

GUVERNUL REPUBLICII MOLDOVA

HOTĂRÂRE nr. ____

din _____ 2025

**cu privire la aprobarea Programului de dezvoltare al sistemului informațional
al Serviciului Fiscal de Stat pentru anii 2025-2027**

În temeiul art. 6 lit. b) și h) din Legea nr. 136/2017 cu privire la Guvern (Monitorul Oficial al Republicii Moldova, 2017, nr. 252, art. 412, cu modificările ulterioare, Programului național de aderare a Republicii Moldova la Uniunea Europeană pentru anii 2025-2029, aprobat prin Hotărârea Guvernului Republicii Moldova nr.306/2025 (Monitorul Oficial al Republicii Moldova, 2025, nr. 269-288, art. 319), Guvernul

HOTĂRĂȘTE:

1. Se aprobă Programul de dezvoltare al sistemului informațional al Serviciului Fiscal de Stat pentru anii 2025-2027 (conform anexei).
2. Ministerul Finanțelor va asigura monitorizarea, coordonarea și realizarea implementării Programului de dezvoltare al sistemului informațional al Serviciului Fiscal de Stat.
3. Controlul asupra executării prezentei hotărâri se pune în sarcina Ministerului Finanțelor.
4. Prezenta hotărâre intră în vigoare la data publicării în Monitorul Oficial al Republicii Moldova.

Prim-ministru

Dorin RECEAN

Contrasemnează:

Ministru finanțelor

Victoria BELOUS

Programul de dezvoltare al sistemului informațional al Serviciului Fiscal de Stat pentru anii 2025-2027

1. Introducere

În ultimele decenii, Serviciul Fiscal de Stat (SFS) din Republica Moldova a inițiat și implementat reforme menite să îmbunătățească eficiența administrării fiscale și să consolideze relația cu contribuabilii. Totuși, în ciuda acestor eforturi, infrastructura sistemului informațional a SFS nu a reușit să țină pasul cu schimbările rapide din tehnologie și cu cerințele tot mai complexe ale unui sistem fiscal modern. Pe măsură ce economia globală devine din ce în ce mai digitalizată, volumele mari de date, nevoia de automatizare și presiunile pentru integrarea cu sistemele fiscale internaționale impun o tranziție inevitabilă către o infrastructură al sistemului informațional mai avansată și o strategie modernă de administrare fiscală.

Un factor determinant în necesitatea modernizării SFS îl reprezintă creșterea exponențială a volumului de date fiscale pe care SFS trebuie să le gestioneze. Digitalizarea economiei, expansiunea comerțului electronic și creșterea numărului de contribuabili care își desfășoară activitățile în multiple jurisdicții creează provocări imense pentru infrastructura actuală. În acest context, procesele tradiționale, dependente de intervenția manuală și bazate pe sisteme învechite, nu mai sunt capabile să facă față acestei presiuni. Datele fiscale trebuie acum procesate rapid și cu un grad ridicat de acuratețe pentru a preveni erorile, evaziunea fiscală și alte forme de non-conformitate. Lipsa unui sistem informațional eficient împiedică monitorizarea în timp real a activităților economice, limitând astfel capacitatea autorității de a detecta riscurile și fraudele în timp util.

În plus, transformările tehnologice globale și emergența noilor tehnologii, cum ar fi inteligența artificială, Big Data și analiza predictivă, oferă oportunități semnificative pentru SFS de a îmbunătăți și automatiza procesele fiscale. Aceste tehnologii permit autorităților fiscale să analizeze volume mari de date pentru a identifica tipare suspecte, comportamente de risc și pentru a îmbunătăți eficiența colectării impozitelor. Prin automatizarea proceselor repetitive și utilizarea de algoritmi avansați, se poate reduce considerabil timpul necesar pentru verificarea și administrarea impozitelor, creând în același timp o infrastructură flexibilă și scalabilă. De asemenea, utilizarea acestor soluții reduce dependența de resursele umane, eliminând erorile și asigurând o administrare fiscală mai transparentă și mai eficientă.

Un alt factor major care impune modernizarea urgentă a SFS este procesul de integrare a Republicii Moldova în Uniunea Europeană. În calitate de țară candidată la aderare, Moldova trebuie să-și alinieze politicile și sistemele fiscale la standardele și cerințele UE. Acest lucru presupune integrarea cu platformele europene de schimb de informații fiscale, cum ar fi VAT Information Exchange System (VIES), One Stop Shop (OSS) și Central Electronic System on Payment Information (CESOP). Aceste sisteme sunt esențiale pentru facilitarea tranzacțiilor economice transfrontaliere și pentru reducerea fraudei fiscale prin schimbul rapid și sigur de date fiscale între statele membre ale UE. În lipsa unei infrastructuri al sistemului informațional capabile să susțină aceste integrări, Republica Moldova riscă să rămână în urmă în procesul de armonizare cu politicile europene, afectându-și astfel șansele de aderare și dezvoltare economică pe termen lung.

Totodată, modernizarea infrastructurii sistemului informațional al SFS este necesară și din perspectiva utilizării mai eficiente a resurselor umane și financiare. În momentul de față, multe dintre procesele administrative ale SFS sunt dependente de sisteme învechite, care nu mai sunt capabile să susțină nevoile actuale. Acest lucru duce la o utilizare ineficientă a resurselor, în special în ceea ce

privește costurile de întreținere și operaționale. Prin adoptarea tehnologiilor cloud și a soluțiilor de virtualizare, SFS poate reduce costurile asociate cu achiziționarea și întreținerea echipamentelor hardware tradiționale, permițând totodată o gestionare mai flexibilă și mai eficientă a datelor și a resurselor. Aceste tehnologii permit, de asemenea, o scalare rapidă a capacității de stocare și procesare, ceea ce este esențial pentru a face față volumelor de date în creștere, fără a investi în mod constant în infrastructuri fizice noi.

Un alt aspect important al modernizării îl reprezintă capacitatea de a răspunde rapid la schimbările globale și crizele economice sau sociale, cum a fost, de exemplu, pandemia de COVID-19. În această perioadă, s-a evidențiat necesitatea unor soluții digitale eficiente care să permită contribuabililor să interacționeze cu autoritățile fiscale de la distanță, fără a fi nevoiți să se deplaseze fizic la birourile locale. Lipsa unor astfel de soluții nu numai că afectează eficiența administrativă, dar subminează și încrederea contribuabililor în capacitatea instituției de a le oferi servicii eficiente și sigure. Modernizarea sistemului informațional ar permite dezvoltarea unor platforme online robuste, capabile să susțină o gamă largă de servicii fiscale digitale, accesibile de oriunde și în orice moment.

Astfel, necesitatea modernizării infrastructurii sistemului informațional a Serviciului Fiscal de Stat din Republica Moldova este determinată de o combinație de factori interni și externi, care variază de la creșterea volumului de date fiscale și oportunitățile oferite de noile tehnologii, până la cerințele de conformitate impuse de integrarea europeană. Modernizarea nu doar că va optimiza procesele fiscale, dar va asigura și o mai bună utilizare a resurselor, îmbunătățind în același timp experiența contribuabilului și întărind încrederea publicului în sistemul fiscal. În acest context, modernizarea sistemului informațional reprezintă o prioritate strategică pentru dezvoltarea economică și administrativă a Republicii Moldova și o condiție esențială pentru integrarea sa reușită în Uniunea Europeană.

Implementarea Programului va contribui la atingerea obiectivelor din Componenta 5: Politici fiscale și vamale și administrarea veniturilor din Strategia de dezvoltare a managementului finanțelor publice pentru anii 2023-2030, aprobată prin Hotărârea Guvernului nr. 71/2023, precum și Capitolul 16: Fiscalitate din Programul Național de Aderare a Republicii Moldova la Uniunea Europeană pentru perioada 2025-2029, asigurând o fiscalitate echitabilă, eficientă, sustenabilă și alinierea sistemelor la standardele și cerințele UE.

Aderarea Republicii Moldova la Uniunea Europeană este un proces complex și de lungă durată, care necesită numeroase ajustări economice, politice și sociale. Un domeniu important în acest proces este alinierea administrării fiscale și infrastructurii sistemului informațional ale Republicii Moldova la cerințele Uniunii Europene. Pentru SFS, această aliniere este importantă, deoarece Uniunea Europeană pune un accent deosebit pe eficiență administrativă, combaterea fraudei fiscale și facilitarea schimbului de informații între statele membre.

Un prim pas în această direcție este adoptarea și integrarea platformelor europene de schimb de informații fiscale, care sunt necesare pentru facilitarea tranzacțiilor economice și comerciale transfrontaliere. În acest sens, Republica Moldova trebuie să asigure compatibilitatea infrastructurii sale al sistemului informațional cu sisteme precum VIES (VAT Information Exchange System), OSS (One Stop Shop) și CESOP (Central Electronic System on Payment Information). Aceste sisteme ajută la monitorizarea și gestionarea eficientă a tranzacțiilor economice internaționale, prevenind evaziunea fiscală și consolidând controlul asupra fluxurilor financiare transfrontaliere.

Un alt aspect important al alinierii la cerințele Uniunii Europene este adoptarea și implementarea directivelor DAC (Directives Administrative Cooperation), care reglementează schimbul automat de informații fiscale între statele membre. DAC include o serie de directive care

impun statelor membre obligații de a schimba automat informații cu privire la diverse domenii, inclusiv rulările fiscale (DAC3), rapoartele de țară (DAC4), proprietarii beneficiari (DAC5) și aranjamentele transfrontaliere (DAC6). Pentru a se conforma acestor cerințe, Republica Moldova trebuie să-și dezvolte capacitatea tehnologică de a colecta, procesa și transmite datele necesare conform standardelor impuse de Uniunea Europeană.

De asemenea, alinierea la cerințele europene presupune și o securizare avansată a infrastructurii sistemului informațional și a schimburilor de date, în special în contextul informațiilor sensibile schimbate între autoritățile fiscale. Uniunea Europeană impune standarde ridicate de securitate cibernetică și protecția datelor, ceea ce înseamnă că SFS trebuie să implementeze soluții moderne de securitate cibernetică, precum criptarea datelor, protecția împotriva atacurilor cibernetice (IDS/IPS) și prevenirea scurgerilor de informații (DLP). Aceste măsuri sunt necesare pentru a asigura integritatea și confidențialitatea datelor fiscale transmise între autoritățile fiscale din diferite state membre ale Uniunii Europene.

Pe lângă integrarea tehnologică și securitatea informațiilor, alinierea la cerințele UE impune și o reformare a cadrului legislativ și a procedurilor administrative ale SFS. Legislația națională trebuie ajustată pentru a se conforma directivelor și reglementărilor europene, iar personalul SFS trebuie să fie instruit corespunzător pentru a aplica noile proceduri și standarde impuse de Uniunea Europeană. Acest proces va necesita investiții semnificative în formare și dezvoltare profesională, precum și colaborare strânsă cu experții europeni și autoritățile fiscale din alte state membre.

Așadar, alinierea la cerințele de aderare la Uniunea Europeană este crucială pentru modernizarea SFS și pentru integrarea Republicii Moldova în spațiul fiscal european. Adoptarea platformelor de schimb de informații fiscale, implementarea directivelor DAC și consolidarea securității cibernetice vor permite SFS să își îndeplinească obligațiile față de Uniunea Europeană și să faciliteze o tranziție lină către un sistem fiscal modern, eficient și transparent, compatibil cu standardele europene. Această aliniere va sprijini dezvoltarea economică a țării și va consolida relațiile comerciale și fiscale cu partenerii europeni.

2. Analiza situației

În prezent, SFS se confruntă cu diverse provocări legate de infrastructura sa al sistemului informațional și de procesele interne, care necesită îmbunătățiri semnificative pentru a se alinia la standardele moderne de eficiență și securitate.

O problemă majoră cu care se confruntă SFS este fragmentarea infrastructurii sistemului informațional. Sistemele existente, deși au capacitatea de a gestiona procese importante precum declarațiile fiscale electronice și de evidență a obligațiilor fiscale, sunt dezvoltate pe platforme diferite, cu tehnologii variate. Această fragmentare creează probleme în ceea ce privește integrarea datelor și eficiența operațională. În plus, multe procese sunt încă realizate manual sau semi-manual, ceea ce duce la erori și la o performanță scăzută.

Un exemplu concret îl reprezintă dificultatea în gestionarea integrată a datelor între diferitele registre naționale și internaționale. Sistemele de înregistrare fiscală nu sunt complet compatibile între ele, ceea ce îngreunează accesul rapid și eficient la date. Deși au fost implementate soluții precum SIA „e-Cerere” și sistemul de facturare electronică SIA „e-Factura”, acestea necesită extinderi și îmbunătățiri pentru a facilita o integrare completă și automatizarea proceselor.

Securitatea cibernetică a sistemelor din cadrul sistemului informațional necesită îmbunătățiri majore. În prezent, SFS nu dispune de un sistem robust pentru gestionarea vulnerabilităților și controlul accesului. Protocolul actual de gestionare a incidentelor nu este suficient de bine definit, iar măsurile de protecție împotriva scurgerilor de informații sau atacurilor cibernetice sunt limitate. Este

necesară implementarea unor soluții mai avansate, cum ar fi criptarea end-to-end și sistemele de detectare a intruziunilor (IDS/IPS).

În ceea ce privește automatizarea proceselor de control fiscal, SFS folosește în prezent sisteme de analiză a riscurilor fiscale, însă majoritatea proceselor de control rămân dependente de intervenția manuală. Integrarea datelor și utilizarea analiticii avansate pentru operațiunile de control și conformare sunt încă în faze incipiente, ceea ce limitează capacitatea SFS de a monitoriza și detecta riscurile în timp real.

Sistemele de control și conformare trebuie îmbunătățite pentru a permite colectarea și analiza automată a datelor în timp real. Implementarea unui standard de raportare fiscală primară și adoptarea de soluții avansate de analiză predictivă vor îmbunătăți capacitatea SFS de a identifica fraudele fiscale și de a optimiza procesul de control și conformare.

O altă provocare majoră este capacitatea limitată a infrastructurii sistemului informațional actual de a susține volumul în creștere de date și cerințele analitice avansate. SFS nu dispune încă de un cadru robust de guvernare a datelor, iar accesul la date în timp real este limitat. Integrarea datelor între diferitele sisteme este fragmentată, ceea ce afectează utilizarea eficientă a acestor date pentru luarea deciziilor informate și optimizarea proceselor interne.

Pentru a remedia aceste probleme, este necesară o modernizare extensivă a infrastructurii sistemului informațional, inclusiv dezvoltarea unui cadru formal de guvernare a datelor care să asigure calitatea, securitatea și integritatea datelor. De asemenea, trebuie implementate soluții de big data, inclusiv implementarea conceptului de Data Warehouse și instrumente de business intelligence, care să permită o analiză detaliată și luarea deciziilor bazate pe date, cu un accent special pe riscurile fiscale și conformitatea contribuabililor.

În ansamblu, analiza situației curente a SFS evidențiază necesitatea unei modernizări substanțiale a infrastructurii sistemului informațional. Problemele de fragmentare a sistemelor, lipsa unei guvernări eficiente și automatizarea limitată a proceselor afectează grav eficiența și securitatea administrării fiscale. Pentru a se alinia la cerințele Uniunii Europene și pentru a îmbunătăți performanța, SFS trebuie să implementeze un cadru de guvernare al sistemului informațional solid, să îmbunătățească securitatea cibernetică și să integreze soluții avansate de automatizare și analiză a datelor.

Managementul contribuabililor în administrația fiscală din Republica Moldova implică o serie de procese și măsuri menite să gestioneze eficient contribuabilii și să permită furnizarea de servicii fiscale electronice. Utilizarea tehnologiilor informaționale moderne joacă un rol semnificativ în eficientizarea acestor procese și în creșterea eficienței generale a procesului de administrare fiscală a contribuabililor. De asemenea, oferă oportunitatea de a transforma serviciile digitale de la servicii de tip cerere-executare-răspuns către servicii instantanee de autoservire prin mijloace on-line. Analiza situației actuale se va prezenta conform principalelor procese de bază (core processes).

Înregistrarea contribuabililor:

O componentă importantă a procesului de administrare fiscală a contribuabililor este sistemul informațional automatizat „e-Cerere” (*în continuare – SIA „e-Cerere”*), care permite contribuabililor să depună diverse cereri în format electronic. SIA „e-Cerere” este o soluție informațională menită să înlocuiască procedura tradițională de depunere a cererilor de către contribuabili cu un mecanism modern, bazat pe tehnologii informaționale.

Astfel, sistemul permite procesarea electronică a cererilor depuse on-line de către contribuabili și emiterea certificatelor de către SFS cu utilizarea semnăturii electronice pentru:

1. înregistrarea/anularea în calitate de plătitor de TVA;
2. înregistrarea on-line a contribuabililor/obiectelor impozabile;

3. înregistrarea/anularea în calitate de plătitor de Accize
4. efectuarea/amânarea controalelor fiscale;
5. modificarea perioadei fiscale;
6. eliberarea confirmării veniturilor;
7. stingerea obligației fiscale prin compensare și/sau restituirea mijloacelor bănești;
8. înregistrarea contractelor de locațiune;
9. eliberarea patentei de întreprinzător.

Nr. d/o	Denumirea serviciului din cadrul SIA „e-Cerere”	Total solicitări	Total solicitări Online	Total solicitări Ghișeu
1	Certificat de atribuire a codului fiscal	163 930	20	163 910
2	Înregistrarea activității de prelucrare și/sau fabricare a mărfurilor supuse accizelor	38	32	6
3	Înregistrarea on-line a contribuabililor	8 577	6	8 571
4	Înregistrarea subdiviziunilor/obiectelor impozabile	76 433	60 432	16 001
5	Confirmarea privind veniturile obținute în Republica Moldova de persoanele fizice cetățeni ai Republicii Moldova	14 722	209	14 513
6	Eliberarea/prelungirea patentei de întreprinzător	38 618	93	38 525
Total		302 318	60 792	241 526

Efectuând analiza datelor dintre numărul total de solicitări depuse în regim online și numărul de solicitări la ghișeu, se atestă că totuși contribuabilii în mare parte preferă procedura tradițională.

Declarații fiscale și raportare:

Pentru depunerea declarațiilor fiscale este utilizat sistemul informațional automatizat „Declarație electronică”. În vederea implementării mecanismului de obligativitate a utilizării metodelor automatizate de raportare, SFS a avut o abordare etapizată prin conformarea treptată a contribuabililor în vederea utilizării mecanismului de raportare electronică. Acest lucru poate fi observat prin prisma modificărilor efectuate la art. 187 alin.(2¹) din Codul fiscal, inițiate încă din anul 2011.

Astfel, în anul 2024 avem o rată de **84,49%** de prezentare a dărilor de seamă fiscală prin metode automatizate de raportare electronică (1 578 045 declarații electronice din totalul de 1 867 685 declarații prezentate).

Colectarea impozitelor și taxelor:

Sistemul informațional automatizat „Contul curent al contribuabilului” permite accesul la informațiile privind obligațiile fiscale ale contribuabililor și verificarea situației actuale a tuturor restanțelor sau sumelor plătite în plus către bugetul public național. În situația actuală se atestă o perioadă de actualizare a datelor care se desfășoară cu întârziere, în cazul plăților procesarea se desfășoară într-o perioadă de la 1 zi la 5 zile, iar calculul cu 1 zile întârziere, or acest proces ar trebui să fie unul instant.

Modulul „Contul unic”, facilitează plata obligațiilor fiscale, oferind oportunitatea achitării tuturor obligațiilor fiscale printr-o singură plată. În anul 2019, modulul „Cont unic” a fost integrat cu serviciul guvernamental MPay, care permite plata obligațiilor fiscale direct de pe interfața modulului menționat, fără necesitatea imprimării și remiterii ordinului de plată la prestatorul de servicii de plată.

Acțiuni de conformare fiscală

SFS este relativ precar în ceea ce privește abundența și disponibilitatea datelor, nu dispune de suficiente integrări de date cu părți terțe și, de fapt, nu utilizează în mod eficient instrumente de analiză generală și/sau avansată pentru a obține valoare din date.

Guvernanța datelor este centralizată și definită prin aplicarea bunelor practici de management în cadrul SFS. SFS trebuie să își îmbunătățească capacitatea de a ști ce tip de date, momentul și modul în care le gestionează, să îmbunătățească în mod sistematic calitatea datelor și să aplice bune practici de guvernanță a datelor.

În prezent, SFS nu poate îmbunătăți în mod semnificativ procesele fiscale de bază fără a consolida sistemul informațional al SFS (SISFS), sub o singură platformă standardizată. Îmbunătățirile părților separate pot aduce mici câștiguri, dar nu schimbări strategice. Principalele limitări sunt următoarele:

1. Infrastructură TIC (Tehnologia informației și comunicațiilor) la IP CTIF aflată la sfârșitul duratei de viață și necesită investiții de capital importante.
2. Tranziția limitată sau imposibilă, a sistemelor dezvoltate pe tehnologii învechite, către Centrul de date al STISC (Serviciul tehnologia informației și securitate cibernetică).
3. O mare varietate de tehnologii utilizate în trecut pentru a crea sisteme de aplicații, neactualizate și potențial vulnerabile la amenințări cibernetice.

Beneficiile exploatării unei infrastructuri TIC și a unei platforme de aplicații standardizate se vor concretiza prin reducerea riscurilor operaționale, a capacității de gestionare, a agilității și a pregătirii pentru schimbări, a costurilor de întreținere și operaționale, a posibilității de a se axa pe dezvoltarea de servicii complementare (non-core), asigurarea calității datelor și multe altele.

Servicii pentru contribuabili:

SFS, ca instituție publică, nu poate funcționa izolată de publicul său, publicul care îi conferă, întrucâtva, legitimitate. Pentru a primi un răspuns favorabil din partea persoanelor pentru care desfășoară activități, trebuie să-și exprime intențiile, să-și creeze o imagine solidă și să se supună unui imperativ: de a se apropia de public prin adaptarea structurii organizaționale la cerințele și/sau așteptările acestuia.

Acest lucru se realizează prin intermediul canalelor existente de comunicare: pagina web oficială www.sfs.md, paginile de pe rețele de socializare (Facebook, Instagram, LinkedIn, Telegram), canalul de Youtube, modulul „Mesagerie” din cadrul SIA „Cabinetul personal al contribuabilului”, seminare de instruire, ședințe cu mediul de afaceri/grupuri de contabili, etc.

Formarea opiniei publice pentru dezvoltarea unei conștiințe fiscale reprezintă o sarcină pe care organizația fiscală și-a asumat-o și va continua să o dezvolte în viitor.

SFS din Republica Moldova se confruntă cu o serie de lacune tehnologice care împiedică optimizarea activităților sale și eficiența în administrarea fiscală. Identificarea acestor lacune este necesară pentru dezvoltarea unui plan de modernizare bine structurat, care să permită alinierea infrastructurii sistemului informațional la cerințele Uniunii Europene și la standardele moderne de eficiență și securitate.

Multe dintre sistemele sistemului informațional existente în cadrul SFS sunt construite pe tehnologii învechite, care nu mai răspund nevoilor actuale de procesare și gestionare a datelor. Aceste sisteme nu sunt integrate eficient, ceea ce duce la dificultăți majore în transferul și utilizarea datelor între departamentele interne și între SFS și alte instituții naționale sau internaționale. Lipsa interoperabilității între diferitele sisteme nu permite accesul eficient și rapid la informații esențiale, ceea ce afectează negativ procesele administrative și de audit.

Volumul de date gestionat de SFS crește continuu, însă capacitatea de stocare și procesare a datelor rămâne limitată. În lipsa unor soluții moderne de cloud computing și de virtualizare a resurselor, SFS se confruntă cu probleme legate de supraîncărcarea serverelor și de eficiența scăzută

a procesării datelor. Această limitare îngreunează analiza datelor și implementarea de soluții avansate de monitorizare a riscurilor fiscale sau de predicție a comportamentului contribuabililor.

Securitatea cibernetică reprezintă un domeniu important în care SFS are nevoie de îmbunătățiri semnificative. Infrastructura actuală nu este pregătită să facă față provocărilor moderne legate de atacurile cibernetice, iar măsurile de protecție existente sunt insuficiente. Sistemele actuale nu beneficiază de protecție avansată împotriva intruziunilor (cum ar fi IDS/IPS), iar lipsa criptării avansate pentru comunicarea datelor sensibile expune organizația unor riscuri semnificative. În plus, procesele de gestionare a incidentelor de securitate nu sunt bine definite, ceea ce crește vulnerabilitatea la atacuri și la scurgerile de informații.

O altă lacună majoră o reprezintă lipsa unei automatizări extinse a proceselor fiscale. În multe cazuri, contribuabilii și personalul SFS trebuie să gestioneze manual procese care ar putea fi automatizate cu ajutorul tehnologiei moderne. Această dependență de proceduri manuale îngreunează activitatea, reduce eficiența și crește riscul de erori umane. Automatizarea proceselor, precum validarea și verificarea declarațiilor fiscale, ar putea reduce semnificativ sarcinile administrative și ar îmbunătăți colectarea și conformitatea fiscală.

Pentru a răspunde acestor provocări, SFS trebuie să investească în modernizarea infrastructurii sale IT. Acest lucru presupune:

1. Implementarea soluțiilor de cloud computing pentru scalabilitate și acces rapid la resursele de stocare și procesare.
2. Virtualizarea resurselor sistemului informațional pentru a crește eficiența utilizării serverelor și pentru a reduce costurile de întreținere a echipamentelor fizice.
3. Dezvoltarea unui sistem de guvernanta a datelor, care să includă proceduri clare pentru colectarea, validarea și stocarea datelor fiscale, asigurând astfel calitatea și securitatea informațiilor.
4. Îmbunătățirea securității cibernetice prin implementarea de măsuri avansate de protecție, inclusiv criptare, detectarea și prevenirea intruziunilor, precum și protocoale clare de gestionare a incidentelor.
5. Automatizarea proceselor fiscale pentru a reduce volumul de muncă manuală și pentru a asigura eficiența în administrarea taxelor și impozitelor.
6. Implementarea unei soluții de tip data warehouse pentru stocarea și gestionarea eficientă a datelor fiscale. În contextul volumului și complexitatea informațiilor care necesită a fi procesate, considerăm că un astfel de sistem ar contribui semnificativ la optimizarea proceselor, îmbunătățirea performanței și asigurarea unui management adecvat al datelor.

Aceste lacune tehnologice indică necesitatea unui plan de modernizare amplu, care să transforme SFS într-o instituție fiscală modernă, capabilă să gestioneze eficient datele și să ofere servicii digitale contribuabililor, în conformitate cu cerințele Uniunii Europene.

Evaluarea riscurilor actuale la SFS relevă o serie de vulnerabilități tehnologice și administrative care necesită o abordare strategică pentru a asigura o tranziție eficientă către cerințele impuse de integrarea cu Uniunea Europeană. Aceste riscuri sunt direct legate de starea actuală a infrastructurii sistemului informațional, fragmentarea sistemelor și lipsa unui cadru clar de guvernanta a datelor, care împiedică o gestionare eficientă și sigură a informațiilor fiscale. Fără o modernizare semnificativă și o consolidare a resurselor, SFS riscă să rămână în urmă în procesul de aliniere la standardele europene.

Un prim risc major identificat este securitatea cibernetică deficitară, care expune infrastructura IT a SFS la atacuri cibernetice și scurgeri de informații sensibile. În contextul cerințelor stricte de protecție a datelor impuse de Uniunea Europeană, securitatea cibernetică reprezintă o

prioritate absolută. În absența unor soluții avansate, cum ar fi criptarea end-to-end, sistemele de detectare și prevenire a intruziunilor (IDS/IPS) și protocoalele clare de gestionare a incidentelor, SFS nu poate asigura integritatea și confidențialitatea datelor fiscale gestionate. Această vulnerabilitate nu doar că amenință securitatea operațională a organizației, dar poate compromite și încrederea contribuabililor, esențială pentru eficiența administrării fiscale.

Un alt risc important este fragmentarea sistemelor sistemului informațional, care afectează interoperabilitatea și schimbul rapid de informații. Pentru a se alinia cu cerințele europene, SFS trebuie să își îmbunătățească capacitatea de a integra și utiliza datele la nivel național și internațional. Lipsa de interoperabilitate între sistemele interne și cele externe limitează accesul la informații și împiedică schimburile rapide de date fiscale între Republica Moldova și statele membre ale Uniunii Europene. Această problemă devine mai critică în contextul unor platforme esențiale, precum VIES (VAT Information Exchange System) și OSS (One Stop Shop), care impun integrarea rapidă și fără erori a datelor fiscale transfrontaliere.

Un al treilea risc semnificativ este dependența de procese manuale și lipsa automatizării în procesele fiscale. Aceste deficiențe nu doar că încetinesc operațiunile, dar și cresc riscul de erori umane și reduc eficiența colectării fiscale. Automatizarea proceselor este o cerință majoră pentru conformitatea cu reglementările europene, mai ales în contextul schimburilor de informații automate și al raportărilor fiscale. Fără o integrare completă a soluțiilor digitale, SFS nu va putea răspunde cerințelor de eficiență și transparență fiscală impuse de Uniunea Europeană.

Lipsa unui cadru formal de guvernare a datelor este un alt factor care agravează riscurile actuale. Standardele europene cer o gestionare riguroasă a datelor, care să asigure calitatea, securitatea și integritatea acestora. Fără un sistem formalizat de guvernare a datelor, SFS riscă să gestioneze date incomplete, redundante sau inaccesibile, ceea ce afectează deciziile strategice și operaționale. Integrarea cu UE necesită un management coerent al datelor, care să permită accesul rapid și sigur la informații fiscale de înaltă calitate, pentru schimburile transfrontaliere.

Necesarul de modernizare devine evident în contextul acestor riscuri. Pentru a se alinia cerințelor Uniunii Europene, SFS trebuie să investească urgent în tehnologii moderne, să îmbunătățească securitatea cibernetică, să automatizeze procesele fiscale și să implementeze un cadru robust de guvernare a datelor. În caz contrar, există riscul de a nu respecta termenele impuse de procesul de integrare și de a rămâne în urmă în ceea ce privește eficiența și transparența fiscală, necesare pentru aderarea la Uniunea Europeană.

Astfel, evaluarea riscurilor actuale scoate în evidență nevoia stringentă de modernizare și integrare. Alinierea la standardele europene nu doar că va îmbunătăți eficiența operațională a SFS, dar va asigura și conformitatea cu reglementările europene, consolidând încrederea în sistemul fiscal și facilitând procesul de aderare la Uniunea Europeană.

3. Obiective generale și specifice ale Programului

Această secțiune stabilește obiectivele generale pe termen mediu aliniate conform Strategiei de dezvoltare a managementului finanțelor publice și Programului Național de Aderare la UE, precum și măsuri/mecanisme pentru atingerea acestor obiective. În plus, stabilește indicatori de performanță și monitorizează progresul așteptat al SFS, rezultatele și efectul financiar, precum și prioritățile pentru fiecare fază a implementării Programului în sine.

3.1. Obiectiv general: Asigurarea eficientizării administrării fiscale prin creșterea calității serviciilor fiscale prestate, digitalizarea proceselor fiscale și creșterea gradului de satisfacție al contribuabililor

Dezvoltarea unui sistem fiscal durabil, nu poate avea loc fără un sistem informațional automatizat care gestionează riscurile de neconformare fiscală și înseamnă, în esență, crearea unui domeniu digital, care colectează date din surse multiple (cum ar fi declarații fiscale sau informații financiare), le analizează și oferă semnale timpurii atunci când există motive de îngrijorare. Practic, acest sistem funcționează ca un detector de nereguli, bazându-se pe algoritmi și modele care pot să recunoască tipare suspecte și să stabilească cine are nevoie de atenție din partea SFS.

Avantajul major este că, în loc să verifice fiecare contribuabil în parte la întâmplare, inspectorii fiscali pot să se concentreze pe cazurile cu adevărat riscante, economisind timp și resurse. De asemenea, pentru contribuabilii onești, acest mecanism asigură un sentiment de echitate: șansele de a fi controlați din greșeală scad, iar aceștia văd cum administrația fiscală își folosește datele într-un mod transparent.

Pe lângă depistarea potențialelor încălcări, acest sistem informațional ajută și la crearea unor politici fiscale mai bine adaptate, pentru că scoate la iveală tiparele de neconformare și oferă o imagine de ansamblu a situației reale. Nu în ultimul rând, soluția respectă regulile privind protecția datelor și include mecanisme de securitate care asigură confidențialitatea informațiilor, astfel încât cei care își desfășoară activitatea corect nu au de ce să-și facă griji.

Realizarea acestui obiectiv general se va asigura prin următoarele direcții prioritare:

- 1) Simplificarea și digitalizarea serviciilor și procedurilor fiscale.
- 2) Dezvoltarea Sistemului informațional al Serviciului Fiscal de Stat.
- 3) Creșterea calității serviciilor destinate contribuabililor, inclusiv a serviciilor electronice.
- 4) Creșterea eficienței controalelor fiscale asigurată prin îmbunătățirea proceselor de control fiscal.

Rezultate pe termen lung:

- 1) Sisteme informaționale modernizate, care oferă funcționalitățile necesare pentru administrarea fiscală modernă.
- 2) Costuri de administrare fiscală reduse.
- 3) Grad de conformare voluntară a contribuabililor majorat.

Obiectiv specific 1.1: Simplificarea și digitalizarea serviciilor și procedurilor fiscale

Indicatori: $\geq 95\%$ servicii digitalizate în 2026; 100% în 2027; ≥ 1 sondaj de opinie anual; 1 declarație precompletată implementată.

Obiectiv specific 1.2: Automatizarea proceselor de colectare a veniturilor

Indicatori: timp de procesare dări de seamă și plăți redus cu 90%; 1 sistem informațional dezvoltat de management a riscurilor de neconformare fiscală; ≥ 20 tipuri de notificări automatizate în 2027; $\geq 98\%$ cazuri confirmate de neconformare în urma controalelor

Obiectiv specific 1.3: Instituirea unui cadru funcțional de governanță a datelor

Indicatori: Ordin SFS privind politica emis (până în 2025); Glosar și dicționar de date aprobate; Conectarea surselor de date la DataLake: 50% (2026), 100% (2027).

Obiectiv specific 1.4: Dezvoltarea competențelor instituționale în analiza riscurilor fiscale

Indicatori: Subdiviziune BI creată și funcțională cu 3 angajați; Cel puțin 2 instruirii desfășurate până în 2027; Cel puțin 1 acord semnat cu universități (2027); Ordin SFS pentru numirea ofițerului de date emis (2025).

Obiectiv specific 1.5: Modernizarea integrală a Centrului de Date

Indicatori: 90% virtualizare în 2026, 100% în 2027; Centru de date modernizat 100% până în 2027; Infrastructura SFS monitorizată prin SIEM: 50% (2026), 70% (2027)

Obiectiv specific 1.6: Asigurarea securității cibernetice avansate

În contextul modernizării Serviciului Fiscal de Stat (SFS) și alinierii la cerințele Uniunii Europene, este esențial să înțelegem conceptul de **infrastructură al sistemului informațional** și componentele cheie ale **securității cibernetice**. Aceste concepte reprezintă pilonii pe care se va baza dezvoltarea și protecția datelor, garantând astfel eficiența, disponibilitatea și securitatea informațiilor fiscale.

Infrastructura sistemului informațional se referă la totalitatea componentelor hardware, software, rețele și resurse necesare pentru funcționarea eficientă a unui sistem informațional. În cadrul SFS, aceasta include:

1. **Data Centru**, care este nucleul infrastructurii IT, unde se stochează și se procesează datele critice. Un centru de date modernizat va asigura scalabilitatea și redundanța necesare pentru a face față volumelor mari de informații fiscale și pentru a oferi continuitate în caz de incidente. Prin utilizarea soluțiilor de stocare redundantă (SAN/NAS) și a tehnologiilor de recuperare în caz de dezastru (DR), SFS va putea proteja datele esențiale și asigura continuitatea operațiunilor.
2. **Tehnologiile de virtualizare** permit rularea mai multor sisteme și aplicații pe o singură platformă hardware, crescând astfel eficiența utilizării resurselor. Virtualizarea reduce costurile, permite un management mai flexibil al resurselor și îmbunătățește recuperarea în caz de incidente, făcând infrastructura sistemului informațional mai agilă și mai rezistentă la avarii.
3. **Rețelele locale (LAN)** conectează serverele și dispozitivele din cadrul instituției, în timp ce rețelele externe permit conectarea la alte instituții și platforme internaționale. Segmentarea rețelelor prin utilizarea VLAN-urilor (Virtual Local Area Network) și implementarea soluțiilor de optimizare a traficului asigură performanță și securitate ridicate, prevenind accesul neautorizat la resursele critice.
4. **Rețele Private Virtuale (VPN)** sunt esențiale pentru accesul securizat la distanță al angajaților și partenerilor, mai ales în contextul colaborărilor internaționale. Aceste rețele folosesc criptarea pentru a proteja datele transmise și autentificarea multifactorială (MFA) pentru a preveni accesul neautorizat.
5. Pe măsură ce digitalizarea avansează, **securitatea cibernetică** devine o prioritate, inclusiv la nivel de stat. Protejarea datelor fiscale sensibile și a infrastructurii sistemului informațional împotriva atacurilor cibernetice este esențială pentru menținerea încrederii contribuabililor și conformitatea cu standardele internaționale. Principalele componente ale securității cibernetice în cadrul SFS includ:
6. **SIEM (Security Information and Event Management)**, care colectează, analizează și monitorizează în timp real evenimentele de securitate din infrastructura sistemului

informațional. Acesta poate detecta și răspunde rapid la atacuri cibernetice, cum ar fi încercările de acces neautorizat, și poate emite alerte atunci când sunt detectate anomalii. Prin implementarea unui SIEM centralizat, SFS va avea o vizibilitate completă asupra incidentelor de securitate și va putea răspunde pro activ la acestea.

7. **Sistemele DLP (Data Loss Prevention)** previn scurgerile de informații sensibile, asigurându-se că datele fiscale importante nu părăsesc sistemul neautorizat. Aceste sisteme monitorizează fluxurile de date și impun politici stricte de control al accesului și transferului de informații. Implementarea unui DLP va proteja SFS împotriva pierderii accidentale sau intenționate a datelor critice.
8. **Firewall și IDS/IPS (Intrusion Detection/Prevention Systems)** sunt componente esențiale pentru protejarea infrastructurii de rețea. Firewall-urile controlează accesul la rețea, permițând doar traficul legitim, în timp ce sistemele IDS/IPS detectează și previn atacurile cibernetice, cum ar fi tentativele de penetrare sau exploatarea vulnerabilităților.
9. **Criptarea și securizarea comunicațiilor** reprezintă un element de protecție a datelor în tranzit, importantă pentru schimburile de informații cu partenerii internaționali și contribuabilii. Criptarea end-to-end și utilizarea soluțiilor VPN asigură că datele sunt protejate împotriva interceptării neautorizate, asigurând totodată integritatea și confidențialitatea acestora.

Indicatori: Politica de securitate aprobată (2026); ≥ 2 instruirii anuale privind măsurile de protecție; DLP activ pe 1200 stații din 1600 în 2027; ≥ 1 audit de securitate realizat anual; Comunicații criptate: 30% (2026), 40% (2027).

Obiectiv specific 1.7: Asigurarea interoperabilității și integrării cu sistemele informaționale europene

Integrarea Republicii Moldova în Uniunea Europeană reprezintă un obiectiv strategic de importanță națională, implicând transformări semnificative în multiple sectoare. Un element esențial al acestui proces îl constituie alinierea și integrarea în sistemele informaționale europene. Acest program de dezvoltare al sistemului informațional își propune să stabilească direcțiile și acțiunile necesare pentru a asigura interoperabilitatea, securitatea și eficiența schimbului de informații cu statele membre ale UE, contribuind astfel la dezvoltarea socio-economică a țării și la creșterea bunăstării cetățenilor.

Obiectivele strategice includ armonizarea cadrului legislativ și normativ, standardizarea și interoperabilitatea tehnologică, consolidarea securității cibernetice, dezvoltarea capitalului uman și a competențelor digitale, modernizarea infrastructurii sistemului informațional și participarea activă la inițiative și programe europene. Adaptarea legislației naționale la acquis-ul comunitar în domeniul tehnologiei informației și comunicațiilor va crea un mediu legal propice integrării în sistemele informaționale ale UE. Este imperativă adoptarea și implementarea integrală a Regulamentului General privind Protecția Datelor (GDPR) pentru a asigura un nivel înalt de protecție a datelor și a facilita schimbul de informații cu statele membre. De asemenea, implementarea [Directivei NIS 2](#) prin prisma strategiei naționale de securitate cibernetică sunt importante pentru a răspunde provocărilor actuale în materie de securitate.

Asigurarea compatibilității tehnice cu sistemele europene se va realiza prin adoptarea standardelor și specificațiilor tehnice recunoscute la nivelul UE. Implementarea protocoalelor și a formatelor de date standardizate va facilita interoperabilitatea sistemelor și va permite un schimb de informații eficient și securizat. Obținerea certificărilor necesare pentru infrastructurile și serviciile

sistemului informațional, conform standardelor și normelor europene, va garanta calitatea și fiabilitatea acestora.

Dezvoltarea unui cadru robust de securitate cibernetică este esențială pentru protejarea infrastructurii IT naționale și asigurarea rezilienței în fața amenințărilor cibernetice. Aceasta implică stabilirea unui cadru legislativ și operațional care să includă politici, proceduri și mecanisme de răspuns la incidente cibernetice. Participarea la rețele și inițiative europene în domeniul securității cibernetice și colaborarea cu agenții precum ENISA vor întări capacitatea de a face față provocărilor transfrontaliere. Identificarea și securizarea infrastructurilor sistemului informațional critice sunt, de asemenea, priorități pentru asigurarea funcționării continue a societății și economiei.

Investiția în educație și formare profesională este vitală pentru dezvoltarea capitalului uman și a competențelor digitale. Integrarea competențelor digitale în curricula educațională și promovarea programelor de formare continuă pentru specialiști IT vor contribui la crearea unei forțe de muncă calificate. Facilitarea participării la programe de schimb și cooperare cu instituții de învățământ și organizații din UE va încuraja transferul de cunoștințe și bune practici.

Modernizarea infrastructurii tehnologice este necesară pentru a satisface cerințele de performanță și scalabilitate impuse de integrarea europeană. Alocarea de resurse pentru modernizarea rețelilor de comunicații, a centrelor de date și a infrastructurilor cloud va asigura capacitatea tehnică necesară. Adoptarea tehnologiilor emergente, precum inteligența artificială, big data și Internet of Things (IoT), va stimula inovația și va spori competitivitatea economică.

Participarea activă la inițiative și programe europene oferă oportunități de dezvoltare și acces la resurse, expertiză și finanțare în domeniul digitalizării. Accesarea fondurilor disponibile prin programe precum Europa Digitală și Horizon Europe va sprijini implementarea proiectelor strategice. Stabilirea de parteneriate cu entități publice și private din UE va facilita implementarea proiectelor comune și va consolida relațiile internaționale.

Implementarea Programului de dezvoltare al sistemului informațional va fi coordonată de un comitet interministerial responsabil cu supravegherea progresului și asigurarea coerenței între diferitele domenii de acțiune. Se vor stabili indicatori de performanță cheie pentru a monitoriza eficient evoluția și pentru a ajusta măsurile, dacă este necesar. Raportarea periodică și transparentă către Guvern și public va asigura responsabilitatea și implicarea tuturor părților interesate.

În acest sens, urmează să fie asigurată interoperabilitatea cu următoarele sisteme/aplicații:

1. TVA

a. VIES – VAT Information Exchange System

VIES (Sistemul de Schimb de Informații privind TVA) este un sistem electronic al Uniunii Europene care permite verificarea numerelor de înregistrare în scopuri de TVA ale companiilor înregistrate în statele membre. Acesta facilitează schimbul de informații privind TVA între autoritățile fiscale ale țărilor UE pentru a combate fraudă fiscală și a asigura conformitatea.

b. OSS – One Stop Shop

OSS (Punct Unic de Contact) este un sistem implementat de UE pentru a simplifica obligațiile de TVA ale companiilor care furnizează servicii și bunuri transfrontaliere. Prin OSS, companiile pot declara și plăti TVA într-un singur stat membru, evitând necesitatea de a se înregistra fiscal în fiecare țară în care au clienți.

c. CESOP – Central electronic system on payment information

CESOP (Sistemul Electronic Central privind Informațiile de Plată) este o platformă centralizată creată de UE pentru colectarea și schimbul de informații privind plățile transfrontaliere.

Scopul principal al CESOP este de a combate fraudă în domeniul TVA, în special în contextul comerțului electronic, prin monitorizarea fluxurilor financiare între statele membre.

d. ViDA – Vat in the digital age

ViDA (TVA în Epoca Digitală) este o inițiativă a Uniunii Europene care vizează modernizarea sistemului de TVA pentru a se adapta provocărilor și oportunităților aduse de economia digitală. Aceasta include propuneri legislative și măsuri menite să îmbunătățească colectarea TVA și să reducă fraudă fiscală în contextul comerțului electronic și al serviciilor digitale.

e. Alte sisteme

2. Accize

a. EMCS – Excise movement and control system

Pe lângă sistemele informaționale ale UE, la care autoritatea competentă din Republica Moldova urmează să se conecteze la platformele de conectare, este necesar de implementat următoarele schimburi de date:

- a. DAC1 (Standard Transmission Format) - stabilește cadrul general pentru cooperarea administrativă în domeniul fiscal și prevede schimbul de informații la cerere, facilitând investigarea cazurilor specifice de evaziune fiscală.
- b. DAC2 (Common reporting standard) - Introduce schimbul automat de informații privind conturile financiare ale nerezidenților, conform Standardului Comun de Raportare (CRS) al OCDE, permițând depistarea veniturilor ascunse în străinătate.
- c. DAC3 (Exchange of tax rulings) - Prevede schimbul automat de informații referitoare la deciziile fiscale anticipate și acordurile de preț în avans, sporind transparența în practicile fiscale ale companiilor multinaționale.
- d. DAC4 (Country by country reporting) - Introduce raportarea țară cu țară pentru grupurile multinaționale, oferind autorităților fiscale o imagine de ansamblu asupra distribuției profiturilor și impozitelor plătite.
- e. DAC5 (beneficial ownership information as collected under Anti-Money Laundering rules (AML)) - Extinde accesul autorităților fiscale la informațiile privind beneficiarii reali ai entităților juridice, contribuind la combaterea spălării banilor și a finanțării terorismului.
- f. DAC6 (Cross-border tax arrangements) - Impune intermediarilor fiscali obligația de a raporta aranjamentele fiscale transfrontaliere care prezintă semne distinctive de planificare fiscală agresivă, prevenind astfel evitarea obligațiilor fiscale.
- g. DAC7 (Model Reporting for Digital Platforms) - Extinde schimbul automat de informații la platformele digitale, obligând operatorii să raporteze veniturile obținute de vânzători și prestatorii de servicii, abordând provocările economiei digitale.
- h. DAC8 (Crypto Asset Reporting Framework) - Include cripto-activelor și monedele electronice în sfera de aplicare a schimbului automat de informații, prevenind utilizarea acestora în scopuri de evaziune fiscală și spălare de bani.
- i. DAC9 (Global Anti-Base Erosion Model Rules) - Vizează îmbunătățirea și actualizarea cadrului existent de cooperare administrativă, sporind eficiența și eficacitatea schimbului de informații fiscale între statele membre.

Întru realizarea schimburilor de date cu UE, utilizând aplicații, sistemele și prin intermediul Directivelor UE, este necesar de conectat la platforme de comunicare, inclusiv

1. CCN/CSI – Common Communication Network/Common System Interface. Care este o infrastructură securizată destinată schimbului de informații între administrațiile naționale și instituțiile Uniunii Europene, în special în domeniile vamal și fiscal. CCN/CSI facilitează interoperabilitatea între diferitele sisteme informatice ale statelor membre, permițând un flux eficient și securizat de date. Acesta asigură fluxul de date pentru următoarele sisteme:
 - a. VIES - VAT Information Exchange System
 - b. OSS – One Stop Shop
 - c. DAC1
 - d. DAC2
 - e. DAC4
 - f. altele
2. CCN Mail, care este un serviciu de mesagerie electronică securizată integrat în cadrul CCN/CSI. Acesta permite transmiterea de mesaje și documente sensibile între autoritățile naționale și instituțiile europene, asigurând confidențialitatea și integritatea informațiilor schimbate. CCN Mail este esențial pentru comunicarea rapidă și sigură în cadrul Uniunii Europene. Acesta asigură fluxul de date pentru următoarele sisteme:
 - a. EOIR (Exchange of information on request)
3. CCN2 - Common Communication Network (v.2), reprezintă evoluția de nouă generație a infrastructurii CCN. Această versiune îmbunătățită oferă performanțe superioare, scalabilitate și securitate sporită, răspunzând cerințelor crescute de comunicare și integrare ale statelor membre și ale instituțiilor UE. CCN2 suportă un număr mai mare de aplicații și servicii, facilitând o cooperare și mai strânsă la nivel european. Acesta asigură fluxul de date pentru următoarele sisteme:
 - a. SME (Small and medium-sized enterprises)
 - b. altele
4. eDelivery, care este o inițiativă a Comisiei Europene care furnizează specificații tehnice și standarde pentru schimbul securizat și fiabil de date între administrațiile publice, companii și cetățeni. Bazându-se pe un model descentralizat și pe standarde deschise, eDelivery asigură interoperabilitatea și compatibilitatea între diferitele sisteme și platforme la nivel european, facilitând comunicarea transfrontalieră. Acesta asigură fluxul de date pentru următoarele sisteme:
 - a. CESOP – System on Payment Data
 - b. altele
5. Central Directory, care este un component central al infrastructurii CCN/CSI care stochează informații esențiale despre participanții la rețea, inclusiv date de contact și rutare. Acesta permite gestionarea eficientă a informațiilor despre entitățile conectate, asigurând o comunicare fluentă și securizată între diferitele sisteme și platforme implicate: Acesta asigură fluxul de date pentru următoarele sisteme:
 - a. DAC7
 - b. altele
6. eFCA (Electronic Forms Carrier Application) este o platformă electronică destinată gestionării și schimbului de formulare și documente oficiale în format digital între statele membre și instituțiile UE. Prin intermediul eFCA, se facilitează procesarea rapidă și eficientă a documentelor, reducând sarcinile administrative și îmbunătățind transparența și colaborarea între diferitele entități. Acesta asigură fluxul de date pentru următoarele sisteme:
 - a. EOIR (Exchange of information on request)

b. altele

Indicatori: Cerințe tehnice identificate pentru 2 sisteme/an; Acte de testare și acceptare elaborate anual; Cel puțin 1 misiune TAIEX și 2 sesiuni FISCALIS până în anul 2027.

4. Impact

Implementarea Programului de dezvoltare al sistemului informațional al SFS va avea efecte semnificative pe termen mediu, contribuind la atingerea indicatorilor de rezultat și de impact prevăzuți. Aceste efecte se manifestă în mai multe domenii esențiale:

1) Creșterea eficienței administrative și operaționale

Prin digitalizarea serviciilor publice și automatizarea proceselor de administrare fiscală, se va reduce semnificativ timpul necesar pentru procesarea datelor și pentru administrarea obligațiilor fiscale. Automatizarea va contribui la:

- a) Scăderea timpului de verificare și procesare a dărilor de seamă fiscale.
- b) Eliminarea erorilor umane prin utilizarea sistemelor inteligente de analiză a riscurilor.
- c) Reducerea costurilor operaționale prin minimizarea dependenței de procese manuale.

2) Îmbunătățirea capacității de analiză a datelor

Implementarea unui sistem integrat de analiză a datelor va permite Serviciului Fiscal de Stat să identifice mai rapid riscurile de neconformitate și să îmbunătățească colectarea veniturilor. Beneficiile includ:

- a) Crearea unei subdiviziuni de business intelligence (BI) pentru analiza datelor fiscale.
- b) Integrarea inteligenței artificiale în procesele de control fiscal.
- c) Creșterea diversității și volumului de date disponibile pentru luarea deciziilor strategice.

3) Consolidarea securității sistemului informațional și protecția datelor

O infrastructură al sistemului informațional modernă va reduce vulnerabilitățile legate de securitatea cibernetică. Printre măsurile implementate se numără:

- a) Adoptarea unui sistem de detecție și prevenire a intruziunilor (IDS/IPS).
- b) Implementarea unui mecanism robust de monitorizare a securității.
- c) Consolidarea protecției datelor prin utilizarea criptării și a protocoalelor avansate de securitate.

4) Alinierea la standardele Uniunii Europene

Un aspect fundamental al programului este interoperabilitatea cu sistemele informatice europene. Acest lucru va permite Republicii Moldova să își armonizeze politicile fiscale cu cele ale UE și să asigure conformitatea cu regulamentele europene, precum:

- a) VAT Information Exchange System (VIES).
- b) One Stop Shop (OSS).
- c) Central Electronic System on Payment Information (CESOP).

Aceste măsuri vor avea un impact economic și social durabil, îmbunătățind transparența, eficiența administrativă și încrederea publicului în sistemul fiscal.

5. Costuri

Finanțarea acțiunilor prevăzute în cadrul prezentului Program se va efectua pe principiile de sinergie și complementaritate din contul și în limitele mijloacelor aprobate anual în bugetul public național și din alte surse identificate, în măsura în care costurile estimate nu vor fi acoperite din bugetul public național. Estimarea generală a costurilor pentru implementarea prezentului Program este efectuată în baza priorităților strategice și a acțiunilor identificate și formulate în Planul de acțiuni.

În Tabelul 1 sunt prezentate total *costuri* estimative pentru implementarea Programului.

Tabelul 1. Total costuri estimative pentru implementarea obiectivelor specifice

Nr. crt.	Obiective specifice	Costuri estimativ 2025-2026, lei	Costuri estimativ 2027, lei
1	Simplificarea și digitalizarea serviciilor și procedurilor fiscale	1 567 640	391 910
2	Automatizarea proceselor de colectare a veniturilor	391 910	1 567 640
3	Instituirea unui cadru funcțional de guvernanta a datelor	10 581 570	5 290 785
4	Dezvoltarea competențelor instituționale în analiza riscurilor fiscale	979 775	2 939 325
5	Modernizarea integrală a Centrului de Date	15 284 490 (serve) 5 545 526	58 786 500
6	Asigurarea securității cibernetice avansate	9 503 817	5 584 717
7	Asigurarea interoperabilității și integrării cu sistemele informaționale europene	> 58 786 500	> 39 191 000
Total		102 641 228	113 751 877

Extinderea și modernizarea centrului de date (Data Centru)

Pentru a face față cerințelor moderne, centrul de date al SFS trebuie extins și modernizat. Echipamentele existente sunt învechite, iar volumul de date gestionat crește constant. Prin urmare, se propune achiziția de servere noi și soluții moderne de stocare, precum și implementarea de tehnologii de redundanță și backup (Tabelul 2).

Tabelul 2. Specificații tehnice recomandate pentru centrul de date

Nr.	Echipament	Specificații	Cantitate	Cost aproximativ, lei
1	Servere rackmount	Procesor 40 nuclee, 768 GB RAM, SSD 2 TB	10	7 838 200
2	Storage SAN/NAS	100 TB SSD, conectivitate Fiber Channel 16 Gbps	2	3 919 100
3	Switchuri de rețea	48 porturi 10 Gbps	4	1 567 640
4	UPS (alimentare de rezervă)	Putere 60 kVA	2	979 775
5	Sisteme de climatizare	Sisteme HVAC pentru centre de date	2	587 865
6	Software de gestionare	Software de monitorizare și management IT	-	391 910

Total	15 284 490
--------------	-------------------

Optimizarea infrastructurii serverelor și soluțiilor eficiente de virtualizare

Virtualizarea infrastructurii sistemului informațional va permite SFS să utilizeze mai eficient resursele disponibile și să reducă costurile operaționale. Soluțiile de virtualizare, cum ar fi VMware sau Hyper-V, vor asigura scalabilitatea și flexibilitatea infrastructurii, permițând gestionarea mai eficientă a cerințelor variabile ale utilizatorilor și aplicațiilor fiscale (Tabelul 3).

Tabelul 3. Specificații tehnice recomandate pentru virtualizare

Nr.	Echipament	Specificații	Cantitate	Cost aproximativ, lei
1	Servere de virtualizare	4 x CPU 32 nuclee, 1.5 TB RAM, 25 Gbps Ethernet	15	29 393 250
2	Licențe VMware/Hyper-V	Licențe pentru 400 mașini virtuale	-	3 919 100
3	Storage virtualizat	500 TB stocare dedicată pentru mașini virtuale	2	9 797 750
4	Software de management	Monitorizare și management resurse virtuale	-	979 775
Total				44 089 875

Implementarea sistemului de management al securității informaționale (SIEM)

Implementarea unui sistem integrat de management al securității informaționale (SIEM) este necesară pentru consolidarea securității cibernetice la nivel național, asigurând o monitorizare pro activă și detectarea rapidă a amenințărilor. SIEM va oferi capacități avansate de colectare, analiză și corelare a datelor din diverse surse pentru a preveni, detecta și răspunde incidentelor de securitate într-un mod eficient și coordonat.

În contextul amenințărilor cibernetice tot mai sofisticate și a volumului din ce în ce mai mare de date critice gestionate la nivel național, implementarea unui SIEM devine foarte importantă pentru a monitoriza în timp real infrastructurile sistemului informațional esențiale. Acest sistem va permite detectarea și gestionarea incidentelor de securitate înainte ca acestea să provoace daune majore, asigurând astfel continuitatea operațiunilor și protecția datelor sensibile.

Funcționalități de bază ale SIEM:

1. **Colectarea centralizată a datelor** – SIEM va agrega în mod automat evenimentele și jurnalele de la diverse componente IT (servere, rețele, aplicații) și sisteme de securitate (firewall, IDS/IPS, DLP), facilitând monitorizarea centralizată și integrată a întregii infrastructuri.
2. **Analiza în timp real** – SIEM va analiza evenimentele în timp real, detectând comportamente anormale și generând alerte pentru incidentele de securitate. Această capacitate va permite o reacție rapidă la posibilele amenințări, reducând timpul de răspuns și impactul asupra sistemelor.
3. **Corelarea datelor** – Sistemul va corela date din surse multiple pentru a identifica tipare de atac complexe, care nu ar fi evidente prin monitorizarea individuală a componentelor. Astfel, va îmbunătăți capacitatea de a detecta atacuri avansate, cum ar fi atacurile cu persistență avansată (APT).

4. **Rapoarte și auditare** – SIEM va genera rapoarte detaliate pentru a satisface cerințele de conformitate cu standardele naționale și internaționale de securitate (ex. GDPR, ISO 27001). Aceste rapoarte vor oferi o imagine clară asupra stării securității infrastructurii și a incidentelor gestionate.
5. **Automatizarea răspunsului la incidente** – SIEM va permite automatizarea unor acțiuni de răspuns la incidente, precum izolarea rețelelor compromise, blocarea adreselor IP suspecte și declanșarea măsurilor de protecție suplimentare. Automatizarea va accelera procesele de răspuns și va minimiza erorile umane.

Implementarea soluției SIEM se propune a fi realizată în următoarele 4 etape:

1. **Evaluarea infrastructurii existente.** Se va face o analiză detaliată a infrastructurii IT curente pentru a identifica sursele de date relevante pentru SIEM și compatibilitatea acestora cu soluțiile disponibile.
2. **Selectarea soluției SIEM.** Va fi organizat un proces de achiziție pentru selectarea soluției SIEM care să îndeplinească cerințele naționale și să se integreze cu infrastructura existentă. Acesta va include o analiză comparativă a opțiunilor disponibile și a costurilor aferente.
3. **Implementare pilot.** Implementarea soluției într-un mediu de testare pentru validarea funcționalităților și integrarea sistemelor IT existente.
4. **Implementarea completă și extinderea.** După validarea soluției pilot, implementarea va fi extinsă la nivel național în toate instituțiile relevante.

Costurile estimative și resursele umane necesare a fi implicate întru realizarea soluției SIEM sunt reflectate în Tabelul 4.

Tabelul 4. Plan de implementare SIEM

Nr.	Indicator	Termeni de realizare	Resurse umane	Resurse financiare, lei
1	Evaluarea infrastructurii existente	3-6 luni	-	
2	Selectarea soluției SIEM	6-9 luni	-	
3	Implementare pilot	9-12 luni	3-4 specialiști în securitate IT	
4	Implementarea completă și extinderea	12-18 luni	Coordonator de proiect, specialiști IT	
5	Licențe software SIEM	-	-	9 797 750
6	Infrastructură hardware	-	-	5 878 650
7	Costuri de implementare și mentenanță	-	Echipa de suport și mentenanță	3 919 100
Total				19 595 500

Prevenirea scurgerilor de informații (DLP)

Implementarea unei soluții de prevenire a scurgerilor de informații (Data Loss Prevention - DLP) are ca scop protejarea datelor sensibile împotriva accesului neautorizat, scurgerilor accidentale sau intenționate și asigurarea conformității cu reglementările naționale și internaționale privind

protecția datelor. Soluția DLP va monitoriza și controla fluxul de date în cadrul infrastructurii sistemului informațional, prevenind expunerea neautorizată a informațiilor confidențiale.

Într-o lume din ce în ce mai conectată, protejarea datelor sensibile reprezintă o prioritate. Implementarea unui sistem DLP este esențială pentru prevenirea pierderii de informații critice, fie prin canale de comunicare neautorizate, fie prin erori umane. DLP va contribui la asigurarea conformității cu legislația națională și europeană privind protecția datelor, cum ar fi GDPR, și va ajuta la prevenirea riscurilor asociate scurgerilor de informații.

Funcționalități de bază ale DLP:

1. **Monitorizarea fluxurilor de date** – Soluția DLP va monitoriza toate fluxurile de date interne și externe, detectând transferurile neautorizate sau nesecurizate de informații sensibile.
2. **Politici de control al accesului** – DLP va permite definirea și implementarea unor politici stricte de control al accesului la date sensibile, prevenind accesul neautorizat la acestea de către utilizatori sau sisteme.
3. **Detecția și prevenirea transferurilor de date nesecurizate** – Sistemul va detecta și bloca tentativele de transfer al datelor sensibile prin canale nesigure, cum ar fi e-mailurile necriptate sau transferurile prin dispozitive de stocare externă.
4. **Audit și raportare** – Soluția DLP va genera rapoarte detaliate privind incidentele de securitate și tentativele de scurgere de date, permițând efectuarea de audituri periodice și luarea măsurilor necesare pentru a îmbunătăți protecția datelor.
5. **Integrare cu alte soluții de securitate** – DLP va fi integrat cu soluțiile existente de securitate, cum ar fi SIEM și firewall-uri, pentru a oferi o protecție completă și a asigura o monitorizare continuă a rețelei și a sistemelor.

Implementarea soluției DLP se propune a fi realizată în următoarele 4 etape:

1. **Evaluarea datelor și a riscurilor.** Identificarea tipurilor de date sensibile și a canalelor de transmitere a informațiilor care necesită protecție.
2. **Selectarea soluției DLP.** Alegerea soluției care să răspundă cerințelor specifice de securitate și conformitate, pe baza evaluării efectuate.
3. **Pilotarea soluției.** Testarea soluției într-un mediu controlat pentru a valida capacitățile de detecție, prevenire și raportare.
4. **Implementarea completă.** Integrarea soluției DLP în infrastructura sistemului informațional național și asigurarea conformității cu reglementările privind protecția datelor.

Costurile estimative și resursele umane necesare a fi implicate întru realizarea soluției SIEM sunt reflectate în Tabelul 5.

Tabelul 5. Plan de implementare DLP

Nr.	Indicator	Termeni de realizare	Resurse umane	Resurse financiare, lei
1	Evaluarea datelor și a riscurilor	3-6 luni	-	-
2	Selectarea soluției DLP	6-9 luni	-	-
3	Pilotarea soluției	9-12 luni	2-3 specialiști în securitate IT	-
4	Implementarea completă și extinderea	12-18 luni	Coordonator de proiect, specialiști IT	-

5	Licențe software DLP	-	-	5 878 650
6	Infrastructură hardware	-	-	2 939 325
7	Costuri de implementare și mentenanță	-	Echipa de suport și mentenanță	1 959 550
Total				10 777 525

Fortificarea protecției împotriva atacurilor cibernetice (firewall, IDS/IPS)

Fortificarea protecției împotriva atacurilor cibernetice prin implementarea și modernizarea soluțiilor de tip firewall și sisteme de detecție și prevenire a intruziunilor (IDS/IPS) este necesară pentru a proteja infrastructura sistemului informațional național de atacuri externe și interne. Soluțiile moderne de firewall și IDS/IPS vor asigura o monitorizare continuă a traficului de rețea, identificând și blocând activitățile rău intenționate înainte ca acestea să producă daune semnificative.

Atacurile cibernetice sunt din ce în ce mai sofisticate, iar protejarea infrastructurii critice necesită soluții avansate de securitate. Implementarea unor soluții de firewall moderne, împreună cu sisteme IDS/IPS, va crește capacitatea de detectare și prevenire a atacurilor cibernetice, asigurând o protecție sporită împotriva amenințărilor. Aceste sisteme vor permite monitorizarea traficului de rețea și detectarea activităților anormale, precum tentativele de acces neautorizat sau exploatarea vulnerabilităților.

Funcționalități de bază ale soluțiilor firewall și IDS/IPS

1. **Monitorizarea traficului de rețea** – Soluțiile de firewall și IDS/IPS vor monitoriza constant traficul de rețea, identificând anomalii și încercări de atac, cum ar fi scanările de porturi sau tentativele de atac prin exploatarea vulnerabilităților.
2. **Controlul accesului la rețea** – Firewall-ul va controla accesul la rețea, permițând doar traficul legitim și blocând conexiunile suspecte sau neautorizate.
3. **Detecția și prevenirea intruziunilor** – IDS/IPS va analiza traficul și va identifica tipare de atacuri cunoscute (atacuri DDoS, exploatarea vulnerabilităților etc.), blocând automat încercările de intruziune și alertând echipa de securitate.
4. **Politici de securitate personalizabile** – Soluțiile vor permite definirea unor politici stricte de securitate, adaptate la specificul infrastructurii sistemului informațional național, pentru a preveni accesul neautorizat și a minimiza riscurile.
5. **Integrarea cu alte soluții de securitate** – Firewall-ul și IDS/IPS vor fi integrate cu alte soluții de securitate (SIEM, DLP) pentru a asigura o protecție unitară și eficientă a infrastructurii sistemului informațional, oferind o monitorizare continuă și un răspuns rapid la incidente.

Fortificarea protecției împotriva atacurilor cibernetice se propune a fi realizată în următoarele 4 etape:

1. **Evaluarea infrastructurii de rețea și a vulnerabilităților.** Identificarea punctelor vulnerabile și a zonelor critice de rețea care necesită protecție suplimentară.
2. **Selectarea soluțiilor firewall și IDS/IPS.** Alegerea soluțiilor care să răspundă cerințelor specifice infrastructurii sistemului informațional și să asigure protecția necesară împotriva atacurilor cibernetice.
3. **Pilotarea soluțiilor în medii controlate.** Testarea soluțiilor firewall și IDS/IPS într-un mediu controlat pentru a valida eficiența acestora în detectarea și prevenirea atacurilor.

4. **Implementarea completă și integrarea soluțiilor.** Extinderea implementării la nivel național și integrarea soluțiilor cu sistemele existente de securitate al sistemului informațional pentru a asigura o protecție unitară.

Costurile estimative și resursele umane necesare a fi implicate întru fortificarea protecției împotriva atacurilor cibernetice în Tabelul 6.

Tabelul 6. Plan de fortificare a protecției împotriva atacurilor cibernetice

Nr.	Indicator	Termeni de realizare	Resurse umane	Resurse financiare, lei
1	Evaluarea infrastructurii și a vulnerabilităților	3-6 luni	-	-
2	Selectarea soluțiilor firewall și IDS/IPS	6-9 luni	-	-
3	Pilotarea soluțiilor	9-12 luni	3-4 specialiști în securitate IT	-
4	Implementarea completă și integrarea	12-18 luni	Coordonator de proiect, specialiști în rețea	-
5	Achiziționarea soluțiilor firewall și IDS/IPS	-	-	7 838 200
6	Infrastructură hardware	-	-	3 919 100
7	Costuri de implementare și mentenanță	-	Echipa de suport și mentenanță	2 939 325
Total				14 696 625

Securizarea comunicațiilor și a schimburilor de date

Securizarea comunicațiilor și a schimburilor de date este esențială pentru protejarea integrității și confidențialității informațiilor transmise prin rețele interne și externe. Implementarea unor soluții de criptare end-to-end și utilizarea de rețele private virtuale (VPN) vor garanta că datele sunt protejate împotriva accesului neautorizat pe durata transmisiei și vor asigura conformitatea cu reglementările internaționale de protecție a datelor.

Într-un context digital din ce în ce mai complex, unde schimbul de date între organizații și utilizatori este constant, asigurarea unei comunicații sigure este de o importanță crucială. Criptarea comunicațiilor și utilizarea soluțiilor VPN vor proteja datele sensibile împotriva interceptărilor, asigurând astfel că informațiile rămân confidențiale pe tot parcursul transmisiei. Aceasta este esențială atât pentru asigurarea integrității datelor, cât și pentru respectarea reglementărilor legale.

Funcționalități esențiale ale soluțiilor de securizare a comunicațiilor:

1. **Criptarea end-to-end** – Soluțiile de criptare vor proteja datele transmise între punctele finale ale rețelei, asigurând că doar destinatarul autorizat poate accesa informațiile transmise.
2. **Utilizarea VPN-urilor securizate** – Rețelele private virtuale (VPN) vor fi utilizate pentru a asigura o conexiune criptată și securizată între dispozitivele utilizatorilor și infrastructura centrală, prevenind interceptarea datelor.
3. **Autentificare multifactorială (MFA)** – Pentru a spori securitatea accesului la rețelele de comunicații, va fi implementată autentificarea multifactorială, care va solicita utilizatorilor să furnizeze mai multe forme de verificare a identității înainte de a accesa sistemele.

4. **Monitorizarea și controlul schimburilor de date** – Soluțiile de monitorizare vor supraveghea schimburile de date și vor bloca orice încercare de transmitere neautorizată sau nesigură a informațiilor sensibile.
5. **Integrarea cu alte soluții de securitate** – Sistemele de criptare și VPN vor fi integrate cu soluțiile existente (firewall, IDS/IPS, SIEM) pentru a oferi o protecție unitară și eficientă a schimburilor de date.

Securizarea comunicațiilor și a schimburilor de date se propune a fi realizată în următoarele 4 etape:

1. **Evaluarea cerințelor de securitate a comunicațiilor.** Identificarea tipurilor de comunicații și schimburi de date care necesită protecție și evaluarea soluțiilor disponibile pentru criptare și VPN.
2. **Selectarea soluțiilor de criptare și VPN.** Alegerea soluțiilor care să răspundă nevoilor specifice de securitate și să asigure protecția necesară a comunicațiilor.
3. **Pilotarea soluțiilor în medii controlate.** Testarea soluțiilor de criptare și VPN într-un mediu controlat pentru a valida eficiența acestora în protejarea comunicațiilor și datelor.
4. **Implementarea completă și extinderea soluțiilor.** Implementarea soluțiilor la nivel național și integrarea acestora în infrastructura sistemului informațional existentă.

Costurile estimative și resursele umane necesare a fi implicate întru securizarea comunicațiilor și a schimburilor de date în Tabelul 7.

Tabelul 7. Plan de securizare a comunicațiilor și schimburilor de date

Nr.	Indicator	Termeni de realizare	Resurse umane	Resurse financiare, lei
1	Evaluarea cerințelor de securitate a comunicațiilor	3-6 luni	-	-
2	Selectarea soluțiilor de criptare și VPN	6-9 luni	-	-
3	Pilotarea soluțiilor	9-12 luni	3-4 specialiști în securitate IT	-
4	Implementarea completă și extinderea soluțiilor	12-18 luni	Coordonator de proiect, specialiști IT	-
5	Licențe software pentru criptare și VPN	-	-	4 898 875
6	Infrastructură hardware	-	-	2 939 325
7	Costuri de implementare și mentenanță	-	Echipa de suport și mentenanță	1 959 550
Total				9 797 750

Integrarea cu sistemele informaționale și platformele Europene

Integrarea cu sistemele informaționale și platformele europene reprezintă un pas esențial în consolidarea interoperabilității și eficienței serviciilor oferite la nivel național și continental. Aceasta facilitează schimbul de date și informații între diferite instituții și organizații, contribuind la îmbunătățirea cooperării transfrontaliere și la creșterea transparenței în gestionarea proceselor administrative. Prin adoptarea standardelor și tehnologiilor comune, se asigură alinierea la practicile

europene, ceea ce permite accesul la resurse și instrumente avansate, precum și participarea activă la inițiativele de dezvoltare digitală în cadrul Uniunii Europene.

Conectarea la sistemele informaționale și platformele UE se efectuează într-o efectuare a schimburilor de date, inclusiv în baza directivelor DAC1 – DAC9, prin intermediul canalelor de schimb dedicate și prin intermediul unor aplicații puse la dispoziție în modul stabilit de către UE.

Conectarea la platformele europene de schimb de informații (VIES, CESOP, OSS, etc.)

Într-o conectare la sistemele informaționale ale UE se propune următorul plan de acțiune de implementare general (Tabelul 8):

Tabelul 8. Plan de implementare general

Nr.	Activitate	Timp de Implementare	Data de Începere	Costuri Aproximative, lei
1	Evaluare Internă	2 săptămâni	01.01.2025	19 595
2	Planificare și Alocare Resurse	3 săptămâni	15.01.2025	39 191
3	Integrare VIES	4 săptămâni	05.02.2025	58 786
4	Automatizare Rambursare TVA	6 săptămâni	01.03.2025	78 382
5	Înregistrare în OSS	2 săptămâni	15.04.2025	29 393
6	Adaptare Sisteme OSS	8 săptămâni	01.05.2025	137 168
7	Implementare CESOP	12 luni	01.07.2025	97 977
8	Accesarea Finanțarilor IMM	3 luni	01.07.2025	58 786
9	Pregătire pentru ViDA	6 luni	01.10.2025	19 595
10	Stabilire Proceduri EOIR	1 lună	01.01.2026	48 988
11	Formare Personal	4 săptămâni	01.02.2026	58 786
12	Monitorizare și Îmbunătățire Continuă	Continuă	01.04.2026	97 977 per an
Total				1 802 786

Implementarea standardelor și reglementărilor DAC

Implementarea schimburilor de date cu țările membre ale Uniunii Europene, în conformitate cu directivele DAC1 până la DAC9, are o importanță majoră pentru Republica Moldova în contextul integrării europene și al cooperării fiscale internaționale. Aceste directive, cunoscute sub denumirea de Directive privind Cooperarea Administrativă (DAC), stabilesc cadrul legal pentru schimbul automat de informații între autoritățile fiscale ale statelor membre, având ca obiectiv principal combaterea evaziunii fiscale și a planificării fiscale agresive.

Implementarea acestor directive aduce multiple beneficii Republicii Moldova, contribuind la:

1. **Combaterea Evaziunii Fiscale și a Fraudei.** Schimbul automat de informații financiare și fiscale permite autorităților să identifice și să investigheze mai eficient cazurile de evaziune fiscală, asigurând astfel colectarea corectă a impozitelor și protejarea veniturilor bugetare.
2. **Promovarea Transparenței și Conformității Fiscale.** Adoptarea directivelor DAC încurajează transparența în raportarea fiscală și stimulează contribuabilii să respecte obligațiile fiscale, reducând riscul practicilor fiscale neloiale.
3. **Armonizarea Legislativă și Integrarea Europeană.** Adaptarea legislației naționale la standardele și cerințele UE facilitează procesul de integrare europeană și consolidează relațiile cu statele membre, recunoscând Republica Moldova ca un partener de încredere.
4. **Îmbunătățirea Cooperării Internaționale.** Schimbul de informații întărește colaborarea între autoritățile fiscale la nivel internațional, permițând un răspuns coordonat la provocările globale în domeniul fiscalității și prevenirea practicilor dăunătoare.
5. **Protejarea Integrității SISFS.** Monitorizarea tranzacțiilor transfrontaliere și a activităților multinaționale previne erodarea bazei impozabile și transferul profiturilor către jurisdicții cu impozitare redusă sau nulă.
6. **Adaptarea la Evoluțiile Tehnologice și Economice.** Directivele mai recente, precum DAC7 și DAC8, abordează noile modele de afaceri digitale și cripto-activelor, asigurând că sistemul fiscal țină pasul cu inovațiile tehnologice și economice.

Implementarea directivelor DAC în cadrul Programului de dezvoltare al sistemului informațional este importantă pentru asigurarea compatibilității tehnice și operaționale cu sistemele informatice ale UE. Aceasta implică:

1. Dezvoltarea Infrastructurii sistemului informațional: Adaptarea sistemelor informatice pentru a putea efectua schimburi automate de informații în conformitate cu standardele tehnice ale UE, asigurând securitatea și integritatea datelor transmise.
2. Formarea Resurselor Umane: Instruirea personalului din administrația fiscală pentru a gestiona noile proceduri și tehnologii asociate schimbului automat de informații, consolidând capacitatea instituțională.
3. Armonizarea Legislativă: Actualizarea cadrului legal național pentru a reflecta prevederile directivelor DAC, asigurând baza juridică necesară pentru colectarea și schimbul de informații fiscale.
4. Securitatea Cibernetică: Implementarea măsurilor de securitate cibernetică pentru a proteja informațiile sensibile și a preveni accesul neautorizat sau breșele de securitate.
5. Impactul Strategic asupra Republicii Moldova
6. Prin alinierea la directivele DAC și implementarea schimburilor de date cu țările membre ale UE, Republica Moldova își consolidează poziția în comunitatea europeană și internațională, demonstrând angajamentul față de transparență și cooperare. Această integrare contribuie la:
7. Eficientizarea Administrării Fiscale: Accesul la informații detaliate despre tranzacțiile transfrontaliere îmbunătățește capacitatea autorităților fiscale de a detecta și corecta neconformitățile.
8. Creșterea Încrederii Investitorilor: Un sistem fiscal transparent și aliniat la standardele internaționale creează un mediu favorabil pentru investiții și dezvoltare economică.
9. Protejarea Economiei Naționale: Combaterea eficientă a evaziunii fiscale și a fluxurilor financiare ilicite contribuie la stabilitatea financiară și la protecția resurselor economice ale țării.

10. Consolidarea Relațiilor Internaționale: Participarea activă în schimburile de informații fiscale întărește relațiile cu partenerii internaționali și facilitează cooperarea în alte domenii de interes comun.

Integrarea directivelor DAC în Programul de dezvoltare al sistemului informațional nu reprezintă doar o conformare la cerințele UE, ci și un pas important către modernizarea și eficientizarea administrației fiscale a Republicii Moldova. Prin adoptarea acestor măsuri, țara își îmbunătățește infrastructura tehnologică, își dezvoltă capitalul uman și își consolidează poziția pe plan internațional, contribuind la creșterea bunăstării cetățenilor și la dezvoltarea durabilă.

Costurile estimative și resursele umane necesare a fi implicate întru implementarea directivelor DAC1-9 sunt reflectate în Tabelul 9.

Tabelul 9. Plan de implementare a directivelor DAC1-9

Nr.	Directivă	Implementare Tehnologică	Resurse Umane	Costuri Estimative, lei
1	DAC1	Dezvoltarea unui sistem informatic securizat pentru schimbul de informații fiscale la cerere.	Programatori specializați, experți în protecția datelor, personal fiscal instruit.	1 959 550 – 3 919 100
2	DAC2	Dezvoltarea unui sistem informatic pentru colectarea și transmiterea automată a informațiilor financiare conform CRS.	Specialiști în integrarea sistemelor IT, experți în securitate cibernetică, personal pentru gestionarea relațiilor cu instituțiile financiare.	9 797 750 – 19 595 500
3	DAC3	Adaptarea sistemelor existente pentru raportarea automată a deciziilor fiscale anticipate și a acordurilor de preț în avans.	Dezvoltatori software, experți fiscali, personal pentru gestionarea și validarea datelor.	2 939 325 – 5 878 650
4	DAC4	Dezvoltarea unui sistem pentru colectarea, stocarea și transmiterea rapoartelor financiare detaliate ale grupurilor multinaționale (CbCR).	Specialiști în baze de date, analiști financiari, experți în securitatea informației.	6 838 200 – 7 156 764 400
5	DAC5	Integrarea sistemelor fiscale cu registrele beneficiarilor reali și dezvoltarea unei interfețe pentru schimbul de informații.	Specialiști IT, experți juridici, personal pentru actualizarea bazelor de date.	3 919 100 - 7 838 200
6	DAC6	Crearea unei platforme digitale pentru raportarea aranjamentelor fiscale transfrontaliere de către intermediarii fiscali.	Dezvoltatori de aplicații web securizate, experți în criptarea datelor, personal pentru analizarea rapoartelor.	5 878 650 – 11 757 300
7	DAC7	Dezvoltarea unui sistem pentru colectarea și transmiterea informațiilor de la operatorii platformelor digitale.	Specialiști în integrarea API-urilor, experți în economia digitală, personal pentru gestionarea datelor colectate.	11 757 300 - 23 514 600
8	DAC8	Dezvoltarea soluțiilor tehnologice pentru monitorizarea și raportarea tranzacțiilor cu crypto-active.	Experți în blockchain, specialiști în securitate cibernetică, analiști în crypto-active.	15 676 400 – 29 393 250

9	DAC9	Actualizarea și optimizarea sistemelor existente pentru eficientizarea schimbului de informații fiscale.	Specialiști IT pentru actualizări, experți în politici fiscale, personal pentru formare.	4 898 875 - 9 797 750
Total				827 370 750

6. Riscuri de implementare

În Tabelul 10 sunt sistematizate *riscurile* în implementarea Programului.

Tabelul 10. Riscuri de implementare a Programului

Riscul anticipat	Impact (Scăzut, Mediu, Înalt)	Probabilitatea (Joasă, Medie, Înaltă)	Măsuri de diminuare/ înlăturare a riscurilor
Securitatea cibernetică deficitară. Infrastructura sistemului informațional poate fi expusă atacurilor cibernetice, ceea ce ar putea duce la scurgeri de date sensibile și compromiterea sistemului informatic. Lipsa unor soluții avansate de protecție (IDS/IPS, criptare end-to-end) crește vulnerabilitatea sistemului.	Mediu	Medie	1. Implementarea unui sistem avansat de securitate cibernetică (IDS/IPS, firewall, criptare). 2. Monitorizarea permanentă a amenințărilor și răspuns rapid la incidente de securitate. 3. Formarea periodică a personalului pentru gestionarea riscurilor cibernetice.
Fragmentarea sistemelor din cadrul sistemului informațional și lipsa interoperabilității. Dificultăți în integrarea sistemelor existente cu platformele europene (VIES, OSS, CESOP). Acces dificil și întârziat la informațiile fiscale între Republica Moldova și Uniunea Europeană	Mediu	Joasă	1. Dezvoltarea unui cadru de interoperabilitate pentru schimbul de date cu UE. 2. Implementarea unui sistem de integrare a bazelor de date și a standardelor comune de schimb de informații
Dependența de procese manuale și lipsa automatizării. Lipsa unui sistem complet automatizat încetinește operațiunile și crește riscul de erori umane. Procesarea manuală afectează eficiența colectării datelor și capacitatea de analiză a acestora.	Mediu	Joasă	1. Digitalizarea completă a proceselor de administrare fiscală. 2. Integrarea inteligenței artificiale și a instrumentelor de business intelligence pentru analiza automată a riscurilor.
Lipsa unui cadru formal de guvernanță a datelor. Date incomplete, redundante sau inaccesibile pot afecta calitatea deciziilor strategice. Lipsa unui management eficient al datelor poate reduce încrederea în sistem.	Mediu	Medie	1. Crearea unei subdiviziuni de business intelligence pentru analiza și managementul datelor. 2. Implementarea unui cadru formal de guvernanță a datelor conform standardelor UE.
Riscuri legate de resursele umane. Deficitul de specialiști IT cu experiență în administrarea și securitatea sistemelor avansate. Necesitatea instruirii continue a personalului pentru a menține conformitatea cu cerințele europene.	Mediu	Înaltă	1. Crearea unor programe de formare profesională în domeniul sistemului informațional și securității cibernetice.

			2. Colaborarea cu universități și instituții de cercetare pentru dezvoltarea competențelor digitale.
Riscuri financiare și de implementare. Costurile ridicate ale implementării și întreținerii infrastructurii sistemului informațional pot depăși bugetul disponibil. Întârzieri în implementare din cauza complexității proiectului și necesității de aliniere la standardele UE.	Înalt	Medie	1. Accesarea fondurilor europene și internaționale pentru finanțarea proiectului. 2. Planificarea detaliată a etapelor de implementare și monitorizarea progresului în timp real.

7. Autorități/instituții responsabile

Autoritatea responsabilă pentru coordonarea implementării prezentului Program este Ministerul Finanțelor.

Totodată, reieșind din actele legislative și normative în vigoare, în procesul de implementare a programului Serviciul Fiscal de Stat va colabora cu Ministerul Finanțelor, Ministerul Dezvoltării Economice și Digitalizării, IP Serviciul Tehnologia Informației și Securitate Cibernetică, Agenția de Guvernare Electronică, IP Centrul de Tehnologii Informaționale în Finanțe.

8. Proceduri de monitorizare, evaluare și raportare

Monitorizarea implementării și evaluarea Programului se va efectua de către Ministerul Finanțelor, în colaborare cu alte autorități/instituții implicate în procesul de implementare a acțiunilor incluse în Planul de acțiuni pentru implementarea Programului. Activitatea de monitorizare va include elaborarea de către SFS a *Rapoartelor anuale de progres*.

Monitorizarea se va realiza în baza indicatorilor și a rezultatelor obținute în cazul fiecărei acțiuni, stabilite în Program. Procesul de monitorizare va fi efectuat semestrial prin colectarea, prelucrarea și analiza datelor, identificarea erorilor sau a efectelor neprevăzute. Conform recomandărilor și concluziilor incluse în rapoartele de monitorizare se va analiza posibilitatea revizuirii intervențiilor planificate.

După finalizarea implementării Programului, SFS va elabora Raportul final de evaluare, conform criteriilor de evaluare prevăzute în pct.57 din Regulamentul cu privire la planificarea, elaborarea, aprobarea, implementarea, monitorizarea și evaluarea documentelor de politici publice, aprobat prin HG 386/2020, și anume:

- 1) relevanța Programului;
- 2) gradul de realizare a obiectivelor (efectivitatea);
- 3) modul de utilizare a mijloacelor bugetare alocate (eficiența);
- 4) capacitatea de a produce efecte de durată (durabilitatea);
- 5) impactul Programului.

9. Planul de acțiuni privind realizarea obiectivelor programului pentru anii 2025-2027

Acțiuni	Indicatori de monitorizare	Termen de realizare	Costuri de implementare, lei			Autorități responsabile
			2025	2026	2027	
1	2	3	4	5	6	7
Obiectiv general 1: Asigurarea eficientizării administrării fiscale prin creșterea calității serviciilor fiscale prestate, digitalizarea proceselor fiscale și creșterea gradului de satisfacție al contribuabililor						
Obiectiv specific 1.1: Simplificarea și digitalizarea serviciilor și procedurilor fiscale						
Creșterea numărului de servicii digitalizate	Cel puțin 95% servicii digitalizate (18/19) 100% servicii digitalizate (19/19)	Trimestrul IV, 2026 Trimestrul IV, 2027	-	În limita alocațiilor bugetare stabilite în TIC – 1 567 640	În limita alocațiilor bugetare stabilite în TIC – 391 910	SFS IP CTIF
Realizarea sondajelor de opinie a contribuabililor pentru îmbunătățirea continuă a serviciilor și platformelor IT	Cel puțin 1 sondaj de opinie efectuat	Anual, Trimestrul IV	În limita resurselor umane și financiare disponibile	În limita resurselor umane și financiare disponibile	În limita resurselor umane și financiare disponibile	SFS
Implementarea funcționalităților rapide și prietenoase pentru utilizator, prin utilizarea declarațiilor precompletate	Sarcină tehnică aprobată 1 declarație nouă precompletată implementată	Trimestrul III, 2026 Trimestrul IV, 2027	-	În limita alocațiilor bugetare stabilite în TIC	În limita alocațiilor bugetare stabilite în TIC	SFS
Creșterea diversității datelor prin realizarea noilor schimburi de date prin intermediul platformei guvernamentale MConnect	3 Anexe tehnice aprobate și implementate 5 Anexe tehnice aprobate și implementate 7 Anexe tehnice aprobate și implementate	Trimestrul IV, 2025 Trimestrul IV, 2026 Trimestrul IV, 2027	În limita resurselor umane și financiare disponibile	În limita resurselor umane și financiare disponibile	În limita resurselor umane și financiare disponibile	SFS IP CTIF AGE
Obiectiv specific 1.2: Automatizarea proceselor de colectare a veniturilor						
Dezvoltarea și implementarea unui sistem informațional automatizat care să permită procesarea instantanee a dărilor de seamă fiscale și a plăților, eliminând necesitatea unei intervenții manuale și reducând riscul de erori	Caiet/sarcină tehnică aprobată 1 sistem informațional dezvoltat	Trimestrul III, 2026 Trimestrul IV, 2027	-	În limita alocațiilor bugetare stabilite în TIC – 391 910	În limita alocațiilor bugetare stabilite în TIC – 1 567 640	SFS IP CTIF

Reducerea timpului de procesare a dărilor de seamă fiscale pentru actualizarea instantanee a informațiilor	Timp de procesare a dărilor de seamă redus cu 90%	Trimestrul IV, 2027	-	-	În limita resurselor umane și financiare disponibile	SFS IP CTIF
Reducerea timpului de procesare a plăților către bugetul public național cu reflectarea instantanee în conturile contribuabililor	Timp de procesare a plăților redus cu 90%	Trimestrul IV, 2027	-	-	În limita resurselor umane și financiare disponibile	SFS IP CTIF
Dezvoltarea/identificarea unui sistem informațional de management al riscurilor de neconformare fiscală	Sistem lansat în exploatare industrială	Trimestrul IV, 2026	-	În limita alocațiilor bugetare stabilite în TIC – 3 919 100	-	SFS IP CTIF
Reducerea timpului de procesare a datelor, pentru stabilirea scorurilor de risc de neconformare fiscală.	Reducerea de până la 40 ore de procesare a datelor Reducerea de până la 24 ore de procesare a datelor	Trimestrul IV, 2026 Trimestrul IV, 2027	-	În limita alocațiilor bugetare	În limita alocațiilor bugetare	SFS
Automatizarea procesului de notificare pentru contribuabili cu risc de neconformare	5 tipuri de notificări automatizate > 20 tipuri de notificări automatizate	Trimestrul III, 2026 Trimestrul IV, 2027	-	În limita resurselor umane și financiare disponibile	În limita resurselor umane și financiare disponibile	SFS IP CTIF
Majorarea ponderii cazurilor de neconformare confirmate în urma controalelor	Cel puțin 75% cazuri de neconformare confirmate Cel puțin 98% cazuri de neconformare confirmate	Trimestrul IV, 2026 Trimestrul IV, 2027	-	În limita resurselor umane și financiare disponibile	În limita resurselor umane și financiare disponibile	SFS IP CTIF
Obiectiv specific 1.3: Instituirea unui cadru funcțional de guvernanță a datelor						
Elaborarea și aprobarea politicii de guvernanță a datelor și de calitate a acestora	Ordin SFS aprobat	Trimestrul IV, 2025 Trimestrul III, 2026 Trimestrul III, 2027	În limita resurselor umane și financiare disponibile	În limita resurselor umane și financiare disponibile	În limita resurselor umane și financiare disponibile	SFS

Crearea unei subdiviziuni de business intelligence (BI)	Ordin MF aprobat cu noua structura SFS 1 subdiviziune nou creată, componenta 3 angajați	Trimestrul IV, 2026 Trimestrul IV, 2027	-	În limita resurselor umane și financiare disponibile	În limita resurselor umane și financiare disponibile	MF SFS
Elaborarea și aprobarea glosarului și a dicționarului de date	Ordin SFS aprobat	Trimestrul IV, 2025	În limita resurselor umane și financiare disponibile	-	-	SFS
Dezvoltarea arhitecturii inițiale DataLake	1 arhitectură identificată 1 arhitectură dezvoltată	Trimestrul III, 2026	-	În limita alocațiilor bugetare stabilite în TIC – 1 058 157	-	SFS IP CTIF
Conectarea surselor de date la DataLake	Surse de date conectate la nivel de 50% Surse de date conectate la nivel de 100%	Trimestrul IV, 2026 Trimestrul IV, 2027	-	În limita resurselor umane și financiare disponibile	În limita alocațiilor bugetare stabilite în TIC – 529 078	SFS IP CTIF
Obiectiv specific 1.4: Dezvoltarea competențelor instituționale în analiza riscurilor fiscale						
Identificarea și încheierea de parteneriate cu universitățile capabile să ofere capacități de cunoștințe matematice, statistice pentru elaborarea abordărilor bazate pe riscuri (identificarea riscului contribuabililor, identificarea riscului de audit, identificarea și gestionarea fraudei pe baza datelor colectate)	Cel puțin o instituție de învățământ superior identificată Cel puțin 1 acord semnat cu o instituție de învățământ superior	Trimestrul II, 2026 Trimestrul I, 2027	-	În limita resurselor umane și financiare disponibile	În limita resurselor umane și financiare disponibile	SFS
Realizarea instruirii pentru angajații din cadrul subdiviziunii BI pentru dezvoltarea competențelor în domeniul aplicării BI	Cel puțin 2 instruirii desfășurate	Trimestrul II, 2027	-	-	În limita resurselor umane și financiare disponibile	SFS
Identificarea și numirea unui ofițer de date	Ordin SFS aprobat	Trimestrul IV, 2025	-	În limita resurselor umane și financiare disponibile	-	SFS

Obiectiv specific 1.5: Modernizarea integrală a Centrului de Date						
Dezvoltarea competențelor profesionale ale angajaților din cadrul Direcției dezvoltare informațională pentru implementarea serviciilor IT	Cel puțin 2 instruirii desfășurate anual	Trimestrul IV, 2025 Trimestrul III, 2026 Trimestrul III, 2027	În limita resurselor umane și financiare disponibile	În limita resurselor umane și financiare disponibile	În limita resurselor umane și financiare disponibile	SFS
Instituirea unui mecanism de control ce va monitoriza implementarea cerințelor TIC	1 mecanism identificat 1 mecanism implementat	Trimestrul IV, 2026 Trimestrul II, 2027		În limita resurselor umane și financiare disponibile	În limita resurselor umane și financiare disponibile	SFS IP CTIF
Modernizarea centrului de date al SFS	Centru de date modernizat în proporție de 80% Centru de date modernizat în proporție de 100%	Trimestrul IV, 2026 Trimestrul IV, 2027	-	În limita alocațiilor bugetare stabilite în TIC – 5 545 526	În limita alocațiilor bugetare stabilite în TIC – 58 786 500	SFS IP CTIF
Asigurarea cu servere virtualizate	servere virtualizate în proporție de 90% servere virtualizate în proporție de 100%	Trimestrul IV, 2026 Trimestrul IV, 2027	-	În limita alocațiilor bugetare stabilite în TIC – 15 284 490	În limita alocațiilor bugetare stabilite în TIC	SFS IP CTIF
Asigurarea monitorizată prin SIEM a infrastructurii SFS	Infrastructură monitorizată prin SIEM în proporție de 50% Infrastructură monitorizată prin SIEM în proporție de 70%	Trimestrul IV, 2026 Trimestrul IV, 2027	-	În limita alocațiilor bugetare stabilite în TIC > 58 786 500	În limita alocațiilor bugetare stabilite în TIC > 39 191 000	SFS IP CTIF
Obiectiv specific 1.6: Asigurarea securității cibernetice avansate						
Desemnarea unui Ofițer principal de securitate a informațiilor în cadrul SFS	Ordin SFS aprobat	Trimestrul I, 2026	-	În limita resurselor umane și financiare disponibile	-	SFS
Definirea politicii de securitate cibernetică a SFS	Ordin SFS aprobat	Trimestrul I, 2026	-	În limita resurselor umane și financiare disponibile	-	SFS

Implementarea măsurilor de monitorizare a securității, control al accesului, gestionare a conturilor privilegiate, monitorizare a vulnerabilităților, jurnale de audit, securitate a logicii de afaceri (piste de auditare), etc. (Implementare recomandată bazată pe Controalele CIS versiunea 8, 3 grupuri de implementare a măsurilor de protecție)	Ordin SFS aprobat Cel puțin 2 instruiți desfășurate anual	Trimestrul IV, 2025 Trimestrul II, 2026 Trimestrul II, 2027	În limita alocațiilor bugetare stabilite în TIC – 3 174 471	În limita alocațiilor bugetare stabilite în TIC – 3 174 471	În limita alocațiilor bugetare stabilite în TIC – 4 408 987	SFS
Desfășurarea misiunilor de audit sau a verificărilor aferent securității IT, protecția datelor și accesul la informații din SISFS	Cel puțin 1 misiune de audit realizată, anual	Anual, Trimestrul II	În limita resurselor umane și financiare disponibile	În limita resurselor umane și financiare disponibile	În limita resurselor umane și financiare disponibile	SFS
Asigurarea monitorizării stațiilor de muncă prin DLP	Cel puțin 500 stații monitorizate din 1600 Cel puțin 1200 stații monitorizate din 1600	Trimestrul IV, 2026 Trimestrul IV, 2027	-	În limita resurselor umane și financiare disponibile	În limita resurselor umane și financiare disponibile	SFS IP CTIF
Asigurarea criptării comunicațiilor	Cel puțin 30% comunicații criptate Cel puțin 40% comunicații criptate	Trimestrul IV, 2026 Trimestrul IV, 2027	-	În limita resurselor umane și financiare disponibile	În limita resurselor umane și financiare disponibile	SFS IP CTIF
Asigurarea desfășurării instruirii angajaților în domeniul securității cibernetice	Cel puțin o instruire desfășurată	Anual, Trimestrul III	În limita resurselor umane și financiare disponibile	În limita resurselor umane și financiare disponibile	În limita resurselor umane și financiare disponibile	SFS IP CTIF
Obiectiv specific 1.7: Asigurarea interoperabilității și integrării cu sistemele informaționale europene						
Identificarea cerințelor funcționale și tehnice ale platformelor europene pentru implementarea DAC 1 – DAC 9	Cerințe pentru 2 sisteme identificate, anual	Anual, Trimestrul IV	În limita resurselor umane și financiare disponibile	În limita resurselor umane și financiare disponibile	În limita resurselor umane și financiare disponibile	SFS IP CTIF
Dezvoltarea și testarea conectorilor de interfațare	Act de testare a lucrărilor realizate Act de acceptare a lucrărilor	Trimestrul IV, 2025 Trimestrul IV, 2026	În limita resurselor umane și	În limita resurselor umane și	În limita resurselor umane și	SFS IP CTIF

		Trimestrul IV, 2027	financiare disponibile	financiare disponibile	financiare disponibile	
Participarea la sesiuni de instruire în domeniul interoperabilității și integrării cu sistemele informaționale europene și cooperare UE	cel puțin 1 misiune TAIEX cel puțin 2 sesiuni FISCALIS	Trimestrul III, 2025 Trimestrul II, 2026 Trimestrul IV, 2027	În limita resurselor umane și financiare disponibile	În limita resurselor umane și financiare disponibile	În limita resurselor umane și financiare disponibile	SFS