Data cleansing-ul va fi integrat cu migration factory. Rulările de migrare pilot vor arăta nu doar câte date pot fi încărcate, ci și ce categorii de date necesită curățare, decizie sau tratament special. Migrarea finală va utiliza regulile și excepțiile deja validate.

Migration Sandbox și Data Cleansing înainte de migrarea finală

Furnizorul va extinde abordarea de migrare printr-un Migration Sandbox, utilizat pentru rulări repetate, profilare, identificarea datelor neconforme și verificarea regulilor de transformare cu mult înainte de migrarea finală. Scopul acestui mecanism este ca problemele de calitate a datelor să fie descoperite și discutate în timpul proiectului, nu în fereastra de cutover.

Data cleansing-ul nu va fi tratat ca operațiune tehnică unilaterală. Furnizorul va identifica anomalii, duplicate, valori lipsă, inconsistențe, referințe rupte, coduri nevalide, perioade suprapuse, sume nereconciliate și cazuri care necesită decizie funcțională. CNAS va decide asupra regulilor de corectare, acceptare, excludere, marcaj sau migrare cu excepție, acolo unde datele au semnificație juridică, financiară sau operațională.

Pentru fiecare rundă de migrare în sandbox, Furnizorul va produce rapoarte de profilare și reconciliere, error bucket, listă de excepții, propuneri de reguli de curățare și status al deciziilor CNAS. Datele curate nu vor fi promise artificial; vor fi obținute prin proces repetabil, decizii documentate și validare pe loturi relevante.

Activitate	Ce livrează Furnizorul	Ce decide / confirmă CNAS	Rezultat urmărit
Profilare date sursă	volume, tipuri de erori, valori lipsă, duplicate, coduri invalide	surse prioritare, toleranțe, zone critice	hartă de risc a datelor
Reguli de cleansing	propuneri de corectare, normalizare, mapare sau excludere	reguli acceptate, excepții, semnificație juridică/funcțională	set de reguli aplicabile în migrare
Rulări sandbox	migrare pilot, error bucket, raport sursă-vs-țintă	verificare eșantioane și decizii asupra cazurilor speciale	reducerea erorilor înainte de cutover
Dress rehearsal	rulare completă temporizată, reconciliere, scenariu de rerun	confirmarea readiness pentru migrarea finală	migrare finală fără surprize majore

Migrarea va fi organizată ca proces repetabil: profilare surse, mapping, reguli de transformare, staging, validare, încărcare, error bucket, reconciliere, rerun controlat și business sign-off. Migrarea finală nu va fi prima migrare completă; ea va fi execuția controlată a unui mecanism demonstrat anterior prin rulări pilot și verificări comparative.

Data governance va clarifica proprietarii funcționali ai datelor, regulile de calitate, sursele de adevăr, tratamentul duplicatelor, datele lipsă, excepțiile și limitele de reconciliere. CNAS va decide asupra excepțiilor

de date care au impact funcțional sau juridic, iar Instrumentele, rapoartele și evidențele necesare acestei decizii fac parte din pachetul de data governance și reconciliere.

Mecanism de date	Ce livrează Furnizorul	Cum intervine CNAS
Profilare surse	Analiză structură, volume, calitate, anomalii și riscuri.	Confirmă sursele relevante și prioritățile de verificare.
Mapping și reguli	Mapping câmpuri, transformări, reguli de validare, excepții.	Validează interpretarea funcțională a datelor și regulilor.
Reconciliere	Rapoarte sursă-vs-țintă, valori de control, duplicate, respingeri.	Confirmă acceptabilitatea rezultatelor și decide cazurile de excepție.
Dress rehearsal	Rulare completă, timp de execuție, error bucket, plan de rerun.	Verifică readiness-ul pentru migrarea finală și cutover.

16.5 Calitate, securitate, integrare, performanță și testare

Furnizorul va integra calitatea în metoda de livrare. Fiecare increment va trece prin verificări interne înainte de demonstrare: teste funcționale, teste de regresie unde este cazul, validări de workflow, verificări de autorizare, verificări de documente/șabloane, teste de integrare și actualizarea documentației relevante.

Securitatea și protecția datelor personale vor fi aplicate încă din proiectare. Modelul de acces, rolurile, permisiunile, jurnalizarea, controlul exporturilor, minimizarea datelor în loguri, separarea responsabilităților și testele de securitate vor fi integrate în SRS/SDD, în incrementuri și în readiness gates.

Testarea nu se va limita la confirmarea funcțiilor individuale. Pentru fluxurile critice, Furnizorul va testa trasee end-to-end: date intrate în sistem, verificare, calcul, decizie, document, notificare, efect asupra plății sau raportării și audit. Scenariile vor include și cazuri negative, pentru a confirma că sistemul blochează acțiunile nepermise.

Furnizorul va aplica principiile Zero Trust într-o formă pragmatică, adaptată cerințelor CNAS și infrastructurii aprobate. Această abordare nu presupune introducerea unei platforme comerciale suplimentare prin ofertă, ci proiectarea sistemului astfel încât accesul la date, funcții, API-uri, documente, rapoarte și acțiuni critice să fie controlat explicit, verificabil și auditat.

Principiul de bază este că sistemul nu va acorda încredere implicită doar pe baza rețelei, mediului sau interfeței din care vine solicitarea. Backend-ul va rămâne limita finală de autorizare. Fiecare acțiune relevantă va fi evaluată în funcție de identitate, rol, drept, context operațional, starea obiectului, scopul accesului și regulile definite în modelul de securitate.

Principiu	Aplicare în soluție
Least privilege	Utilizatorii și serviciile primesc doar drepturile necesare rolului și acțiunii.
Backend authorization	UI-ul poate ascunde acțiuni, dar backend-ul validează obligatoriu fiecare acțiune.
Context and object state	Accesul depinde și de starea cererii, dosarului, deciziei, plății sau documentului.
Audit by design	Acțiunile relevante sunt jurnalizate cu utilizator, obiect, timp, rezultat și context.
Export control	Exporturile și rapoartele cu date sensibile sunt controlate prin drepturi și audit.
Service-to-service control	API-urile interne și integrările folosesc contracte, autentificare tehnică și logare controlată.

Testarea de securitate va include cazuri negative: acces insuficient, tranziție nepermisă, export neautorizat, acces la obiect din alt domeniu, apel API fără drepturi suficiente și modificare de status în afara workflow-ului. Rezultatele vor fi incluse în security readiness evidence înainte de UAT și go-live.

Modelul intern de calitate și controlul de design

Furnizorul va aplica un model intern de calitate care începe înainte de scrierea codului. Calitatea va fi controlată prin claritatea cerinței, design verificat, contracte interne stabile, reutilizare a shared artefacts, reguli de coding, code review, testare, documentație și readiness înainte de demonstrare. Această abordare reduce riscul ca problemele să fie descoperite abia în UAT sau în stabilizare.

Controlul de design va acoperi cel puțin modelul de date, modelul de securitate, workflow-urile, contractele API, integrarea, raportarea, migrarea, auditul și componentele comune. Design Authority va verifica dacă o soluție propusă respectă functional backbone-ul, nu creează duplicări între domenii, nu ocolește mecanismele comune, nu pune reguli critice doar în interfață și nu afectează performanța, securitatea sau operabilitatea.

Furnizorul va trata documentația ca parte a calității, nu ca activitate finală. SRS, SDD, ghidurile, catalogul de integrare, modelul de date, catalogul de rapoarte, runbook-ul și instrucțiunile de deployment vor fi actualizate progresiv. Un increment nu va fi considerat pregătit pentru review dacă funcționalitatea rulează, dar documentația, testele sau evidențele aferente sunt absente.

Testare și verificare pe niveluri

Testarea va fi organizată progresiv, astfel încât fiecare nivel să producă evidență pentru nivelul următor. Testarea nu va fi tratată ca etapă finală de curățare, ci ca mecanism continuu de confirmare a cerințelor, datelor, securității, integrărilor și operabilității.

Nivel de testare	Ce verifică	Cine pregătește / execută	Evidență
Unit / component	reguli locale, servicii, validări, mapping, transformări	echipa de dezvoltare / QA	rezultate automate, build log
Integration / contract	API-uri interne, gateway, servicii externe, erori, timeout, retry	echipa tehnică + QA	contract test report, logs, scenarii negative
Functional / UC	comportamentul fiecărui UC, roluri, acțiuni, date obligatorii	QA + echipă domeniu	test cases, screenshots/output, defect log
End-to-end chains	lanțuri instituționale: cerere-dosar-decizie-document-notificare-audit	QA + analiști + CNAS la review	scenarii executate, feedback log
Migration / reconciliation	date migrate, valori de control, excepții, duplicate, referințe	echipa date/migrare + CNAS pentru decizii	rapoarte reconciliere, error bucket

Nivel de testare	Ce verifică	Cine pregătește / execută	Evidență
Performance / load	timpi, concurență, rapoarte grele, batch, integrări	echipa tehnică + QA	raport performanță, recomandări operare
Security / access	roluri, permisiuni, exporturi, audit, cazuri negative	echipa tehnică + QA	security readiness evidence
UAT	acceptanța funcțională pe scenarii aprobate	CNAS cu suportul Furnizorului	UAT report, observații, sign-off

Scenariile de testare vor include cazuri pozitive și negative. Sistemul trebuie să demonstreze nu doar că permite acțiunile corecte, ci și că blochează acțiunile nepermise, accesul insuficient, tranzițiile invalide, documentele incomplete, datele inconsistente și operațiunile care nu respectă starea obiectului.

Integrare și interoperabilitate în metoda de livrare

Furnizorul va gestiona interoperabilitatea printr-un Integration Gateway și prin contracte controlate, nu prin apeluri dispersate în fiecare domeniu. Gateway-ul va standardiza autentificarea tehnică, logarea, timeout-urile, retry, tratarea erorilor, auditul și snapshot-ul răspunsurilor relevante.

Această separare permite reutilizarea serviciilor externe în mai multe fluxuri. Mecanismul de apelare rămâne comun, iar interpretarea business a datelor aparține domeniului care folosește informația. De exemplu, aceeași categorie de verificare externă poate avea efect diferit într-un flux de pensie și într-un flux de beneficiu, dar apelul, jurnalizarea și tratarea erorilor trebuie să rămână unitare.

Testarea integrărilor va include contract testing, scenarii de indisponibilitate, răspunsuri incomplete, timeouts, retry, erori de validare și auditarea schimburilor. O integrare va fi considerată pregătită nu doar când răspunde tehnic, ci când efectul ei funcțional este demonstrat într-un flux CNAS.

Performanță sub sarcină reală și procesări de volum

Furnizorul va trata performanța ca proprietate verificabilă a sistemului, nu ca rezultat implicit al stivei tehnologice. SI „Protecția Socială” va fi proiectat pentru utilizare operațională concurentă, interogări frecvente asupra registrelor, generare de documente, acces la rapoarte, apeluri de integrare și procesări de volum precum calculuri, recalculări, indexări, exporturi, agregări statistice sau rulări de sfârșit de lună.

Metodologia de livrare va separa fluxurile interactive de procesările grele. Operațiunile utilizatorilor - căutare, deschidere dosar, examinare, schimbare statut, generare document sau consultare cont - vor fi protejate de joburile batch, rapoartele grele și importurile/exporturile de volum. Unde este necesar, procesările de durată vor fi executate asincron, cu cozi, stare, jurnalizare, posibilitate de reluare controlată și notificare la finalizare.

Testarea de performanță va acoperi scenarii reprezentative, nu doar teste sintetice. Furnizorul va pregăti scenarii pentru acces concurent al operatorilor, căutări pe registre, rulare rapoarte, generare documente, apeluri de integrare, procesări batch, vârfuri operaționale și comportament în perioade cu activitate intensă. Rezultatele vor fi prezentate prin rapoarte de performanță, observații, recomandări de operare și, unde este cazul, ajustări ale planului de indexare, caching, partiționare, job scheduling sau dimensionare infrastructurală.

Zonă verificată	Risc controlat	Mecanism propus	Evidență pentru CNAS
Utilizare concurentă operatori	degradarea fluxurilor zilnice	teste de încărcare pe scenarii de lucru, profile de utilizator și date reprezentative	raport performanță, percentile, rată de erori, recomandări
Batch / calcule masive	blocarea interfeței sau a tranzacțiilor critice	execuție asincronă, ferestre de rulare, cozi, retry și monitorizare	job logs, runbook, rezultat/restart controlat
Rapoarte grele	interogări costisitoare pe tabele tranzacționale	dataseturi pregătite, materialized views/agregări, limitare acces după rol	catalog rapoarte, test valori, test timp de răspuns
Integrare externă	latență sau timeouts în fluxuri operaționale	timeout/retry, cache/snapshot unde e permis, fallback controlat	integration test report, scenarii negative
Go-live / stabilizare	surprize de volum în producție	production rehearsal, monitoring, praguri de alertare	readiness checklist, rapoarte stabilizare

16.6 Readiness gates, phase-in, BCDR și acceptanță pe evidențe

Furnizorul va utiliza readiness gates pentru a controla trecerea între etape și pentru a evita intrarea prematură în activități pentru care sistemul, datele, utilizatorii sau suportul nu sunt pregătite. Fiecare gate se va închide pe evidențe: documente aprobate, componente dezvoltate, teste executate, defecte controlate, date reconciliate, integrări validate, utilizatori instruiți, runbook pregătit sau suport operațional activat, după caz.

Phase-in-ul va fi stabilit pe baza dependențelor reale dintre domenii. Unele capabilități pot fi pilotate separat, altele trebuie grupate pentru a păstra consistența datelor și a fluxurilor. Strategia de lansare va evita atât big-bang-ul nejustificat, cât și exploatarea prelungită a două surse de adevăr concurente.

Acceptanța va fi susținută prin evidențe, nu doar prin demonstrații informale. Pentru fiecare capabilitate critică, Furnizorul va prezenta cerințe/UC-uri acoperite, scenarii executate, defecte tratate, date validate, documentație actualizată și decizii CNAS relevante.

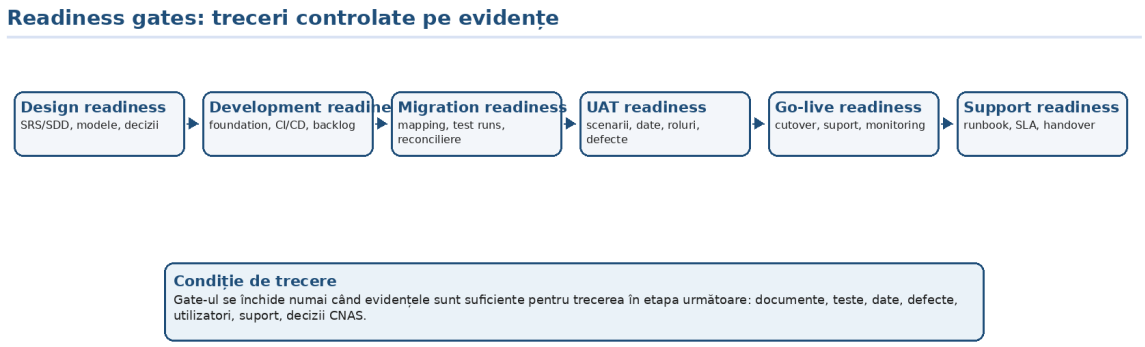


Figura Readiness gates pentru trecerea controlată între etape

Business Continuity & Disaster Recovery la nivel de proces CNAS

Furnizorul va trata continuitatea operațională ca parte a pregătirii pentru producție, nu doar ca subiect de infrastructură. Pentru un sistem CNAS, indisponibilitatea nu afectează doar servere sau aplicații; ea poate afecta examinarea cererilor, accesul la dosare, generarea deciziilor, rapoartele, procesările de plată, integrările și suportul utilizatorilor.

Planul de Business Continuity & Disaster Recovery va fi construit împreună cu CNAS în limitele infrastructurii disponibile și ale cerințelor contractuale. Planul va defini scenarii de incident, roluri, canale de comunicare, priorități operaționale, proceduri de reluare, tratamentul operațiunilor amânate, validarea datelor după restabilire și raportarea incidentului. Valorile RTO/RPO vor fi confirmate în documentația de proiectare și operare, conform cerințelor și posibilităților infrastructurale aprobate.

Pentru fluxurile critice, Furnizorul va pregăti runbook-uri care explică ce se întâmplă în caz de indisponibilitate a aplicației, bazei de date, serviciului de autentificare, integrării externe, jobului batch sau raportării. Reluarea după incident va include verificarea consistenței datelor, reluarea joburilor eșuate, reconcilierea operațiunilor amânate și confirmarea că utilizatorii pot continua lucrul fără efecte ascunse asupra datelor.

Scenariu	Mecanism de continuitate	Restabilire / verificare	Evidență
Indisponibilitate aplicație	comunicare incident, prioritizare fluxuri, suport utilizatori	reporire controlată, smoke tests, validare acces	incident report, checklist
Indisponibilitate integrare externă	coadă/retry unde este permis, status clar al verificării	reluare apeluri, snapshot/jurnal, verificare efect business	integration log, reconciliation
Eșec job batch	stare job, reluare controlată, prevenire dublare efecte	rerun, comparații, confirmare rezultat	job log, runbook
Problemă date după incident	blocare operațiuni afectate, analiză impact	reconciliere, corecție aprobată, audit	data incident record
Indisponibilitate raportare	protecția tranzacționalului, raportare amânată	rulare controlată după restabilire	raport execuție, audit export

Business Continuity & Disaster Recovery în metodologia de implementare

Furnizorul va include pregătirea pentru continuitate operațională și recuperare în caz de incident major în metodologia de implementare. Pentru SI „Protecția Socială”, disponibilitatea sistemului, integritatea datelor, recuperarea serviciilor și continuitatea proceselor critice nu pot fi tratate doar ca setări de infrastructură. Ele trebuie proiectate, documentate, testate și predate ca parte a readiness-ului operațional.

Obiectivele de continuitate, inclusiv RTO și RPO, vor fi stabilite împreună cu CNAS în limitele infrastructurii disponibile, ale cerințelor contractuale și ale criticității proceselor. Furnizorul va propune scenarii de continuitate pentru componentele aplicației, baza de date, fișiere/documente, șabloane, integrare, rapoarte și mecanisme de audit. CNAS va confirma nivelul acceptabil de indisponibilitate și pierdere de date pentru procesele critice.

Clarificare terminologică. RTO indică timpul maxim acceptabil pentru restabilirea unui serviciu după incident. RPO indică punctul în timp până la care datele trebuie recuperate după incident. Valorile concrete trebuie stabilite cu CNAS și administratorii infrastructurii.

Componentă BCDR	Ce se pregătește	Evidență
Clasificare procese critice	Identificarea fluxurilor care au impact asupra plăților, deciziilor, raportării, accesului public sau suportului.	Catalog procese critice și priorități de recuperare.
Backup / restore	Proceduri pentru date, configurări, fișiere, șabloane și artefacte de release.	Runbook, teste restore, evidențe de execuție.
Disaster recovery scenario	Scenarii de indisponibilitate aplicație, bază de date, integrare, storage sau mediu.	Plan DR, responsabilități, pași de recuperare.

Componentă BCDR	Ce se pregătește	Evidență
Testare BCDR	Verificare periodică a procedurilor relevante înainte de go-live și în stabilizare.	Raport test, timp de recuperare, observații.
Operational handover	Predarea procedurilor și responsabilităților către CNAS / echipa de operare.	Runbook final, instruire tehnică, sign-off.

Readiness intern înainte de review formal

Înainte de transmiterea unui livrabil sau increment spre verificare formală, Furnizorul va executa un readiness intern. Acest control are rolul de a evita situația în care CNAS primește materiale incomplete, demonstrații nepregătite sau funcționalități fără evidențe. Review-ul CNAS trebuie să se concentreze pe validare funcțională, priorități și acceptanță, nu pe lipsuri elementare care trebuie depistate intern de Furnizor.

Tip livrabil / rezultat	Readiness intern verificat	Pachet transmis către CNAS
Document SRS/SDD	completitudine, consistență, trasabilitate, decizii deschise	document, matrice cerințe, decision log, open points
Increment funcțional	build, teste, documentație, defecte cunoscute, scenariu demo	release notes, test evidence, demo script, defect log
Integrare	contract, medii, date test, timeout/retry, logs	catalog integrare, test report, sample payloads, error handling
Migrare	mapping, rulare, erori, reconciliere, excepții	raport migrare, error bucket, reconciliation report
UAT	scenarii, utilizatori, date, mediu, defecte blocate	UAT pack, user guide, defect baseline
Go-live	deployment, date, training, suport, rollback/contingență	go-live checklist, runbook, support readiness

Dacă readiness-ul intern identifică lipsuri majore, Furnizorul va trata lipsurile înainte de transmiterea formală. Dacă există limitări cunoscute care nu blochează review-ul, acestea vor fi declarate explicit împreună cu impactul și planul de remediere.

16.7 Raportare, riscuri, schimbări și control operațional

Raportarea de progres va arăta starea reală a proiectului pe mai multe axe: milestone-uri, UC-uri, lanțuri funcționale, fluxuri de domeniu, Shared Services, defecte, riscuri, dependențe, migrare, integrări, documentație, feedback CNAS și readiness gates. Această structură permite identificarea timpurie a zonelor unde progresul tehnic nu este încă susținut de validare funcțională sau operațională.

Indicatorii urmăriți pot include: UC-uri implementate și validate, lanțuri funcționale demonstrate, shared artefacts reutilizate, defecte deschise/închise, procent date migrate și reconciliate, integrări validate, rapoarte/documente validate, utilizatori instruiți, release-uri trasabile și gates închise.

Managementul schimbărilor va separa clar clarificările de proiectare de schimbările de scop. Ajustările cerute de analiză, modificările legislative, completările funcționale, modificările de date, extinderile de integrare și schimbările de raportare vor fi evaluate prin impact asupra cerințelor, calendarului, testării, migrației,

documentației și suportului. CNAS va decide asupra schimbărilor care afectează obiectul, prioritatea sau acceptanța funcțională.

Raportare, întâlniri de lucru și transparență de proiect

Transparența proiectului este organizată printr-o cadență de comunicare adaptată etapelor, nu printr-un calendar rigid de întâlniri fără efect operațional. Fiecare tip de întâlnire va avea scop, intrări, ieșiri și evidență. Deciziile, acțiunile, riscurile, observațiile și blocajele vor fi urmărite până la închidere.

Eveniment / mecanism	Scop	Participanți tipici	Rezultat
Kick-off / mobilizare	confirmă guvernanța, canalele, calendarul și registrele	CNAS + Furnizor	plan de mobilizare, listă contacte, registre inițiale
Workshop cerințe / UC	clarifică procese, reguli, date, roluri și excepții	CNAS funcțional + BA/architect	notes, decisions, SRS updates
Architecture / design review	verifică opțiuni tehnice, shared services, date, interop	CNAS tehnic/funcțional + Design Authority	design decision, impact, action items
Increment review	demonstrează funcționalitatea lunară pe scenarii	CNAS + echipe domeniu + QA	feedback log, defecte, ajustări
Readiness review	confirmă pregătirea livrabilului/gate-ului	CNAS + PM + QA + leads	checklist, evidence package
Risk/issue review	urmărește blocaje, dependențe și mitigări	PM, leads, CNAS unde e necesar	risk/issue register actualizat
Acceptance discussion	pregătește acceptanța formală pe evidențe	CNAS + Furnizor	acceptance package, observații, concluzii

Raportarea periodică va include starea milestone-urilor, starea UC-urilor, progresul pe fluxuri funcționale, shared services, defecte, riscuri, schimbări, migrare, integrări, documentație, feedback CNAS și readiness gates. Raportarea nu va reduce proiectul la procent de dezvoltare, ci va arăta ce este demonstrabil, ce este blocat, ce depinde de decizie și ce este pregătit pentru acceptanță.

Defecte, issue log, prioritizare și retestare

Furnizorul va menține un registru unic pentru defecte și issue-uri, astfel încât problemele identificate în dezvoltare, demonstrare, Model Office, UAT, migrare, integrare sau stabilizare să fie vizibile și gestionate până la închidere. Fiecare înregistrare va avea identificator, sursă, descriere, cerință/UC afectată, severitate, prioritate, domeniu, responsabil, status, termen țintă, rezoluție, evidență de retestare și decizie asupra închiderii.

Defectele vor fi separate de schimbările de scope. Un defect reprezintă abatere de la cerință, design aprobat, criteriu de acceptanță sau comportament așteptat. O schimbare reprezintă modificare sau extindere a cerinței ori a obiectului. Această distincție protejează calitatea și predictibilitatea contractuală: defectele se corectează în cadrul obligațiilor de livrare, iar schimbările se evaluează prin mecanismul de control al schimbărilor.

Prioritizarea defectelor va ține cont de impactul operațional, efectul asupra datelor, efectul asupra plăților, blocarea utilizatorilor, riscul de securitate, imposibilitatea de testare și efectul asupra acceptanței. Defectele critice care blochează fluxuri esențiale, integrări obligatorii, migrare, acces sau securitate vor fi escaladate prin guvernanța proiectului.

Managementul riscurilor și failure modes specifice CNAS

Furnizorul va trata managementul riscurilor ca instrument viu de livrare, nu ca anexă formală. Riscurile vor fi identificate, actualizate și discutate pe tot parcursul proiectului, cu proprietar, impact, probabilitate, acțiuni de mitigare, decizii necesare și expunere reziduală. Pentru un sistem CNAS, multe riscuri nu sunt strict tehnice; ele apar din date, dependențe, decizii instituționale, disponibilitatea utilizatorilor pentru review, interpretări legislative, integrări externe și pregătirea operațională.

Risc / failure mode	Impact posibil	Mecanism de prevenire	Evidență de control
Shared services întârzie fluxurile de domeniu	echipele nu pot livra vertical sau creează soluții proprii	foundation baseline minim + prima verticală demonstrativă + extindere incrementală	catalog shared artefacts, dependency board
Fluxurile paralele se fragmentează	modele diferite de cerere, decizie, audit, documente	Design Authority și reutilizare obligatorie a artefactelor comune	decision log, design reviews
Datele istorice sunt mai slabe decât se presupune	migrare întârziată, reconciliere dificilă, blocaje UAT	profilare timpurie, rulări pilot, error bucket, decizii CNAS pe excepții	rapoarte de profilare și reconciliere
Integrarea externă nu este disponibilă la timp	fluxuri incomplete, testare întârziată	contracte, mock/stub controlat, plan de test, escaladare dependențe	integration log, risk register
Feedback funcțional vine târziu	rework în UAT sau stabilizare	Model Office și demo lunar pe scenarii CNAS	feedback log, backlog ajustat
Raportarea devine logică paralelă necontrolată	valori inconsistente, performanță afectată	curated datasets, guvernanță șabloane, validare valori	catalog rapoarte, test reports
Securitatea este verificată prea târziu	rework pe roluri/acces/exporturi	security by design, teste pe roluri, readiness gate	security evidence package
Go-live se tratează ca instalare tehnică	sistem nepregătit operațional	go-live readiness, training, runbook, support readiness	checklist readiness, service transition package

Riscurile cu impact ridicat nu vor rămâne note tehnice interne. Ele vor fi prezentate în raportarea de progres și, atunci când este necesar, escaladate către nivelul de guvernanță care poate decide asupra priorității, dependenței sau interpretării funcționale.

Planul de implementare și ordinea logică a livrării

Planul de implementare va combina structura formală a milestone-urilor cu ordinea logică a dependențelor. Primele activități vor stabili guvernanța, SRS/SDD, modelul de date, modelul de securitate, foundation baseline, contractele comune și mecanismele CI/CD. Dezvoltarea de domeniu va avansa în paralel, dar pe același nucleu comun.

Ordinea logică recomandată este: mobilizare și guvernanță, foundation baseline, prima verticală demonstrativă, extindere pe fluxuri paralele, integrare și migrare repetabilă, UAT pregătit prin Model Office, go-live readiness, stabilizare și service transition. Această ordine permite progres paralel, dar păstrează controlul asupra dependențelor critice.

Moment metodologic	Scop	Rezultat verificabil
Mobilizare	Aliniere guvernanță, roluri, calendare, registre, mod de lucru.	Plan detaliat, registre inițiale, mecanism de raportare și decizie.
Foundation baseline	Crearea mecanismelor comune minime.	Roluri, workflow skeleton, audit, documente, CI/CD, standarde API/UI.
Verticală demonstrativă	Demonstrarea comportamentului end-to-end pe un flux reprezentativ.	Cerere-dosar-decizie-document-notificare-audit rulate și comentate.
Extindere paralelă	Dezvoltarea contribuțiilor, pensiilor și beneficiilor pe nucleu comun.	UC-uri implementate, shared artefacts reutilizate, dependențe urmărite.
Migrare și UAT	Validarea datelor și proceselor cu utilizatori CNAS.	Rapoarte de reconciliere, scenarii executate, defecte tratate, sign-off.
Go-live și stabilizare	Trecere controlată în producție și suport operațional.	Readiness checklist, runbook, service desk, rapoarte de stabilizare.

Institutional Change Management și adoptare operațională

Furnizorul va include în metodologia de implementare un mecanism de management al schimbării instituționale. Noul SI „Protecția Socială” nu schimbă doar interfața utilizatorilor; el schimbă modul în care sunt primite cererile, distribuite sarcinile, aplicate verificările, generate deciziile, urmărite documentele, controlate rapoartele și verificate acțiunile prin audit. Această schimbare trebuie pregătită înainte de go-live, nu explicată utilizatorilor după lansare.

Managementul schimbării va fi orientat spre adoptare operațională. Furnizorul va pregăti împreună cu CNAS mesaje clare despre modificările de proces, rolurile utilizatorilor, diferențele față de modul vechi de lucru, beneficiile operaționale, punctele de atenție și canalele de suport. Utilizatorii-cheie vor fi implicați în Model Office, demonstrații, validarea scenariilor și pregătirea instruirii pe roluri.

Componentă	Rol în adoptare
Impact assessment	Identifică procese afectate, roluri, schimbări de responsabilitate, riscuri de adoptare.
Rețea de utilizatori-cheie	Desemnează persoane care validează fluxuri, transmit feedback și susțin adoptarea în structurile CNAS/CTAS.
Comunicare operațională	Pregătește mesaje scurte despre ce se schimbă, de ce se schimbă și cum se lucrează în noul sistem.
Training pe scenarii	Leagă instruirea de sarcini reale: cerere, dosar, decizie, document, raport, audit.
Suport de tranziție	Asigură canale clare pentru întrebări, defecte, dificultăți de utilizare și solicitări de clarificare.

Această abordare reduce riscul ca sistemul să fie acceptat tehnic, dar utilizat incomplet sau inconsistent. CNAS va putea controla nu doar livrarea aplicației, ci și pregătirea instituțională pentru exploatarea ei.

16.8 Instruire, handover, service transition și reducerea dependenței de Furnizor

Furnizorul va organiza instruirea pe roluri și scenarii reale de lucru. Utilizatorii CNAS/CTAS vor fi instruiți pe sarcini operaționale: dashboard, căutare, înregistrare cerere, examinare, verificare documente, decizie,

generare document, raportare, administrare și suport. Instruirea va fi legată de fluxurile reale, nu doar de prezentarea ecranelor.

Handover-ul tehnic va include cod sursă, repository, instrucțiuni de build/rebuild, scripturi, configurări, model de date, catalog de integrare, ghiduri de administrare și utilizare, ghid de dezvoltator, runbook operațional, documentație de deployment, backup/restore, monitorizare și proceduri de suport.

Service transition va conecta stabilizarea de perioada de suport. Înainte de intrarea în regimul de garanție/mentenanță, Furnizorul va pregăti canalele de suport, clasificarea solicitărilor, SLA, registrul de incidente, procedurile de escaladare, raportarea de suport și mecanismele de actualizare a documentației în cazul remedierilor.

Mentenanță adaptivă și granița dintre suport și schimbare

Furnizorul va gestiona perioada de stabilizare, garanție și suport astfel încât sistemul să rămână utilizabil, documentat și susținut, fără transformarea suportului într-un flux nelimitat de dezvoltare nouă. Remedierile defectelor, ajustările de configurare, rafinările de șabloane, corecțiile de raportare, parametrii de integrare, clarificările operaționale și completările necesare pentru funcționalitatea livrată vor fi tratate prin registrul de suport și mecanismele de change control, după natura solicitării.

O solicitare va fi încadrată ca defect atunci când sistemul livrat se abate de la cerință, design aprobat, criteriu de acceptanță sau comportament demonstrat. O solicitare va fi încadrată ca schimbare atunci când introduce funcționalitate nouă, modifică reguli de business, extinde integrări, schimbă rapoarte în afara modelului aprobat sau afectează domenii nelivrate. Această distincție asigură predictibilitate pentru CNAS și protejează calitatea serviciului.

Pe durata suportului, Furnizorul va păstra actualizate evidențele relevante: registrul solicitărilor, statusul defectelor, versiunile remediate, documentația modificată, instrucțiunile operaționale și rapoartele de suport. Service transition-ul va fi considerat complet doar atunci când sistemul are canale de suport, clasificare solicitări, responsabilități, SLA, runbook, mecanism de escaladare și proceduri de actualizare a documentației.

Guvernanță post-implementare și reducerea dependenței de Furnizor

Furnizorul va pregăti transferul către operarea post-implementare încă din etapa de dezvoltare, nu doar la finalul stabilizării. Scopul este ca CNAS să poată administra, înțelege, verifica și continua sistemul pe baza codului sursă, documentației, configurărilor, runbook-ului, registrului de decizii și cunoștințelor transferate. Reducerea dependenței de Furnizor este tratată ca rezultat metodologic, nu ca anexă formală de predare.

Guvernanța post-implementare va defini cum se gestionează schimbările, defectele, configurările, șabloanele, rapoartele, nomenclatoarele, integrările, release-urile și documentația după go-live. CNAS va primi nu doar fișiere și ghiduri, ci și explicația modului de operare: cum se investighează o problemă, cum se urmărește o decizie, cum se verifică o integrare, cum se actualizează un șablon, cum se citește un log și cum se pregătește un release.

Componentă	Conținut propus
Knowledge transfer plan	Sesiuni tehnice și funcționale pentru administratori, suport și personal IT CNAS.
Operational runbook	Proceduri de operare, monitorizare, backup/restore, deployment, incident și escaladare.

Componentă	Conținut propus
Configuration governance	Reguli pentru nomenclatoare, șabloane, fluxuri, roluri și parametri administrabili.
Release governance	Mod de promovare versiuni, release notes, rollback, migrații DB și evidențe.
Support governance	Clasificare solicitări, SLA, defect vs schimbare, raportare și închidere.
Exit readiness	Confirmarea că documentația, codul, configurările și cunoștințele sunt transferabile.

Pe durata suportului, Furnizorul va continua să actualizeze documentația pentru remedierile și schimbările aprobate. Astfel, sistemul nu rămâne doar funcțional în producție, ci și administrabil, audibil și transferabil după încheierea perioadei contractuale.

Aliniere la bune practici internaționale relevante

Furnizorul va utiliza bune practici internaționale relevante ca repere de proiectare și guvernanță, fără a transforma oferta într-un exercițiu teoretic sau într-o obligație de certificare necerută. Pentru SI „Protecția Socială”, aceste repere sunt utile în special în patru zone: registre și sisteme de protecție socială, infrastructură publică digitală, reutilizare de componente comune și protecția datelor personale.

Alinierea metodologică va fi aplicată pragmatic. Sistemul va fi proiectat pentru interoperabilitate, trasabilitate, securitate, administrare a ciclului de viață, reutilizare controlată și transferabilitate. Principiile de tip digital public infrastructure, digital public goods, social protection information systems și privacy/security by design vor fi folosite ca repere pentru decizii, nu ca etichete decorative.

Reper	Ce aduce metodologic	Aplicare în oferta CNAS
Sisteme de protecție socială integrate	date corelate, registre, eligibilitate, procese instituționale, interoperabilitate	Functional Backbone, data governance, migrare și reconciliere
Digital Public Infrastructure	building blocks reutilizabile, standarde comune, interoperabilitate	Shared Services / Shared Artefacts, Integration Gateway, API standards
Digital Public Goods principles	deschidere, interoperabilitate, protecția datelor, evitare lock-in când scenariul o cere	transfer cod, documentație, standarde, guvernanță și portabilitate
Security / privacy by design	minimizare date, control acces, audit, protecție la nivel de resursă	Zero Trust pragmatic, RBAC/ABAC unde este justificat, audit și export control

Aceste repere nu înlocuiesc cerințele caietului de sarcini. Ele sunt utilizate pentru a întări modul de implementare și pentru a susține deciziile privind interoperabilitatea, securitatea, reutilizarea și operarea pe termen lung.

Rezultatul metodologic livrat către CNAS

Prin metodologia propusă, CNAS primește un cadru de implementare care susține simultan controlul formal, livrarea incrementală, reutilizarea componentelor comune, verificarea pe date, implicarea funcțională activă și operarea post-go-live. Abordarea este construită pentru a reduce riscul de fragmentare, întârziere, migrare necontrolată, acceptanță superficială și dependență informală de Furnizor.

Rezultatul urmărit este un SI „Protecția Socială” funcțional, explicabil, operabil și transferabil. Funcționalitatea va fi demonstrată prin UC-uri și lanțuri operaționale; arhitectura va fi controlată prin shared services și design authority; datele vor fi migrate și reconciliate; release-urile vor fi trasabile; CNAS va valida activ fluxurile și readiness-ul; iar suportul va prelua un sistem documentat, monitorizabil și administrabil.

Prin această metodologie, Furnizorul își asumă livrarea SI „Protecția Socială” ca sistem instituțional verificabil, nu ca sumă de dezvoltări tehnice executate separat. Controlul pe milestone-uri, incrementurile lunare,

backbone-ul funcțional comun, reutilizarea serviciilor și artefactelor partajate, validarea activă de către CNAS, guvernanța deciziilor, migrarea repetabilă, release-urile trasabile și readiness gates formează împreună mecanismul prin care proiectul rămâne controlabil de la analiză până la suport. CNAS va putea urmări nu doar dacă sistemul este dezvoltat, ci dacă acesta funcționează corect în procesele sale reale, pe datele sale, cu utilizatorii săi, cu regulile sale și cu evidențele necesare pentru acceptanță, exploatare și dezvoltare ulterioară.

17. Corespondență cu anexele suport și documentele de lucru ale ofertei

Document / anexă de lucru	Rol în pachetul pregătit de ofertant	Fisier
Anexa 1 Profil Companie	Detalii companie ofertantă	Anexa_1_Profil_Companie
Anexa 2 Matrice functionala	Leagă cerințele ToR de răspunsurile din ofertă și de documentele suport.	Anexa_2_Matrice_functionala
Anexa 3 Registru Procese Scenarii	Grupează procesele, scenariile și anexele funcționale utilizate ca bază pentru analiza, proiectarea și testarea ulterioară. Anexa are rol de trasabilitate la etapa de ofertare. Ea indică modul în care procesele, registrele, web-serviciile, rapoartele și modelele documentare din anexele Caietului de sarcini sunt reflectate în soluția propusă. Scenariile/verificările incluse sunt indicative pentru demonstrarea acoperirii și vor fi detaliate în SRS, SDD și planul de testare/UAT în etapa de implementare.	Anexa_3_Registru_Procese_Scenarii
Anexa 4 Plan Detaliat Implementare	Prezintă calendarul, etapele, milestone-urile, mecanismele de control și evidențele de implementare.	Anexa_4_Plan_Detaliat_Implementare
Anexa 5 Gantt Detaliat	Prezintă calendarul, etapele, milestone-urile, mecanismele de control și evidențele de implementare.	Anexa_5_Gantt_Detaliat
Anexa 6 Matrice Livrabile Acceptanta	Clarifică tratamentul livrabilelor, criteriile de acceptanță și livrabilele fără plată separată.	Anexa_6_Matrice_Livrabile_Acceptanta
Anexa 7 Plan Cadru Migrare	Detaliază modelul de migrare	Anexa_7_Plan_Cadru_Migrare
Anexa 8 Plan Calitate Suport	Detaliază modelul de suport, SLA, raportarea, hypercare-ul și mecanismele de tranziție operațională.	Anexa_8_Plan_Calitate_Suport
Anexa 9 Plan Financiar Detaliat	Corelează livrabilele, termenele, efortul și costurile asumate în oferta financiară pregătită.	Anexa_9_Plan_Financiar_Detaliat