

GUID 5259

Sisteme Informatice privind datoria publică



INTOSAI

Ghidurile INTOSAI sunt publicate de către Organizația Internațională a Instituțiilor Supreme de Audit, INTOSAI, ca parte a Cadrului INTOSAI de Declarații Profesionale. Pentru mai multe informații, accesați www.issai.org

Document pre-IFPP – acest document a fost elaborat înainte de crearea Cadrului INTOSAI de Declarații Profesionale (IFPP) în 2016. Din acest motiv, scopul său oficial ar putea diferi de cel al unor Ghiduri de Audit INTOSAI mai recente.



INTOSAI



INTOSAI, 2019

1) Avizat sub denumirea “ISSAI 5450 – Ghid de Auditare a Sistemelor Informatice de administrare a Datoriei Publice” în 2016

2) Odată cu stabilirea Cadrelui INTOSAI de Declarații Profesionale (IFPP), documentul a fost redenumit „GUID 5259 - Sisteme Informatice de administrare a Datoriei Publice”, cu schimbări editoriale, în 2019



CUPRINS

PREFAȚĂ	5
LISTA ABREVIERILOR	7
INTRODUCERE	8
1. PLANIFICARE	9
2. CONTROALE GENERALE	13
Controale organizaționale	13
Controale privind Accesul Fizic	14
Controale privind Accesul Logic	14
Controale de Mediu	14
Controale pentru Schimbări aduse Programelor	14
Planificarea Continuității Activității și Plan de Redresare în urma Dezastrelor	15
3. CONTROALE DIN APLICAȚII	15
3.1. STANDARDE PRIVIND DOCUMENTAȚIA	16
3.2. CONTROALE PRIVIND INTRĂRILE	17
Ecrane pentru Introducerea Datelor	18
Rutine de Pregătire a Datelor	19
Autorizarea Introducerii Datelor	19
Retenția Documentelor privind Introducerea Datelor	19
Validarea Introducerii Datelor	19
Erori la Introducerea Datelor	21
Mecanisme de Suport pentru Introducerea Datelor	21
3.3. CONTROALE PRIVIND PRELUCRAREA	22
Caracterul complet	22
3.4. CONTROALE PRIVIND IEȘIRILE	23

3.5. TESTAREA CONTROALELOR DIN APLICAȚII	25
3.6. RAPORTAREA REZULTATELOR AUDITULUI	26
ANEXA I: TABEL DE PLANIFICARE	27
ANEXA II: MATRICEA DE TESTARE PENTRU CONTROALE GENERALE	32
ANEXA III: MATRICEA DE TESTARE PENTRU CONTROALE DIN APLICAȚII	38
FIGURA 1: AUDITURI ALE DATORIEI PUBLICE EFECTUATE DE SAI-URI: CAZUL BRAZILIEI	56
FIGURA 2: AUDITURI ALE DATORIEI PUBLICE EFECTUATE DE SAI-URI: CAZUL MOLDOVEI	61
BIBLIOGRAFIE	63

PREFAȚĂ

- 1) Datoria publică se află în centrul oricărei discuții care vizează administrarea finanțelor publice. În efortul lor de a-și dezvolta economiile și a optimiza serviciile sociale în propria țară, cele mai multe guverne înregistrează necesități financiare semnificative. În teorie, datoria publică reprezintă un instrument eficace de creștere economică și de distribuție echitabilă a poverii fiscale între generația de contribuabili actuală și cea viitoare. Însă, dată fiind importanța sa pentru echilibrul economic, estimarea și gestionarea cu deosebită atenție a datoriei publice devin esențiale.
- 2) Principalul obiectiv în administrarea datoriei publice constă în asigurarea necesarului de finanțare al administrației publice pe fondul minimizării costurilor asociate datoriei publice și limitarea riscurilor specifice asociate portofoliului de datorie publică. . Liniile directoare cu privire la modul de administrare a datoriei publice revizuite de Banca Mondială și Fondul Monetar Internațional (FMI) oferă un set de bune practici privind controlul intern în administrare datoriei publice. Printre considerentele cu privire la sistemul de control intern acestea identificăm „activitățile privind administrarea datoriei publice trebuie să fie susținute de un sistem informatic cuprinzător care să asigure gestionarea cu acuratețe a datelor aferente managementului datoriei publice și care să asigure securitatea corespunzătoare a datelor”. Statele preocupate de asigurarea administrării eficiente a datoriei publice trebuie să prioritizeze dezvoltarea unor sisteme fiabile pentru înregistrarea și raportarea informațiilor referitoare la datoria publică. Această măsură este necesară nu doar pentru a crea o bază de date a datoriei publice ci pentru a asigura plata la timp a serviciului datoriei publice și pentru a îmbunătăți calitatea raportărilor privind bugetul și a asigura transparența financiară în domeniul finanțelor publice, permițând

astfel factorilor de decizie și administratorilor datoriei publice să atingă obiectivele aferente datoriei publice.

- 3) Auditul sistemelor informatice de gestionare a datoriei publice urmărește să asigure eficiența, randamentul și eficacitatea administrării datoriei publice. De aceea, orice audit de acest tip va fi considerat un audit al performanței.

Totodată, această activitate poate fi extrem de relevantă și în contextul auditurilor financiare, care urmăresc să stabilească dacă informațiile financiare transmise de administrația publică sunt în conformitate cu cadrul de reglementare aplicabil modului de prezentare a raportărilor financiare și dacă acele informații sunt credibile și nu conțin acte de fraudă sau erori. În acest context, activitatea în cauză devine deosebit de importantă, putând facilita realizarea unui sistem informatic care colectează și furnizează informații exacte și fiabile despre unul dintre cele mai importante elemente ale finanțelor guvernamentale, respectiv datoria publică.

- 4) Prezentul GUID oferă auditorilor îndrumări descriptive privind auditarea sistemelor informatice de gestionare a datoriei publice. Întrucât Organizația Internațională a Instituțiilor Supreme de Audit (INTOSAI) dispune deja de o serie de documente privind auditurile sistemelor IT (IT), elaborate de către Grupul de Lucru pentru Auditul IT (WGITA), acest GUID se axează pe controalele aplicațiilor, controale care trebuie să fie specifice sistemului informatic de gestionare a datoriei publice.

LISTA ABREVIERILOR

BCP – planificarea continuității activității

CAAT – tehnici de audit asistate de calculator

CS-DRMS – Sistemul de Înregistrare și Administrare a Datoriilor al Secretariatului Commonwealth

DMFAS – Sistemul de Administrare a Datoriei și Analiză Financiară

DMO – oficiul de administrare a datoriei

DRP – planul de redresare în urma dezastrelor

FMIS – Sistem Informatic de Management Financiar

FMI – Fondul Monetar Internațional

INTOSAI – Organizația Internațională a Instituțiilor Supreme de Audit

IT – tehnologia informației

PDMIS – sistem informatic de gestionare a datoriei publice

SAI – instituție supremă de audit

SID – Sistemul Guvernului Federal Brazilian de Administrare a Datoriei

UNCTAD – Conferința Organizației Națiunilor Unite pentru Comerț și Dezvoltare

WGITA – Grupul de Lucru pentru Auditul IT

WGPD – Grupul de Lucru pentru Datoria Publică

Introducere

Potrivit termenilor de referință stabiliți de Consiliul de Conducere al of INTOSAI, Grupul de Lucru pentru Datoria Publică (WGPD) a primit sarcina de a publica ghiduri și alte materiale informative destinate utilizării de către instituțiile supreme de audit (SAI) pentru a încuraja gestionarea și raportarea corectă a datoriei publice.

Prezentul GUID urmărește să consolideze capacitatea WGPD, oferind un cadru general ce poate fi aplicat în cadrul SAI-urilor pentru a evalua controale generale și ale aplicațiilor sistemelor informatice de gestionare a datoriei publice (PDMIS). Este important de reținut faptul că, în referințe, PDMIS este interpretat drept unul sau mai multe sisteme informatice utilizate în administrarea datoriei publice.

În paralel cu progresul IT, organizațiile guvernamentale au manifestat o dependență tot mai mare de utilizare IT în desfășurarea propriilor operațiuni economice și în furnizarea serviciilor, dar și pentru a prelucra, întreține și raporta informații esențiale. După cum afirmă un Document de Lucru al FMI, „un FMIS (Sistem Informatic de Management Financiar) se referă, de regulă, la computerizarea procesului de gestionare a cheltuielilor publice, incluzând formularea bugetului, execuția și contabilitatea bugetară, cu ajutorul unui sistem complet integrat de gestiune financiară al ministerelor de resort și al altor agenții responsabile cu cheltuielile”.

Standardul 1471 al Institutului de Inginerie Electrica si Electronica definește sistemele drept „o colecție de componente organizate pentru a îndeplini o anumită funcție sau un anumit set de funcții”. În mod deosebit, principala activitate a unui sistem dintr-un oficiu de gestionare a datoriilor este de a întreține baza de date a creditelor acordate în sectorul public utilizând componente software adecvate atât înregistrării, cât și îndeplinirii funcțiilor analitice ale oficiului de administrare a datoriei (DMO).

Auditul IT poate fi clasificat, cu referire la abordările predominante, după cum urmează:

- » guvernanță IT,
- » auditul datelor,
- » auditarea sistemelor informatice,
- » contractare servicii IT, și
- » securitatea informației.

În general, un auditor IT aplică o serie de metode în loc de una singură; totuși, auditorul poate alege o abordare predominantă. În prezentul ghid, abordarea predominantă este auditarea sistemelor informatice.

Acest GUID este structurat pe trei secțiuni: planificare, evaluarea controalelor generale și evaluarea controalelor aplicațiilor.

1. PLANIFICARE

Un PDMIS poate fi considerat un set de componente interdependente (structuri fizice, personal și instrumente tehnologice) care interacționează cu scopul de a înregistra, controla, evalua și gestiona tranzacții generate prin contractarea, administrarea și rambursarea datoriei publice.

În această etapă auditorul dobândește o înțelegere a operațiunilor și controalelor aferente sistemului IT și riscurile specifice în raport cu riscurile inerente ale fluxului de operațiuni aferente datoriei publice. Pe baza acestei înțelegeri, auditorul evaluează mediul general de control, identifică sistemele utilizate în administrarea datoriei publice, examinează întreaga documentație referitoare la aceste sisteme și formulează o evaluare preliminară a riscului. Rezultatul evaluării va orienta în ce măsură vor fi extinse procedurile utilizate în faza de testare.

De asemenea, SAI va examina toate structurile din cadrul oficiului de administrare a datoriei publice, precum personalul, procesul propriu-zis, tipul datoriilor, securitatea datelor, instrumentele tehnologiei informaționale și nu numai.

În această fază, auditorul va realiza o evaluare preliminară a structurii organizatorice a oficiului de administrare a datoriei publice și a fluxurilor de operațiuni aferente datoriei publice, care va viza următoarele:

- » Cum este organizat PDMIS: ce sisteme există pentru înregistrarea, prelucrarea, raportarea, controlul și gestionarea datoriei publice și ce procese și funcții principale sunt realizate/îndeplinite de către fiecare sistem.
- » Funcționarea auditului intern.
- » Rezultatele auditurilor anterioare (interne sau externe) la nivelul PDMIS.
- » Stocarea fizică a documentelor referitoare la operațiuni.
- » Utilizarea componentelor informatice hardware și software și responsabilitatea întreținerii acestora.
- » Operațiunile prelucrate de sistemele informatice și importanța lor relativă.
- » Relația dintre informațiile aferente componentelor datoriei publice.
- » Metode și proceduri de implementare a noilor operațiuni sau revizuirea operațiunilor existente.
- » Evaluarea anterioară a controalelor interne ale DMO. Dacă respectivele controale interne ale DMO nu au fost evaluate anterior, SAI va realiza această evaluare. Această procedură este foarte importantă în evaluarea nivelului riscurilor existente, deci și pentru a stabili volumul de teste ale controalelor.

Gradul de complexitate al sistemului nu afectează evaluarea controalelor generale, care ar trebui să fie întotdeauna efectuate. Totuși, acesta determină procedurile de audit ce urmează a fi utilizate și indică numărul de specialiști IT necesar pentru a realiza activitatea de audit. O sugestie este ca cel puțin un specialist IT din echipă să desfășoare întreaga activitate pe marginea sistemelor. În ce privește auditorii din echipă fără experiență în auditul IT, aceștia trebuie să dobândească cunoștințe despre terminologia specifică. De aceea, un dicționar tehnic IT de calitate reprezintă o reală necesitate pentru o SAI. Auditarea Sistemelor Informatice – Glosar de

Termeni, publicat de WGITA, este util în acest sens. Pot fi utile și unele glosare web; vezi <http://www.webopedia.com> sau <http://whatis.techtarget.com>.

Auditorii care sunt deja familiarizați cu terminologia IT trebuie să cunoască și terminologia folosită în DMO, în special acronime și abrevieri (tipuri de titluri, sectoare ale DMO, creditori, denumiri de sisteme, software utilizat de DMO, etc.). Este esențială dobândirea unor cunoștințe specifice înainte de a realiza interviurile. Un glosar util elaborat de Conferința Organizației Națiunilor Unite pentru Comerț și Dezvoltare (UNCTAD) este disponibil la următoarele linkuri:

- » <http://unctad.org/en/Docs/pogiddmfasm3r3.en.pdf> – Glosar în materie de datorii și DMFAS (versiune în limba engleză)
- » <https://unctad.org/es/docs/pogiddmfasm3r3.sp.pdf> – Glosario de la deuda y del SIGADE (versiune în limba spaniolă)

Pentru a înțelege un PDMIS în detaliu, se impune cunoașterea fluxurilor inerente de date și informații. Astfel, sunt foarte importante în etapa de planificare identificarea operațiunilor cheie privind administrarea datoriei publice (înregistrare, prelucrare, control, securitatea datelor, raportare și analiză) și înțelegerea modului în care aceste operațiuni sunt realizate prin intermediul sistemului informatic. Ulterior, se impune realizarea unei evaluări a riscului pentru a identifica riscurile semnificative asociate proceselor operaționale și de gestionare a datoriei publice, ținând cont de impactul lor și probabilitatea de a se produce. Evaluarea riscului este decisivă în stabilirea ariei de aplicabilitate a procedurilor necesare gestionării nivelelor de risc aferente. Fostul *ISSAI 5410, Ghid de Planificare și Efectuare a Auditului Controalelor Interne privind Gestionarea Datoriei Publice*¹ poate fi consultat când se realizează evaluarea riscului. De asemenea, evaluarea riscului se realizează și în contextul efectuării unor audituri financiare.

Fluxurile unui PDMIS sunt aproape întotdeauna dimensionate în DMO. Și alte oficii pot fi primi sarcini de introducere a datelor privind datoria publică, de exemplu, în cazul contractării datoriei publice. Dacă DMO este organizat în trei departamente respectiv Front Office, Middle Office și Back Office fiecare având atribuțiile sale specifice. Între atribuțiile specifice Departamentului Front Office/Contractare care asigură contractarea și gestionarea datoriei publice se regăsesc de regulă realizarea tranzacțiilor pe piețele financiare, lansarea și derularea emisiunilor de titluri de

¹ Această declarație a fost retrasă din cadru în septembrie 2019

stat, administrarea/gestionarea tuturor operațiunilor financiare. Departamentul Back Office/Operațiuni asigură derularea tranzacțiilor și organizarea evidenței înregistrărilor operațiunilor financiare. Atribuțiile Departamentului Middle Office sunt între altele analiza și managementul riscului, monitorizarea și raportarea riscurilor asociate portofoliului de datorie publică, evaluarea performanței managementului cu privire la îndeplinirea obiectivelor și țăntelor strategice specifice. Cele mai multe fluxuri de informații privind datoria publică, inclusiv informații externe, se derulează în departamentul de operațiuni, responsabil cu înregistrarea și controlul datelor.

Întrucât multe țări folosesc un sistem disponibil în domeniul public, dezvoltat și actualizat de către terțe organizații internaționale (de ex., Sistemul de Administrare și Analiză Financiară a Datoriei (DMFAS) ori Sistemul de Înregistrare și Administrare a Datoriilor al Secretariatului Commonwealth (CS-DRMS)), în administrarea datoriei publice, utilizarea rapoartelor referitoare la performanță - de exemplu, solicitări de mentenanță a sistemului și evidențe ale incidentelor - este deosebit de importantă.

Programul DMFAS, dezvoltat de UNCTAD, se axează pe activități „din aval”. Sunt incluse aici mentenanța bazelor de date asociate datoriei publice, validarea datelor aferente datoriei publice, operațiuni asociate datoriei publice, raportări interne și externe cu privire la datoria publică, raportări statistice și analize privind datoria publică, precum și crearea legăturilor de sistem între programele informatice de administrare a datoriei și cele financiare. Aceste activități completează activități specifice „din amonte”, precum analiza sustenabilității datoriei efectuată de alte organisme, cum ar fi de exemplu Banca Mondială. În plus, DMFAS ajută tot mai mult țările să stabilească legături între programul informatic pentru administrarea datoriei publice și alte programe informatice guvernamentale (cum ar fi spre exemplu cele utilizate pentru întocmirea bugetului, gestionarea fluxurilor de trezorerie și gestionarea subvențiilor) sau între alte sisteme complexe și integrate de management financiar, în contextul eforturilor țărilor în gestionarea finanțelor publice. Pentru mai multe informații, vezi <http://unctad.org/dmfas>.

Aplicarea CS-DRMS, furnizat de Secretariatul Commonwealth, ajută SAI-urile în înregistrarea, gestionarea și analiza propriilor datorii dintr-o perspectivă globală. Sistemul oferă un fișier centralizat cu privire la datoria publică după tipul datoriei și rezidența creditorului, respectiv cu privire la datoria publică și privată internă și externă garantată, în această categorie fiind inclusă și datoria pe termen scurt. De asemenea, sistemul gestionează finanțările nerambursabilei, împrumuturile garantate de stat. Pentru mai multe informații, vezi <https://thecommonwealth.org/about-cs-drms>.

În cazul țărilor care utilizează DMFAS sau CS-DRMS în administrarea datoriei publice, rapoartele de audit al PDMIS întocmite de către alte țări (alte SAI-uri) ar putea fi utile în identificarea celor mai frecvente deficiențe și care au un impact semnificativ.

Un tabel ce conține informațiile și procedurile necesare și întrebările la care SAI va răspunde și pe care echipa de audit îl poate utiliza în faza de planificare a activității de auditare a sistemelor de gestionare a datoriei publice este disponibil în anexa I.

2. CONTROALE GENERALE

Controalele generale asigură cadrul controalelor generale pentru funcțiile IT. Acele controale sunt concepute pentru abordarea aspectelor referitoare la îmbunătățirea activităților de întreținere a echipamentelor și mentenanță IT. Obiectivele controalelor generale sunt: securitatea datelor, protecția aplicațiilor programelor informatice și asigurarea continuității operațiunilor computerizate în cazul apariției unor întreruperi neprevăzute.

Cu toate că un audit al sistemului IT de administrare a datoriei publice necesită verificarea controalelor generale IT, prezentul document nu tratează acele controale în detaliu, întrucât INTOSAI a emis documente privind auditul IT, care detaliază controalele generale IT.

Este recomandat ca în efectuarea unui audit asupra sistemului IT, echipa de audit să examineze conținutul fostului *ISSAI 5310*², *Ghid privind Auditurile Securității Sistemelor Informatice (ISec)*, cu îndrumări de verificare a securității sistemelor informatice din organizații guvernamentale.

Un alt document care ar putea fi util în planificarea controalelor generale este Manualul IDI (Inițiativa de Dezvoltare a INTOSAI) al WGITA privind Auditul IT, destinat Instituțiilor Supreme de Audi, ce oferă informații esențiale și întrebări cheie necesare în planificarea eficientă a auditurilor IT.

În anexa II există o matrice de testare cu o serie de controale generale și proceduri sugerate de testare, care pot ajuta auditorul în testarea controalelor generale.

² Începând din septembrie 2019, această declarație se află în curs de revizie, putând fi retrasă sau înlocuită în viitor.

Un set cuprinzător cu diversele categorii de controale generale include elementele descrise mai jos.

» **Controale organizaționale**

Controalele Organizaționale sunt politicile, procedurile și cadrul organizațional stabilite pentru a asigura politici privind resursele umane și practici de management sănătoase, separarea corectă atribuțiilor și politici solide de securitate a informațiilor, precum și a metode menite să evalueze eficacitatea și să asigure eficiența și controalele operaționale.

» **Controale privind Accesul Fizic**

Controalele privind accesul fizic cuprind reguli și practici de prevenire a accesului neautorizat la și a interferenței cu serviciile IT, incluzând proceduri administrative, precum ecusoane obligatorii de identificare pentru personal și controlul vizitatorilor, dar și măsuri fizice precum încuietoare fizice cu cheie și încuietoare electronice pentru uși, camere video și alte mijloace de limitare a accesului fizic la servere și alte secțiuni critice de infrastructură.

» **Controale privind Accesul Logic**

Controalele privind accesul logic utilizează măsurile integrate de securitate ale unui sistem informatic pentru a preveni accesul neautorizat la fișiere și date sensibile și a asigura faptul că toți utilizatorii au drepturi de acces limitate la cerințele aferente fișei postului. Aceste controale include firewall-uri, programe antivirus și de detecție a intruziunilor și a aplicațiilor de tip malware.

În sistemele moderne, aceste controale sunt obținute pe multe și variate căi. Ele sunt implementate prin intermediul programelor de aplicații, sistemului de operare, sistemului de gestiune a bazelor de date, componentelor software pentru controlul accesului, sistemelor de monitorizare a prelucrărilor de tranzacții online, serverelor, rețelei, rețelei locale și al altor posibile aplicații informatice.

» Controale de Mediu

Controale de Mediu sunt reguli, practici și condiții integrate menite să prevină daunele cauzate de instabilități electrice, incendii, praf, apă, alimente, temperaturi extreme, umiditate sau electricitate statică.

Chiar dacă obiectivul central al acestor controale este centrul de date (sau zona destinată echipamentelor IT, care necesită un mediu ambiant specific sau cel puțin protecție antifurt), acestea se aplică și în cazul oricărui mediu ambiant de birou.

» Controale pentru Schimbări aduse Programelor

Controalele pentru schimbări aduse programelor includ reguli prin care se asigură faptul că toate schimbările aduse configurației sistemului se realizează cu acuratețe, integral și în timp util.

Modernizările și schimbările vor dispune de un proces oficial menit să asigure înregistrarea tuturor schimbărilor și capacitatea de a reveni la o versiune anterioară în cazul unor eventuale probleme cu noua versiune.

Aprobarea oficială va fi obligatorie înainte de trecerea programelor de la versiuni de test la biblioteci de producție, în timp ce toate sistemele, operațiunile și documentațiile programelor vor fi permanent integrale, actualizate și în conformitate cu standarde, politici și proceduri.

» Planificarea continuității activității și Planul de redresare în urma dezastrelor

Planificarea continuității activității (BCP) și Planul aferent de redresare în urma dezastrelor (DRP) sunt concepute pentru a facilita îndeplinirea obiectivului de disponibilitate. Planurile de intervenție și planul de redresare în urma dezastrelor, viabilitatea, testarea și monitorizarea planurilor și necesitatea de actualizare permanentă a planurilor sunt factori decisivi.

BCP este o abordare globală a efortului de a asigura direcții alternative de sprijin pentru procese esențiale de afaceri în situații de urgență, dacă se produc dezastre sau alte întreruperi. Se pune accent pe supraviețuirea integrală a entității, nu doar pe funcția IT.

Totuși, planul general trebuie să ia în considerare sistemele informatice și cerințele rețelelor de telecomunicații. Această porțiune din BCP include și DRP.

BCP și DRP aferent pot fi dezvoltate concomitent cu scopul de a fi toate aspectele luate simultan în calcul. Un plan va include cel puțin proceduri și criterii de catalogare a unei situații drept dezastru, persoana însărcinată cu acea catalogare și metoda de catalogare oficială a unui eveniment drept dezastru și de demarare a implementării planului.

3. CONTROALE DIN APLICAȚII

Controalele din aplicații sunt automatizate în aplicațiile sistemului informatic pentru a facilita asigurarea autorizării, integrității, acurateței și validității tranzacțiilor. Aceste controale sunt integrate în programarea unei aplicații și vizibile în operațiunile de intrare, prelucrare și ieșire ale aplicației. Obiectivul lor este de a garanta caracterul complet, credibilitatea și acuratețea prelucrării datelor.

Exemple de controale din aplicații includ verificări realizate de aplicație în ce privește formatul datelor introduse pentru a preveni introducerea unor date invalide, controale ale prelucrării ce nu permit utilizatorilor să posteze tranzacții neautorizate, precum și rapoarte și controale detaliate privind volumul total de tranzacții, prin care se asigură înregistrarea completă și exactă a tuturor tranzacțiilor.

Controalele din aplicații pot fi clasificate după cum urmează:

- » de intrare,
- » de prelucrare, și
- » de ieșire.

3.1. STANDARDE PRIVIND DOCUMENTAȚIA

Standardele privind documentația asigură păstrarea documentațiilor adecvate și actualizate ale aplicațiilor. Importantă este și actualizarea atentă a documentației.

Documentația corespunzătoare este importantă pentru a determina ce controale sunt sau ar trebui să fie implementate.

De asemenea, buna documentație a aplicațiilor reduce pentru utilizatori riscul de a nu respecta procedurile de control prevăzute de către conducere. O examinare a documentației cuprinzătoare și actualizate ajută auditorul să înțeleagă modul în care funcționează fiecare aplicație și, eventual, să identifice anumite riscuri de audit.

- » Documentația aplicațiilor: ajută programatorii specializați în mentenanță să înțeleagă aplicația, să elimine probleme și să efectueze optimizări. Documentația se îmbogățește în fiecare fază a procesului de dezvoltare și poate fi creată în diverse formate, precum diagrame de flux, grafice, tabele, sau text. Documentația poate include detalii privind sursele datelor, atribute de date, ecrane de introducere a datelor, validări de date, proceduri de securitate, descrierea calculelor, proiectări de programe, interfețe cu alte aplicații, proceduri de control, metode de gestionare a erorilor, instrucțiuni de operare, proceduri de arhivare, backup stocare și redresare. Documentația aplicației va fi actualizată în paralel cu modificarea aplicației.
- » Documentația pentru utilizatori: include descrieri ale fluxurilor automate și manuale de activitate, utile în instruirea inițială pe marginea unei aplicații, dar și ca referință curentă.

În ambele cazuri, documentația pentru utilizatori va fi actualizată pe măsură ce aplicația suferă modificări.

Documentația va include

- » o prezentare generală a aplicației,
- » specificarea cerințelor utilizatorilor,
- » descrieri și enumerări de programe,
- » descrieri de intrări/ieșiri,
- » descrieri de conținuturi ale fișierelor,
- » manuale de utilizare,
- » instrucțiuni procedurale,

- » descrieri ale controalelor privind securitatea aplicațiilor,
- » un rezumat recent al evaluărilor de securitate,
- » decizii și măsuri recomandate recente în materie de securitate, și
- » situația curentă a măsurilor recomandate.

3.2. CONTROALE PRIVIND INTRĂRILE

Controalele privind intrările sunt extrem de importante în reducerea riscului de eroare sau fraudă în aplicații computerizate. Controalele privind intrările sunt esențiale pentru integritatea datelor.

Controalele privind intrările facilitează asigurarea autorizării, acurateței, caracterului complet și caracterului de actualitate al datelor introduse într-o aplicație. Autorizarea este asigurată prin impunerea unor aprobări secundare pentru tranzacții ce depășesc un prag predefinit. Acuratețea este asigurată prin verificări de versiuni, care validează datele introduse înainte de a accepta o tranzacție în vederea prelucrării.

Caracterul complet se asigură prin proceduri de gestionare a erorilor, care asigură jurnalizarea, raportarea și corectarea erorilor. Caracterul de actualitate este asigurat prin monitorizarea fluxului de tranzacții, jurnalizarea și raportarea excepțiilor.

Controalele privind intrările se pot regăsi

- » pe ecrane de introducere a datelor,
- » în rutine de pregătire a datelor,
- » în procesul de autorizare a introducerii datelor,
- » în cadrul retenției documentelor privind introducerea datelor,
- » în procesul de validare a introducerii datelor,
- » în procedurile privind erorile în introducerea datelor, și

- » în cadrul mecanismelor de suport pentru introducerea datelor.

Controalele subliniate mai sus pot fi eludate dacă este posibilă evitarea lor introducând sau modificând date din afara aplicației. Trebuie să existe verificări automate ale integrității aplicațiilor, concepute pentru a detecta și raporta eventuale modificări cu origine externă a datelor. De exemplu, ar fi necesară o verificare concepută pentru a detecta și raporta modificări neautorizate aduse bazei de date subiacente de tranzacții.

» Ecrane pentru Introducerea Datelor

Ecranele standardizate pentru introducerea datelor pot asigura consecvența introducerii datelor.

PDMIS poate include următoarele funcționalități:

- » ecrane de introducere a datelor structurate după o formă și o dispunere standardizate;
- » câmpuri de introducere a datelor cu restricții privind datele ce pot fi introduse de utilizatori;
- » introducerea obligatorie a datelor în anumite câmpuri; și
- » o funcție de asistență (de ex., F1) ce ajută utilizatorii să completeze câmpurile în care se introduc date.

» Rutine de Pregătire a Datelor

Scopul rutinelor de pregătire a datelor este de evita disfuncționalități în timpul procedurilor de introducere a datelor.

PDMIS poate include medii integrate destinate procedurilor de partajare a datelor, prin care pot fi transferate date către alte aplicații.

» Autorizarea Introducerii Datelor

Autorizarea introducerii datelor urmărește să asigure faptul că toate introducerile de date au fost înregistrate și autorizate de către persoana responsabilă.

PDMIS poate include următoarele funcționalități:

- » parolă obligatorie de acces;
- » evidențe din jurnalul de acces în cazuri de introducere manuală a datelor; și
- » obligativitatea unui număr de două aprobări pentru anumite operațiuni sensibile (de ex., activarea contractelor, modificarea ratelor de dobândă și modificarea valorilor contractuale).

» Retenția Documentelor privind Introducerea Datelor

Această dimensiune a controalelor privind introducerea datelor vizează întreținerea și controlul documentelor originale de suport pentru evidențele de date referitoare la datorii. În cazul transferurilor automate de fișiere între aplicații, PDMIS trebuie să păstreze datele originale primite de la alte aplicații pe o perioadă prestabilită de către DMO.

» Validarea Introducerii Datelor

Controalele privind validarea datelor sunt concepute să asigure validitatea și acuratețea datelor de intrare.

PDMIS poate include următoarele funcționalități:

- » Liste automate de verificare a absenței anumitor valori (de ex., când se descarcă o serie istorică de indexuri, PDMIS verifică dacă lipsește o valoare zilnică, lunară sau anuală).
- » Toate ecranele de introducere a datelor identifică în mod clar câmpurile obligatorii, iar aplicația permite confirmarea operațiunii doar dacă toate informațiile obligatorii au fost introduse.
- » Fiecare tabel de bază de date trebuie să conțină o regulă specifică privind câmpurile în care nu este permisă duplicarea datelor.
- » Dacă aplicația consideră să sunt introduse date duplicate, aceasta nu va accepta intrarea de date decât după eliminarea duplicării.
- » Aplicația nu permite modificarea anumitor date după introducerea acestora (de ex., rata cursului de schimb din data operațiunii). În ce privește alte date, aplicația ar putea permite modificarea lor dacă sunt îndeplinite unele

condiții (de ex., ori de câte ori un contract se află în starea „Blocat” sau „Încheiat”, nu este posibilă modificarea datelor).

- » Anumite câmpuri, în faza de completare, necesită completarea prealabilă a altor câmpuri (de ex., dacă utilizatorul introduce comisionul de angajament contractual, utilizatorul va introduce și taxa de angajament).
- » Câmpurile intitulate „data” sunt esențiale pentru controlul general al unui contract de datorie. Acestea sunt deosebit de utile în calcularea tranșelor, pentru a fi evitate întârzieri la plată, dispunerea unor amenzi și așa mai departe. Astfel, aplicația trebuie să dispună de reguli de bază privind inserarea datei.
- » Cu excepția operațiunilor simulate, aplicația de sistem nu permite înregistrarea datelor la o dată viitoare, de exemplu, pentru vărsământ, revocare de vărsământ, anulare de contract sau completare la contract.

» Erori la Introducerea Datelor

O pistă de audit sau un jurnal de este o evidență (sau un set de evidențe) cronologică relevantă din punct de vedere al securității, sau o destinație și o sursă a evidențelor, care furnizează documente justificative pentru succesiunea activităților care au afectat la un moment dat o anumită operațiune, procedură sau un anumit eveniment. Circulația fișierelor de tip pistă sau jurnal de audit va fi rezervată strict personalului responsabil.

PDMIS poate include următoarele funcționalități:

- » DMO va defini responsabilitatea gestionării fișierelor provizorii;
- » programele concepute pentru jurnaliza erori, raporta erori curente și a înregistra corectări de erori vor fi integrate în aplicație;
- » într-un proces de descărcare automată a datelor, dacă aplicația identifică lipsuri în serie, se va transmite un e-mail automat de follow-up utilizatorilor vizați; și

- » aplicația va transmite rapoarte periodice pe marginea erorilor nesoluționate – inclusiv intervalul de timp în care acestea au rămas nesoluționate și prioritatea acestora – personalului responsabil.

» Mecanisme de Suport pentru Introducerea Datelor

Aceste controale au legătură cu procedurile de suport din DMO care ajută utilizatorii să introducă date în aplicația informatică, să reinițializeze aplicații și să monitorizeze activități ale utilizatorilor pentru a evita posibile deviații de la reguli stabilite.

De multe ori, aceste mecanisme sunt incluse printre controalele generale.

3.3. CONTROALE PRIVIND PRELUCRAREA

Controalele privind prelucrarea asigură acuratețea, caracterul complet și caracterul de actualitate al datelor pe durata prelucrării pe loturi sau online. Aceste controale asigură faptul că datele sunt prelucrate cu exactitate în cadrul aplicației și că nu vor fi adăugate, pierdute sau modificate date pe durata prelucrării.

» Caracterul complet

Caracterul complet se poate asigura în prelucrarea pe loturi realizând un echilibru între tranzacții primite de un sistem și tranzacții transmise de un sistem auxiliar.

Acest echilibru se va realiza între aplicații care partajează date comune, prin întocmirea unui raport de conciliere care enumeră date din ambele aplicații și transmite eventuale diferențe la nivelul unui grup de utilizatori.

Echilibrarea valorilor totale va include o numărătoare a tranzacțiilor și valori totale ale câmpurilor numerice pentru fiecare tip de tranzacție, precum și verificarea încrucișată a valorilor totale de la câmpuri individuale la câmpuri de totalizare.

În fișiere ce nu conțin totaluri relevante, se pot crea totaluri de control care adaugă toate figurile într-o coloană pentru a verifica dacă același total este acceptat de următorul proces. De exemplu, totalizarea valorilor din contracte de datorie nu este

relevantă, însă acest total se poate utiliza pentru a verifica dacă toate valorile corecte din contractele de datorie au fost incluse în prelucrare.

PDMIS poate include următoarele funcționalități:

- » În interfața cu alte sisteme de trecere între aplicații, dacă există o eroare în prelucrarea unui fișier, se va genera un fișier de eroare, care se va înregistra în aplicația de sistem. Utilizatorii vor adopta o abordare de interoperabilitate mai aprofundată pentru domenii și instrucțiuni tehnice în cadrul entității.
- » Aplicația conține loturi de acțiuni pentru numeroase sarcini, de exemplu, actualizare de stocuri, planificare financiară, indexuri și plăți viitoare. Utilizatorii vor evalua rezultate ale sistemelor în timp real pasive, axându-se pe jurnale bazate pe loturi, precum și capacități în timp real active pentru a măsura prelucrarea informațiilor actualizate.
- » Dacă intervine o eroare în prelucrarea acțiunilor pe loturi, aplicația transmite utilizatorului un mesaj cu informații despre eroare. Utilizatorul poate verifica acele capacități de consolidare în cadrul sistemului, în ce privește respectarea politicilor de corectare a erorilor, și poate configura procedurile de control.
- » După finalizarea unei operațiuni, aplicația afișează un mesaj ce confirmă faptul că prelucrarea s-a realizat cu succes și prezintă un rezumat al datelor introduse.
- » După o modificare a unor date înregistrate anterior, aplicația afișează un mesaj conform căruia modificarea s-a realizat cu succes și prezintă un rezumat al datelor modificate.
- » După ștergerea unor date introduse anterior, aplicația afișează un mesaj conform căruia ștergerea s-a realizat cu succes și prezintă un rezumat al datelor șterse.
- » Dacă ștergerea unei evidențe afectează integritatea relațională a bazei de date, aplicația nu permite acea ștergere și afișează un mesaj indicând faptul că evidența nu poate fi ștearsă. De exemplu, datele unei bănci creditoare nu pot fi șterse din tabelul cu creditorii dacă acel creditor figurează cu contracte în plină desfășurare în aplicație.

- » Aplicația realizează anumite verificări între datele departamentului de interfață cu clienții și cele ale departamentului de operațiuni. De exemplu, este nevoie de aportul departamentului de operațiuni pentru a valida date de intrare produse de licitații. Utilizatorii pot verifica în comunicări eventuale interconexiuni la nivel de arhitectură a datelor între componente și sisteme pentru a examina fluxurile de date conform diagramei de interoperabilitate.

3.4. CONTROALE PRIVIND IEȘIRILE

Controalele privind ieșirile asigură integritatea ieșirilor și distribuția corectă și în timp util a rezultatelor produse. Deficiențele de prelucrare pot fi uneori compensate prin controale ferme ale rezultatelor. O aplicație cu controale solide la nivel de intrări și prelucrare va fi, probabil, subminată integral dacă nu dispune de controale pentru ieșiri. Caracterul complet și integritatea rapoartelor de ieșire depind de restricționarea capacității de modificare a ieșirilor și de integrarea verificărilor privind caracterul complet, precum numerotarea paginilor și sume de control.

Fișierele de ieșire vor fi securizate pentru a reduce riscul modificării neautorizate. Posibile motive ale modificării rezultatelor de procese informatice includ mușamalizarea prelucrării neautorizate sau manipularea unor rezultate financiare nedorite.

Datele de ieșire ale unei aplicații IT pot constitui date de intrare pentru o altă aplicație. În astfel de cazuri, auditorul va verifica existența unor controale care garantează transferul cu acuratețe al ieșirilor de la o etapă de prelucrare la alta.

În PDMIS, controalele privind ieșirile pot fi și programate pentru a identifica informații critice care necesită măsuri prioritare din partea structurilor de administrare a datoriei publice. De exemplu, în cazul contractelor care expiră în luna curentă, aplicația poate afișa alerte zilnice, pe primul ecran al sistemului, referitoare la contracte ale căror termen de plată expiră în următoarele 5 zile.

De asemenea, aplicația poate permite anumitor profiluri de utilizatori să genereze rapoarte în modul de prioritate, având astfel capacitatea de a prioritiza rapoartele ce urmează a fi generate.

PDMIS poate include următoarele funcționalități:

- » aplicația oferă o comparație automată între suma datelor inițiale și suma datelor prelucrate;

- » aplicația va informa utilizatorii în legătură cu situația solicitărilor de generare de rapoarte, de exemplu, „neîncepută”, „în desfășurare” și „încheiată”; și
- » la finalul unui proces de generare a unui raport, aplicație transmite utilizatorului care a lansat solicitarea un mesaj prin care îl informează în legătură cu finalizarea sarcinii.

3.5. TESTAREA CONTROALELOR DIN APLICAȚII

Având controalele identificate, următorul pas într-un audit este de a verifica eficacitatea acestora.

Acest lucru se poate realiza prin

- » transmiterea unui set de date de test care, dacă aplicația funcționează corespunzător, va produce rezultate cunoscute;
- » dezvoltarea unor programe independente care vor executa din nou funcțiile logice ale aplicației; și
- » evaluarea rezultatelor aplicației.

Procedurile de mai sus testează integritatea unui program creat în cadrul PDMIS, însă nu și integritatea datelor.

Dacă aplicația dispune de un mediu de test, se poate recurge la acesta pentru a testa controale, cu condiția ca mediul de test să fie o reproducere confirmată a mediului de producție.

Pentru a testa reguli de calcul, precum cele având legătură cu actualizarea stocurilor sau cu serviciul datoriei, auditorul ar putea fi nevoit să utilizeze tehnici de audit asistate de calculator (CAAT), care include numeroase tipuri de instrumente și tehnici, precum software generalizat de audit, programe utilitare, date de test, identificarea și maparea programelor de aplicații și aplicații specializate de audit. Pot fi aici incluse instrumente care analizează acuratețea logicii și calculelor din foi de calcul. Pot fi utilizate instrumente și pentru a analiza aplicații ale bazelor de date și a genera o diagramă logică de flux. Programele generalizate de audit pot fi utile în analiza datelor produse de majoritatea aplicațiilor.

Auditorul va determina necesitatea utilizării unei CAAT. Folosirea acestora va depinde de gradul de sofisticare al aplicației care administrează datoria publică.

Prezentul document include o matrice propusă de testare (vezi anexa III), pe care echipa de audit o poate folosi drept punct de referință în testarea controalelor din aplicații. Această matrice identifică unele cerințe și funcționalități pe care ar trebui să le asigure sistemele de gestionare a datoriei publice, interogări pe care sistemele ar trebui să le poată efectua și cerințele minime privind capacitățile acestor sisteme.

Este important de reținut faptul că, întrucât datoria fiecărei țări prezintă o structură și caracteristici diferite, sistemele de administrare a datoriei prezintă și ele caracteristici diferite. Astfel, echipa de audit are sarcina de a identifica, a ajusta dacă este necesar, și a utiliza elementele aplicabile sistemului de gestionare a datoriei din țara acesteia.

3.6. RAPORTAREA REZULTATELOR AUDITULUI

Pe lângă respectarea conformității cu *INTOSAI-P 1 Declarația de la Lima*, unde este cazul, rapoartele privind auditul PDMIS ar putea lua în considerare conținutul fostului *ISSAI 5440*³, *Ghid privind Efectuarea unui Audit al Datoriei Publice – Utilizarea Testelor de Fond în Audituri Financiare*, secțiunea 2.6 Raportarea Rezultatelor Auditului.

După cum s-a precizat mai sus, auditul unui PDMIS este un audit al performanței, fiind astfel importantă întocmirea unui raport aliniat la standardele de raportare pe marginea auditurilor performanței, după cum indică *ISSAI 3000 Standardul Auditului Performanței* și *ISSAI 300 Principiile Auditului Performanței*.

³ Începând din septembrie 2019, această declarație se află în curs de revizie, putând fi retrasă sau înlocuită în viitor.

ANEXA I: TABEL DE PLANIFICARE

Informații, Documente și Rapoarte Obligatorii

- » Inventar al sistemelor informatice utilizate de DMO și documentația aferentă sistemelor
- » Inventar al sistemelor de operare de pe computere și al rețelei utilizate de către DMO
- » Cartografierea actualizată a fluxurilor de procese din cadrul DMO
- » Rapoarte anterioare de audit pe marginea DMO
- » Rapoarte anterioare de audit pe marginea sistemelor IT de administrare a datoriei publice
- » Legi și regulamente referitoare la cadrul DMO și administrarea datoriei publice
- » Lista directorilor din cadrul DMO plus personalul responsabil cu managementul informatic, managementul continuității activității, managementul resurselor umane, managementul riscului, auditul intern și nu numai, rolurile, adresele de domiciliu și de e-mail și numerele de telefon ale acestor persoane
- » Documente menite să reflecte funcționarea DMO și/sau sistemele sale, sub formă de politici scrise și manuale de procedură ale DMO sau ale ministerului de finanțe, după cum urmează:
 - Managementul personalului
 - Managementul schimbării

- Accesul fizic
 - Cerințe IT specifice mediului ambiental / amplasamentului
 - Accesul logic
 - Planificarea continuității activității (BCP)
 - Planul de redresare în urma dezastrelor (DRP)
 - Planul de Backup
 - Servicii terțe (servicii IT)
 - Rapoarte anterioare de evaluare a riscului
 - Rezumat recent al evaluărilor securității
 - Decizii în materie de securitate și măsuri recomandate recente
 - Situația curentă a măsurilor recomandate
 - Aprobarea implementării sistemului de către conducerea de rang superior
- » Rapoarte diseminate de către entități externalizate responsabile cu asigurarea mentenanței sistemului
 - » Alte documente referitoare la DMO, sistemul acestuia, sau al ambele (de ex., diapozitive, texte, ținte și rapoarte anuale privind administrarea datoriei)
 - » Numărul de angajați ai DMO care sunt utilizatori ai sistemului și profilurile lor de acces
 - » Numărul angajaților departamentului IT și specificațiile posturilor ocupate de aceștia (definirea rolurilor), atât pentru personalul DMO, cât și cel IT
 - » Lista angajaților cu acces la sala serverului
 - » Descrierea profilului de acces al PDMIS
 - » Specificarea oficială a modalității de actualizare a sistemelor de operare, a firewall-urilor și a programelor antivirus, precum și a regularității actualizărilor

- » Roluri ale obstacolelor fizice și instrumentelor automate utilizate în prevenirea accesului neautorizat la unitatea centrală, stații de lucru, servere și alte echipamente DMO
- » Localizarea fiecărei încăperi din interiorul și din exteriorul DMO
- » Listă a personalului, stațiilor de lucru și serverelor
- » Alocarea bugetului pe ultimii 5 ani
- » Lista instructajelor anterioare atât pentru utilizarea PDMIS (personalul DMO), cât și actualizarea cunoștințelor informatice (personalul IT)
- » Reguli precizate, practici și descrieri integrate cu scopul de a preveni daune cauzate de instabilități electrice, incendii, praf, apă, alimente, temperaturi extreme, umiditate sau electricitate statică
- » Specificații privind funcționarea sursei de alimentare neîntreruptibile (dacă există)
- » Jurnale de incidente referitoare la solicitările DMO privind erori ale PDMIS sau rapoarte pe marginea instrucțiunilor de utilizare
- » Rapoarte pe marginea jurnalelor cu incidente de securitate
- » Lista modificărilor din PDMIS din ultimele 12 luni
- » Jurnale cu și rapoarte despre teste și evenimente relevante pe marginea BCP și DRP
- » Documentații ale aplicațiilor și pentru utilizatori
- » Termeni de utilizare pentru fiecare aplicație
- » Manual de proceduri de gestionare de erorilor de prelucrare
- » Eșantion de date colectate pentru reefectuarea unor operațiuni, scopul fiind de a testa controalele și calculele din aplicații

Proceduri

- Studierea documentației de sistem (manuale și termen ide utilizare) cu scopul de a înțelege principalele procese de gestionare a datoriei desfășurate în sistemele informatice; dacă documentația privind procesele DMO este insuficientă, echipa de audit va supraveghea și cartografia procesele
- Verificarea existenței unor reguli juridice privind utilizarea, mentenanța și managementul activităților economice în cadrul PDMIS
- Identificarea, cu ajutorul auditurilor precedente, a constatărilor referitoare la deficiențe ale fluxurilor de operațiuni aferente datoriei publice și/sau ale sistemelor de administrare a datoriei publice
- Identificarea controalelor generale principale pe baza documentației de sistem
- Identificarea controalelor principale din aplicații pe baza documentației de sistem: controale privind intrări, prelucrări și ieșiri de date
- Realizarea unei evaluări a riscului pe marginea acestor controale principale generale și din aplicații pentru a determina riscurile care afectează respectivele sisteme și severitatea impactului lor asupra administrării datoriei publice
- Determinarea sistemelor care afectează funcționarea și datele esențiale, precum cele de intrare, prelucrare și ieșire date, care rulează lista creditorilor, sau calcule ale datoriei publice, care generează rapoarte și cele decizionale
- Identificarea controalelor interne implementate pentru a atenua sau reduce riscurile constatate
- Ierarhizarea sistemelor și a proceselor pe baza evaluării riscului și stabilirea ariei de cuprindere a auditului

- Estimarea resurselor și a graficului de activități
- Planificarea interviurilor cu directorul departamentului IT, manageri și organismul tehnic responsabil cu activitățile de dezvoltare/mentenanță/operare a sistemului
- Dezvoltarea matricei pentru auditul controalelor generale și din aplicații și determinarea testelor de efectuat (vezi matricea sugerată în anexa III)

SAI va răspunde la următoarele întrebări

- Care sunt sistemele informatice de gestionare a datoriei publice și care este rolul fiecărui sistem în administrarea datoriei publice?
- PDMIS a fost dezvoltat în exclusivitate de către DMO sau a fost achiziționat dintr-o terță sursă? În al doilea caz, au fost realizate eventuale personalizări pentru a satisface o anumită necesitate a DMO?
- Cine ar trebui interviuat cu privire la controalele IT generale în cadrul DMO?
- Cine ar trebui interviuat pentru a oferi clarificări privind controalele din aplicații ale PDMIS?
- Cine sunt principalii utilizatori ai PDMIS?
- Care sunt controalele generale și din aplicații ale PDMIS?
- Au controalele interne capacitatea de a reduce riscurile sistemului informatic care pot afecta administrarea datoriei publice?
- Care sunt cele mai semnificative riscuri în ce privește intrările, procesările și ieșirile de date efectuate de PDMIS?
- Ce teste specifice controalelor generale și de aplicații ar trebui implementate?

ANEXA II: MATRICEA DE TESTARE PENTRU CONTROALE GENERALE

CONTROALE GENERALE		
<p>Obiectivele controalelor generale sunt de a securiza datele, proteja programele de aplicații și asigura continuitatea operațiunilor informatice în eventualitatea unor întreruperi neprevăzute.</p>		
CERINȚĂ/ FUNCȚIONALITATE	CONTROL GENERAL	PROCEDURI SUGERATE DE TESTARE
<p>Întrebări generale</p>	<p>Acțiunile departamentului IT trebuie să fie în concordanță cu misiunea DMO.</p> <p>Trebuie să existe o monitorizare a performanței PDMIS în raport cu obiectivele DMO</p> <p>Se vor efectua audituri interne periodice ale operațiunilor DMO/PDMIS</p>	<p>Analiza pe baza unui eșantion a unor decizii ale conducerii sau memorandum-uri, referitoare la măsuri din sfera IT, pentru a obține asigurarea că aceste măsuri sunt clare, corect fundamentate și respectă misiunea DMO</p> <p>Evaluarea performanței măsurilor ale PDMIS în raport cu indicatorii previzionați și asigurarea respectării de către conducere a acelor măsuri</p> <p>Evaluarea precedentelor rapoarte interne de audit privind controalele IT generale pentru a identifica deficiențe grave</p> <p>Evaluarea cantității relative și a capacității stațiilor de lucru IT și a altor dispozitive IT și asigurarea deținerii de către personal a competențelor necesare</p> <p>Evaluarea sumelor corespunzătoare alocării bugetare și compararea acestora cu</p>

		cele din perioade anterioare și cu cele ale departamentelor IT ale altor entități publice
--	--	---

<p>Controale organizaționale</p>	<p>Conducerea DMO sau ministerul de finanțe se va angaja să dezvolte și să mențină un mediu IT general pozitiv</p> <p>Personalul DMO și cel al departamentului IT va beneficia de instruire corespunzătoare periodică ce includ conștientizarea în materie de securitate a datelor</p> <p>Va exista un program de instruire</p> <p>Vor exista politici scrise și proceduri standard pentru următoarele aspecte:</p> <ul style="list-style-type: none"> • Securitatea informației • Resurse umane • Servicii IT terțe • Managementul schimbării • Acces fizic și logic • Plan de remediere și continuitate în urma dezastrelor • Politicile și procedurile standard vor fi actualizate periodic • Politicile vor fi diseminate corespunzător de către conducerea DMO • Angajații DMO vor cunoaște aceste politici 	<p>Interviuri cu membri din conducerea DMO de rang superior pe tema interesului lor față de domeniul IT, cu scopul de a evalua angajamentul acestora față de dezvoltarea și menținerea unui mediu IT general pozitiv</p> <p>Analiza probelor ce indică faptul că s-au desfășurat activități de instruire</p> <p>Interviurea personalului DMO și din departamentul IT pe următoarele teme:</p> <ul style="list-style-type: none"> • frecvența instructajelor • necesarul de cunoștințe/instruire • cunoașterea politicilor <p>Evaluarea gradului de adecvare al politicilor scrise și al procedurilor standard privind serviciile IT</p> <p>Monitorizare personalului DMO pentru a constata dacă acesta lucrează în conformitate cu procedurile standard (prevăzute într-un manual)</p>
---	---	---

<p>Controale organizaționale (cont.)</p>	<ul style="list-style-type: none"> • Vor exista proceduri documentate pentru toate activitățile de administrare a datoriei • Organizația va implementa o separare adecvată a sarcinilor pentru a se asigura faptul că utilizatorii nu dețin mai multe drepturi decât este necesar pentru activitatea pe care aceștia o realizează 	
<p>Controale fizice</p>	<p>Accesul fizic la unitatea centrală și servere va fi limitat (de exemplu, prin folosirea unor uși, încuietori etc.)</p> <p>Va exista supraveghere video</p> <p>Ferestrele încăperii care găzduiește unitatea centrală și serverele vor fi protejate împotriva pătrunderii forțate</p> <p>Toate persoanele care accesează camera serverului vor fi autorizați în acest sens</p>	<p>Se verifică existența efectivă și funcționarea unor obstacole fizice care ar preveni accesul neautorizat la unitatea centrală, serverele și stațiile de lucru ale DMO</p> <p>Se verifică dacă procedurile administrative aplicabile personalului funcționează pentru scopul pentru care acestea au fost instituite astfel încât să prevină accesul neautorizat și bruiajele serviciilor IT</p> <p>Pentru a identifica eventuale deficiențe ale controalelor automate, se va observa în ce mod funcționează instrumentele electronice – precum încuietori electronice de uși, sisteme electronice de blocare a ușilor, camere video și alte mijloace de limitare a accesului fizic la servere și alte componente critice de infrastructură</p> <p>În cazul unor sisteme de încuietori cu cheie, se va verifica partajarea parolelor între angajați</p>

<p>Controale logice</p>	<p>Dacă serviciile IT de gestionare a datoriei publice sunt externalizate, vor fi prevăzute în contract controale adecvate care interzic accesul terților la informații cu caracter secret, date importante și strategii privind administrarea datoriei publice</p>	<p>Se determină dacă profilurile de acces sunt bazate pe rolurile angajaților</p> <p>Se verifică dacă un eventual fost angajat sau o persoană ce nu este angajată de DMO încă deține un profil cu acces activ</p> <p>Se verifică dacă există firewall-uri, precum și programe antivirus, anti-malware și sisteme de alarmă antiefracție</p>
--------------------------------	---	---

<p>Controale logice (cont.)</p>	<p>Nu vor exista sub nicio formă foști angajați, persoane ce nu sunt angajate de DMO sau utilizatori virtuali cu profil activ</p> <p>Drepturile de acces vor fi verificate periodic</p> <p>Programele actualizate antivirus, de tip firewall și de detectare a breșelor și aplicațiilor malware vor fi funcționale</p> <p>Vor exista actualizări sistematice a sistemelor de operare de pe stațiile de lucru și servere</p> <p>Organizația își va defini procedurile prin care autorizează, revocă sau modifică respectivul control al accesului în urma modificării condițiilor (noi angajați, disponibilizări, schimbări de atribuții etc.)</p> <p>Organizația va comunica politica sau ghidurile sale privind parolele de securitate și alte controale de securitate (carduri de acces etc.) tuturor utilizatorilor PDMIS</p>	<p>Se verifică dacă sistemul de operare este actualizat în mod sistematic pe stațiile de lucru și servere</p> <p>Se determină dacă politica privind parolele este corect implementată</p> <p>Se verifică dacă procedurile sunt definite și documentate</p>
--	--	--

<p>Controale de mediu</p>	<p>Vor exista țevi/canale (de apă, ale sistemului de termoficare, de cabluri electrice etc.) în perimetrul camerei serverului</p> <p>Vor exista detectoare de apă, căldură și umezeală</p> <p>Camera serverului va fi prevăzută cu un sistem anti-inundații</p> <p>Vor fi prevăzute dispozitive de detecție a fumului/incendiilor</p> <p>Va exista o pardoseală înălțată sau echipamentele vor fi poziționate cu 15 – 20 de centimetri deasupra pardoselii, pe rafturi</p>	<p>Controlul și evaluarea condițiilor ambientale din camera serverului bazei de date</p> <p>Verificarea existenței și întreținerii eficiente a dispozitivelor de prevenire a incendiilor, inundațiilor și umidității</p> <p>Verificarea existenței și a funcționării eficiente a unor surse alternative de alimentare prin care se urmărește evitarea întreruperii serviciilor IT</p>
<p>Controale pentru modificări la nivelul programelor</p>	<p>Conducerea departamentului IT va păstra un jurnal de audit al problemelor, incidentelor și erorilor operaționale</p> <p>Jurnalul va permite trasabilitatea fiecărui incident, de la stabilirea cauzei care stă la baza acestui incident și până la soluționarea acestuia</p> <p>Nu vor exista în evidența biroului de asistență întrebări importante și nesoluționate privind instrucțiuni PDMIS</p> <p>Vor exista facilități de transfer decizional pe scară ierarhică pentru evenimente critice și de răspuns adecvat în funcție de prioritatea evenimentului</p>	<p>Evaluarea duratei necesare pentru a răspunde solicitărilor DMO privind instrucțiunile de utilizare sau disfuncționalități ale PDMIS</p> <p>Identificarea acelor disfuncționalități mai frecvente ale PDMIS și a cauzelor probabile</p> <p>Compararea modificărilor anterioare cu procedurile standard</p>

<p>Controale pentru modificări la nivelul programelor (cont.)</p>	<p>Se va întocmi un raport al incidentelor de securitate, care se va transmite managerilor DMO</p> <p>Modificările anterioare vor fi respectat procedurile standard</p> <p>Dacă se utilizează un sistem non-standard de administrare a datoriei, organizația va documenta procedurile de control al modificărilor și va preciza persoanele autorizate să opereze modificările în sistem</p> <p>Organizația va urmări și monitoriza toate modificările aduse sistemului de gestionare a datoriei (pistă de audit)</p>	
<p>BCP și DRP</p>	<p>Vor exista un BCP și un DRP elaborate de către DMO</p> <p>Personalul responsabil cu continuitatea operațiunilor își va cunoaște rolurile și responsabilitățile</p> <p>Vor fi raportate deficiențele indicate de teste sau evenimente efective anterioare în cadrul BCP și DRP și măsurile luate de DMO pentru a elimina acele deficiențe</p> <p>Documentația privind împrumuturile va fi stocată în mod securizat și protejată împotriva furtului, incendiului, inundației sau altor incidente care o pot deteriora sau distruge</p>	<p>Se vor evalua caracterul unitar și caracterul complet al BCP și DRP și se va verifica gradul lor de actualizare</p> <p>Se vor evalua rapoarte privind testele anterioare ale BCP, DRP și ale planului de backup</p> <p>Se va verifica dacă BCP și DRP sunt corect diseminate la nivelul întregului personal</p> <p>Se va verifica dacă respectivele copii de rezervă stocate în afara incintei se află în bune condiții și pot fi utilizate pentru a reporni sistemul în cazul unei avarii/disfuncționalități</p>

ANEXA III: MATRICEA DE TESTARE PENTRU CONTROALE DIN APLICAȚII

STANDARDE PRIVIND DOCUMENTAȚIA		
<p>Obiectivele standardelor corespunzătoare pentru documentații sunt de a asigura funcționarea controalelor în mod continuu și de a reduce riscul de eroare.</p>		
CERINȚĂ/ FUNCȚIONALITATE	CONTROL GENERAL	PROCEDURI SUGERATE DE TESTARE
Controale privind documentația	Documentația aplicației va fi suficient de cuprinzătoare (cu referire la toate funcționalitățile aplicației și la funcționalități conexe)	Verificarea documentației
	Documentația va fi actualizată pentru a reflecta modificările aduse aplicației	Verificarea documentației
	Controalele din aplicații incluse în documentație vor fi implementate și efectiv funcționale	Verificarea unui eșantion de controale de aplicații pentru a determina dacă acestea sunt implementate potrivit documentației și funcționează efectiv
copii de siguranță pentru documentații	Va fi păstrată o copie de rezervă a documentației	Verificarea facilităților copiilor de siguranță pentru documentații
CONTROALE PRIVIND INTRĂRILE		

Obiectivul controalelor privind intrările este de a asigura autorizarea, acuratețea, caracterul complet și caracterul de actualitate al datelor introduse într-o aplicație.		
CERINȚĂ/ FUNCȚIONALITATE	CONTROL de APLICAȚIE	PROCEDURI SUGERATE DE TESTARE
Câmpuri cu introducere obligatorie a datelor	Aplicația nu permite confirmarea funcționării dacă eventuale câmpuri cu introducere obligatorie a datelor nu sunt completate	Confirmarea funcționării prin omiterea datelor necesare și asigurarea faptului că tranzacția nu a fost prelucrată Aplicarea acestui test pentru următoarele procese: înregistrare contract, intrare în efectivitate contract, înregistrare emisiune titlu de stat și așa mai departe
Introducerea datelor corecte și adecvate	Aplicația nu acceptă introducerea unor date incorecte și necorespunzătoare	Verificarea formatului datelor în baza de date Analiza specificațiilor de înregistrare și verificarea unora la nivel de aplicație Se încearcă introducerea unor date incorecte sau inadecvate și se asigură faptul că datele nu sunt acceptate și este generat un mesaj de eroare Aplicarea acestor teste pentru următoarele procese: înregistrare contract, activare contract, înregistrare emisiune titlu de stat, actualizări ale formulelor de calcul din prospectele de emisiune în conformitate cu anumiți indici, răscumpărarea titlului de stat, și așa mai departe
	Aplicația nu permite duplicarea datelor	Se încearcă înregistrarea unui contract sau titlu de stat purtând denumirea unuia deja existent și se asigură faptul că datele nu sunt acceptate și se generează un mesaj de duplicare

	În cazul ratelor de dobândă contractuale, nu vor exista perioade suprapuse sau neacoperite cu privire la aplicabilitatea ratelor de dobândă	Verificarea existenței în baza de date a unor perioade cu rate de dobândă suprapuse sau neacoperite
--	---	---

Introducerea datelor corecte și adecvate (cont.)	În cazul unui contract de donație, aplicația va permite introducerea tragerilor întrucât, în acest caz, nu există înregistrări de rambursări și operațiuni de plată a dobânzilor	Se încearcă introducerea unui vărsământ dintr-un contract de donație și se asigură faptul că aplicația nu impune efectuarea unor operațiuni de rambursare și plăți de dobânzi
	În ecranul de înregistrare a datelor referitoare la trageri, când utilizatorul caută contracte pentru a înregistra o trageri, aplicația va afișa doar contracte cu starea actuală „activ” în faza de trageri sau cea de trageri și rambursări	Se încearcă introducerea unei trageri și să verifice faza contractelor afișată de către aplicație
	Dacă rata dobânzii este variabilă, aplicația va impune includerea indicelui	Se verifică dacă aplicația solicită anumiți indici când este selectată o rată variabilă a dobânzii
	Aplicația nu va permite introducerea unor numere cu zecimale pentru valorile emisiunilor de titluri de stat	Se încearcă introducerea unor numere zecimale pentru valorile titlurilor de creanță emise și se asigură faptul că aplicația nu acceptă intrarea de date
	Aplicația va permite înregistrarea operațiunii de emiteri a unui titlu de stat anterior datei lansării titlului de stat	Simularea înregistrării unei operațiuni de emiteri a unui titlu de stat anterior datei lansării titlului de stat
Caracterul complet al informațiilor	Toate informațiile relevante despre datorii vor fi introduse în aplicație	Se verifică dacă toate datele importante despre datorii sunt introduse în aplicație, de exemplu, operațiuni de credit, garanții,

		împrumuturi, rate ale dobânzii și cursuri de schimb valutar
Compatibilitate între date calendaristice	Data de începere a calculului comisionului de angajament va fi anterioară datei de finalizare a proiectului	Se încearcă introducerea unei date de începere a calculării comisionului de angajament ulterior datei de finalizare a proiectului și se verifică dacă datele nu sunt acceptate și dacă este generat un mesaj de eroare

Compatibilitate între date calendaristice (cont.)	Data intrării în efectivitate a proiectului va fi anterioară datei limită de efectuare a plăților	Se încearcă introducerea unei date de intrare în efectivitate a proiectului ulterior datei de finalizare a proiectului și se verifică dacă datele nu sunt acceptate și dacă este generat un mesaj de eroare
	Data intrării în efectivitate trebuie să fie anterioară datei limită pentru efectuarea plăților	Se încearcă introducerea unei date de intrare în efectivitate ulterioară datei limită pentru efectuarea plăților și se verifică dacă datele nu sunt acceptate și dacă este generat un mesaj de eroare
	Data limită pentru efectuarea plăților trebuie să fie anterioară datei de finalizare a proiectului	Se încearcă introducerea unui termen limită pentru efectuarea plăților ulterior datei de finalizare a proiectului și se verifică dacă datele nu sunt acceptate și dacă este generat un mesaj de eroare
	Pentru a întocmi graficul de rambursare, data scadenței titlului de stat va fi ulterioară datei emisiunii	Se încearcă introducerea unei date a emisiunii ulterioară datei finale a scadenței titlului de stat și se verifică dacă este generat un mesaj de eroare

	<p>Aplicația nu acceptă date ulterioare pentru operațiuni</p>	<p>Se încearcă efectuarea unor operațiuni prin introducerea unei date ulterioare și se verifică dacă datele nu sunt acceptate și dacă este generat un mesaj de eroare</p> <p>Se aplică acest test pentru următoarele procese: înregistrare contract, activare contract, înregistrare emisiune titlu de stat, actualizări ale formulelor de calcul din prospectele de emisiune în conformitate cu anumiți indici, răscumpărare titlu de stat, înregistrare plăți efectuate, act adițional la contract și așa mai departe</p>
	<p>Data emisiunii titlului de stat va fi anterioară datei scadenței/maturității</p>	<p>Se încearcă introducerea unei date de emisiune a titlului de stat ulterioară datei scadenței și se verifică dacă datele nu sunt acceptate și dacă este generat un mesaj de eroare</p>

<p>Compatibilitate între date calendaristice (cont.)</p>	<p>Când se înregistrează o sumă aferentă unui grafic de rambursare [graficul datelor și sumelor de rambursare a unui împrumut], în situații în care suma sau data introdusă diferă de cea din aplicație, aplicația va informa utilizatorul, printr-un mesaj afișat, în legătură cu o astfel de situație, înainte de a finaliza confirmarea operațiunii</p>	<p>Se înregistrează o plată a cărei date și valori sunt diferite de cele din aplicație și se verifică dacă aplicația afișează un mesaj</p>
	<p>Dacă data lichidării este diferită de data scadenței, aplicația va impune completarea câmpului</p>	<p>Se introduc date diferite pentru scadență și lichidare și se verifică dacă aplicația solicită o justificare sau o aprobare</p>

	„justificare” sau „aprobat de creditor”	
	Calendarul plăților nu va prezenta perioade suprapuse; de exemplu, data inițială a celei de-a doua plăți nu va fi la o dată anterioară datei finale a primei plăți de-al doilea vărsământ nu poate fi înainte de data primului vărsământ	Se încearcă înregistrarea clei de-a doua plăți la o dată anterioară datei primei plăți și se verifică dacă datele nu sunt acceptate și dacă este generat un mesaj de eroare

Securitatea introducerii datelor și a operațiunilor cu date	Aplicația nu va permite persoanelor neautorizate să introducă eventuale date și să execute eventuale operațiuni	<p>Se asigură faptul că există token și alte cerințe pentru anumite profiluri de utilizatori</p> <p>Se încearcă introducerea unor date și execuția unor operațiuni fără a dispune de un profil corespunzător și se asigură faptul că acest lucru nu este permis</p> <p>Se aplică acest test pentru următoarele procese: înregistrare contract, activare contract, înregistrare emisiune titlu de stat, actualizări ale formulelor de calcul din prospectele de emisiune în conformitate cu anumiți indici, răscumpărare titlu de stat, înregistrarea unei plăți și așa mai departe</p>
	Aplicația va înregistra un jurnal de acces privind introducerea manuală a datelor	Se verifică jurnale de acces restricționat și se asigură faptul că jurnalele nu pot fi vizualizate sau modificate de persoane fără aprobare în acest sens

	Aplicația nu va permite modificarea unei valori dintr-un contract activ	Se încearcă modificarea unei valori dintr-un contract activ și se asigură faptul că acest lucru nu este permis
	Aplicația va preveni modificarea datelor și ștergerea contractelor cu stare actuală „anulat” sau „finalizat”	Se încearcă modificarea și ștergerea unui eșantion de contracte cu stare actuală „anulat” sau „finalizat”, și se asigură faptul că acest lucru nu este permis
	Aplicația nu va permite ștergerea unui contract activ decât dacă acel contract este în faza de negocieri	Se încearcă ștergerea unui contract activ ce nu se află în etapa negocierilor și se asigură faptul că acest lucru nu este permis
	Aplicația nu va permite excluderea necorespunzătoare a unui titlu de stat emis decât în cazul în care nu există nicio operațiune care are legătură cu acel titlu de stat	Se încearcă ștergerea unui titlu de stat emis care nu are nicio legătură cu o operațiune și se verifică faptul că acest lucru nu este permis

Securitatea introducerii datelor și a operațiunilor cu date (cont.)	Aplicația va impune dublă autorizare pentru a efectua operațiuni critice	Se verifică dacă operațiunile critice impun dublă autorizare pentru a fi realizate Se aplică acest test pentru următoarele procese: activare contract, emisiune unui titlu de stat, grafic de rambursare , răscumpărare titlu de stat, modificări ale valorii contractului , plata cuponului, răscumpărare anticipată a titlului de stat [tranzacția de rambursare înainte de scadență a unei datorii existente], modificări de rată a dobânzii și așa mai departe
--	--	---

	<p>Aplicația acceptă doar înregistrări de date din surse recunoscute; împrumutul introdus va fi în conformitate cu acordul de împrumut/acordul de finanțare și cu standardele acceptate</p>	<p>Se verifică dacă informații cheie sunt introduse de două ori și se asigură afișarea unui mesaj de eroare atunci când înregistrările sunt diferite</p>
	<p>Aplicația va permite reducerea valorii contractului doar dacă aceasta nu depășește valoarea „sumei rămășiță de rambursat”</p>	<p>Se încearcă reducerea valorii contractului la o valoare care este mai mare decât valoarea soldului rămas de rambursat și se verifică dacă datele nu sunt acceptate și dacă este generat un mesaj de eroare</p>
	<p>Aplicația va înregistra toate tranzacțiile o singură dată</p>	<p>Se efectuează o serie de tranzacții identice (de exemplu, plata unor tranșe din graficul de amortizare de amortizare) și se asigură faptul că tranzacțiile nu sunt dublate în baza de date</p>
	<p>Când se înregistrează o plată, dacă se revocă permisiunea utilizatorului, aplicația va raporta revocarea doar în cazul în care utilizatorul încearcă să introducă plata, permițând astfel jurnalizarea atât pentru tentativa eșuată, cât și pentru datele pe care utilizatorul a dorit să le introducă</p>	<p>Se încearcă înregistrarea unei plăți cu permisiune revocată și se asigură faptul că datele nu sunt acceptate iar tentativa este jurnalizată</p>
<p>Compatibilitate între valori</p>	<p>În cazul transferurilor automate de fișiere între aplicații, PDMIS va păstra datele inițiale primite de la alte aplicații pe o perioadă prestabilită de către DMO</p>	<p>Se verifică datele întreținute transferate din alte aplicații pentru a se asigura faptul că datele sunt criptate sau protejate împotriva daunelor, pierderii sau breșelor</p>

	Aplicația nu va permite modificarea ratelor de dobândă ale unei tranșe care a fost deja plătită, și orice modificare a unei rate de dobândă necesită o a doua aprobare pentru a fi finalizată	Se încearcă modificarea unei rate de dobândă a unei tranșe plătite și se verifică dacă datele nu sunt acceptate; de asemenea, se verifică dacă aplicația necesită o a doua aprobare pentru modificarea unei rate de dobândă
	Valoarea tranșei va fi mai mică decât valoarea contractată	Se încearcă introducerea unei tranșe mai mari decât valoarea din contract și se verifică dacă datele nu sunt acceptate și dacă este generat un mesaj de eroare
	Valoarea de răscumpărare va fi mai mică decât valoarea titlurilor de stat subscrise în cadrul unei emisiuni de titluri de stat	Se încearcă efectuarea răscumpărării titlurilor de stat la o valoare mai mare decât valoarea titlurilor de stat subscrise în cadrul unei emisiuni de titluri de stat și se verifică dacă datele nu sunt acceptate și dacă este generat un mesaj de eroare
	Înainte de prelucrarea datelor aplicația afișează o alertă privind plățile restante sau plățile nedatorate	Se simulează înregistrarea unei plăți restante sau a unei plăți nedatorate și se verifică emiterea alertei
Documente sursă	Va exista o pistă de documente sursă referitoare la intrări, garantând autenticitatea intrărilor de date	Sunt selectate câteva intrări de date și se verifică dacă acestea prezintă documente sursă aferente (de ex., contract de împrumut, email, etc.)

CONTROALE PRIVIND PRELUCRAREA

Obiectivul controalelor privind prelucrarea datelor este de a asigura faptul că datele sunt corect prelucrate prin intermediul aplicației și că nu se vor adăuga, pierde sau modifica date pe parcursul prelucrării.

CERINȚĂ/ FUNCȚIONALITATE	CONTROL DE APLICAȚIE	PROCEDURI SUGERATE DE TESTARE
-----------------------------	----------------------	----------------------------------

Indicarea stării actuale corecte	Aplicația va modifica starea actuală a contractului după tragerea integrală a sumelor din împrumut	Se simulează tragerea integrală și se verifică dacă starea actuală a contractului se schimbă din „trageri în curs desfășurare” în „integral tras”
	Aplicația va schimba starea actuală a titlurilor de stat atunci când emisiunile de titluri de stat sunt lansate în cadrul unui Program	Se simulează lansarea emisiunii de titluri de stat și se verifică dacă starea actuală a titlului de stat se schimbă din „inactiv” în „activ”
	Aplicația va modifica starea actuală a unui contract sau titlu de stat după plata integrală a sumei datorate respectiv după rambursare/răscumpărare	Se simulează ultima plată și se verifică dacă s-a modificat starea actuală a contractului sau a titlului de stat
	<p>Aplicația trebuie să prevadă cel puțin următoarele faze:</p> <ul style="list-style-type: none"> • Trageri: în această fază sunt efectuate trageri din împrumut • Integral tras: în această fază tragerile nu sunt permise • Finalizat: în această fază, nu mai pot fi efectuate operațiuni financiare aferente tragerilor și nu este permisă modificarea datelor 	Se înregistrează un contract de împrumut, se încearcă efectuarea unei trageri în fiecare fază, și se asigură faptul că datele nu sunt acceptate și se generează un mesaj de eroare

Indicarea stării actuale corecte (cont.)	<p>Aplicația va conține reguli privind redarea unui statut de contract (activ sau inactiv) compatibil cu fazele (trageri, , , integral tras, rambursare, tras și rambursat) pentru a preveni eventuale contradicții în informațiile oferite; de exemplu, un contract care figurează cu stare actuală „inactiv” nu se poate afla în faza de trageri sau rambursări</p>	<p>Se simulează anumite modificări în statutul contractului și în fazele contractului și se verifică dacă există compatibilitate între contract și faze</p>
	<p>Aplicația trebuie să conțină un program care actualizează fazele contractului; de exemplu, când soldul ce urmează a fi tras este egal cu zero, aplicația va modifica faza din „trageri în curs de desfășurare” în „ integral tras”</p>	<p>Se simulează condițiile necesare pentru a modifica faza contractuală și se verifică producerea modificării</p>
Calcul corect	<p>Aplicația va efectua calculul corect</p>	<p>Se verifică respectivul calcul prin reefectuare. Se aplică acest test de calcul următoarelor informații: stocul datoriei datorie publică directă și datorie publică garantată), scadență, grafic de amortizare (date calendaristice și valori), valoarea comisioanelor agenților, graficul rambursărilor titlurilor de stat , valoarea nominală a titlului de stat răscumpărat și așa mai departe</p>

Calcul corect (cont.)	După o serie de modificări la nivelul intrărilor, aplicația va actualiza datele	Se efectuează o serie de modificări la nivelul intrărilor și se verifică actualizările datelor; de exemplu: <ul style="list-style-type: none"> • Se simulează o plată și se verifică dacă soldul restant/datoriile exigibile și graficul de amortizare au fost actualizate • Se modifică unii indici și se verifică dacă valoarea stocului datoriei s-a actualizat
	Aplicația va conține în programarea sa cel puțin următoarele metode de calcul a tranșelor: distribuție uniformă, dobândă simplă, tranșă, aplicare a prețului, rambursare constantă, structura coșului valutar (BIRD) și coș de valute UAC (IDB)	Se verifică metodele utilizate de sistem pentru a calcula tranșele; corectitudinea metodelor poate fi verificată utilizând eșantionarea datelor
	Ori de câte ori se schimbă valoarea din câmpul „Valoarea Contractată”, aplicația va recalcula valoarea din câmpul „Sold sume netrase ”	Se modifică Valoarea Contractată și se verifică dacă Soldul netras a fost actualizat corect

Calcul corect (cont.)	<p>Aplicația va genera automat calendarul tranșelor printr-una din metodele posibile de mai jos:</p> <ul style="list-style-type: none"> • Data primei trageri și numărul tranșelor cu sume fixe • Data primei trageri, data finală de tragere și valoarea tranșelor în ordine descrescătoare • Data primei trageri , data finală de tragere și numărul tranșelor cu sume fixe • Data primei trageri și termenele de tragere • Termene 	<p>Se inserează datele solicitate de fiecare metodă posibilă și se verifică dacă datele calendaristice ale tranșelor sunt corecte</p>
	<p>Când data tranșei cade într-o zi nelucrătoare, aplicația va oferi două opțiuni: mutarea datei în următoarea zi lucrătoare sau în ziua lucrătoare anterioară</p>	<p>Se configurează o tranșă cu data unei zile nelucrătoare și se verifică dacă aplicația oferă opțiunea de a schimba data în ziua lucrătoare anterioară sau în următoarea zi lucrătoare</p>
	<p>Sistemul va actualiza automat valoarea nominală a titlurilor de stat ori de câte ori se modifică anumiți indici</p>	<p>Se modifică formulele de calcul din prospectele de emisiune în conformitate cu anumiți indici și se verifică dacă valoarea nominală a titlurilor de stat este actualizată</p>
	<p>În cazul achitării unei sume mai mici decât cea calculată de aplicație, se va afișa un mesaj în momentul introducerii plății; mesajul se va repeta până la data scadenței următoarei tranșe de plată</p>	<p>Se simulează o plată mai mică decât suma calculată de aplicație și se verifică generarea unui mesaj, precum și dacă mesajul se repetă până la data următoarei tranșe de plată</p>

Calcul corect (cont.)	În baza sa de date, sistemul va fi capabil să diferențieze instrumentele de datorie publică prin simulări de emisiuni de titluri de stat	În cadrul bazei de date, se verifică dacă emisiunile de titluri de stat sunt diferențiate și dacă sunt excluse din calcul stocului datoriei și al maturității titlurilor de stat
	Când un utilizator șterge un titlu de stat, aplicația va șterge valorile aferente din baza de date	Se șterge un titlu de stat și se verifică dacă valoarea sa este ștearsă din baza de date
	Titlurile de stat cu statutul „anulat” nu vor fi incluse în calculul instrumentelor datoriei publice (de ex., RIR, maturitate etc.), mai exact, după anularea acestora, valorile respective vor fi excluse permanent din baza de date	Se modifică statutul unui titlu de stat în „anulat” și se verifică dacă valoarea sa este exclusă din calcule (respectiv din calculul stocului datoriei publice, al scadențelor etc.)
Control adecvat al erorilor de prelucrare	Aplicația va trata diferit plățile restante	Se verifică dacă aplicația calculează corect toate costurile aferente plăților restante
	Prelucrarea erorilor cu vechime de mai multe zile / săptămâni nu va rămâne nesoluționată	Se verifică dacă există eventuale criterii privind numărul de zile necesare pentru a soluționa erorile din sistem, se verifică eventuale mesaje de eroare și se discută cu managerii de sistem/datoriei măsurile luate pentru a remedia eventuale disfuncționalități
	Dacă există o eroare de prelucrare, aplicația va anula prelucrarea și va stoca în baza de date data calendaristică, ora și motivele tehnice ale problemei	Se simulează o eroare de proces și se verifică dacă aplicația stochează în baza de date data calendaristică, ora și motivele tehnice ale problemei

Înregistrare corectă	Aplicația va permite administratorilor datoriei să înregistreze cu acuratețe fluxurile de numerar (asociate împrumuturilor în monede naționale și în valute străine, activităților de acoperire și tranzacționare, garanțiilor și creditărilor din fonduri atrase), , aferente tuturor tranzacțiilor	Se efectuează o tranzacție și se verifică dacă evidența acesteia este corectă și exactă
	Aplicația va păstra un istoric al tranzacțiilor realizate pe perioada contractului și va include detalii despre creditor, valoarea contractată și data de finalizare a proiectului, dar și datele limită de tragere	Se verifică dacă tranzacțiile din istoric asociate unui titlu de stat sau contract corespund datelor din jurnalul de datorii al aplicației
Sarcini corecte în graficul lucrărilor	Aplicația va avea facilitate de inițiere automată a sarcinilor din graficele fixate de DMO pentru actualizarea indicilor, stocului datoriei și așa mai departe	Se verifică inițierile automate și funcționarea corespunzătoare a acestui proces
	Pentru un tip de titlu de stat a cărui maturitate este stabilită la aceeași dată ca și cea a plății dobânzii, sistemul va asigura faptul că atât dobânda, cât și maturitatea au același grafic de plăți	Se creează un titlu de stat a cărui maturitate este stabilită la aceeași dată ca și cea a plății dobânzii și se verifică dacă cele două au același grafic de plăți
	Se va păstra o pistă de audit al PDMIS, ce permite identificarea etapelor respectiv contractarea datoriei publice, emisiunile de titluri de stat respectiv de la data semnării unui acord de împrumut/data lansării emisiunilor până la data rambursării/răscumpărării	Se verifică pista de audit pentru un eșantion de contracte de împrumut și emisiuni de titluri de stat, de la semnare / lansare emisiune până la rambursare/răscumpărare

CONTROALE PRIVIND IEȘIRILE		
Obiectivul controalelor privind ieșirile este de a asigura integritatea datelor de ieșire, precum și distribuția corectă și în timp util a datelor de ieșire produse.		
CERINȚĂ/ FUNCȚIONALITATE	CONTROL DIN APLICAȚIE	PROCEDURI SUGERATE DE TESTARE
Control privind utilizatorii informațiilor	Aplicația va dispune de un jurnal de raportare în care va înregistra numele utilizatorilor care au solicitat rapoarte, precum și datele calendaristice și orele solicitărilor	Se solicită a serie de rapoarte și se verifică dacă aplicația înregistrează solicitările
	Aplicația va solicita autorizație specială pentru a încărca anumite rapoarte (în special cele care conțin informații sensibile)	Se încearcă generarea acestor rapoarte
Raportare credibilă și în timp util	Aplicația va furniza rapoarte predefinite (clasificare în funcție de instrumentele datoriei publice cum ar fi spre exemplu obligațiuni, împrumuturi, tranșe, de ex., scadență, statut, surse de finanțare, tip de finanțare, credit, tip de instrument, termeni, facturi neachitate etc.)	Se încearcă generarea unor rapoarte predefinite
	Aplicația va furniza rapoarte în mod corespunzător, asigurând caracterul complet și integritatea informațiilor	Se verifică dacă rapoartele sunt generate în conformitate cu termenii de utilizare Se verifică dacă rapoartele au paginile numerotate și conțin valori totale Se aplică acest test următoarelor rapoarte: Raport privind scadența (pentru datoria publică directă și datoria publică garantată), Raport privind Soldul

		Restant, Raport de Intrări, și așa mai departe
--	--	--

<p>Raportare credibilă și în timp util (cont.)</p>	<p>Aplicația va permite următoarele tipuri de raportare, atât globală (toate titlurile de stat) cât și specifică:</p> <ul style="list-style-type: none"> • După starea actuală a titlurilor de stat (emise, anulate, răscumpărate etc.) • Pentru evenimente dintr-un anumit interval calendaristic (emisiuni, răscumpărări etc.) • După scadențe termen scurt și lung • După criteriul rezidenței • După tipul instrumentului de datorie publică • După scadență 	<p>Se încearcă generarea unor rapoarte, globale și specific, folosind drept criterii datele de mai jos:</p> <ul style="list-style-type: none"> • starea actuală a titlurilor de creanță (emise, anulate, răscumpărate etc.) • Evenimente dintr-un anumit interval calendaristic (emisiuni, răscumpărări etc.) • Datorie publică contractată pe termen scurt și lung • criteriul rezidenței • Tipul instrumentului de datorie publică • Maturitatea titlurilor de stat
	<p>Rapoartele vor prezenta informații complete și corecte</p>	<p>Se generează rapoarte și se reevaluează calculele</p> <p>Se aplică acest test următoarelor rapoarte: grafic de rambursare (pentru datoria publică directă și datoria publică garantată), Raport privind Soldul Restant, Raport de Intrări, și așa mai departe</p>

	Rapoartele vor prezenta exact aceleași informații redade și în forma în care acestea sunt redade pe ecranele aplicației	Se compară rapoarte pentru a se determina corelarea cu informațiile prezentate pe ecranele aplicației Se aplică acest test următoarelor rapoarte: grafic de rambursare la scadență (pentru datoria publică directă și datoria publică garantată), Raport privind Soldul Restant, Raport de Intrări, și așa mai departe
	Valorile prezentate în Raportul de Scadență, Raport privind Soldul Restant și Raportul privind stocul de datorie publică se vor corela	Se compară aceste rapoarte pentru a se determina gradul lor de corelare

Raportare credibilă și în timp util (cont.)	Sistemul va avea capacitatea de a produce rapoarte privind totalurile datoriei, individuale și agregate, cu preconizarea serviciului datoriei pentru împrumuturi și titluri de creanță existente și viitoare	Se încearcă generarea unor rapoarte de acest gen Se verifică dacă rapoartele acoperă concomitent operațiuni existente și așteptate privind datoriile
	Aplicația va genera automat rapoarte privind operațiunile financiare zilnice pentru toate contractele active; de asemenea, va permite generarea manuală a rapoartelor pentru anumite contracte	Se verifică generarea automată a unor rapoarte pentru toate contractele active și se încearcă generarea manuală a rapoartelor pentru anumite contracte
Transfer corect al datelor	Transferul datelor între aplicații, etapele de prelucrare, sau ambele tipuri de operațiuni, vor fi exacte și complete	Se simulează un transfer de date între aplicații și se verifică acuratețea și caracterul complet al datelor

Mesaje utile de ieșire	<p>Când un utilizator accesează aplicația, aceasta va afișa un mesaj cu următoarele informații:</p> <ul style="list-style-type: none"> • Contracte care ajung la scadență în următoarele 5 zile • Contracte cu plăți restante ale tranșelor • Contracte cu tranșe parțial achitate • Contracte cu date depășite ale tragerilor • Contracte cu termen limită de plată de 5 zile (aplicația va transmite un mesaj zilnic până când se efectuează plata, valoarea sumei netrase este anulată sau se modifică termenul limită de tragere) 	Se accesează aplicația și se verifică dacă aceasta afișează toate mesajele în cauză
-------------------------------	--	---

Mesaje utile de ieșire (cont.)	Aplicația va indica statutul calculului drept „calcul în desfășurare” sau „calcul finalizat”	Se solicită un calcul și se verifică dacă aplicația indică statutul operațiunii
	La finalul generării raportului, aplicația va afișa un mesaj de finalizare a generării acelui raport sau va afișa raportul solicitat	Se solicită un raport și se verifică dacă aplicația afișează un mesaj de finalizare a operațiunii sau afișează raportul solicitat
	Aplicația va indica statutul raportului generat drept „în desfășurare” sau „finalizat”	Se generează un raport și se verifică dacă aplicația indică statutul operațiunii
	Dacă ratele dobânzilor suferă modificări, aplicația va afișa un mesaj de alertă	Se modifică ratele dobânzilor și se verifică emiterea unui mesaj de alertă

	<p>Înainte de a prelucra ștergerea sau răscumpărarea unui titlu de creanță, aplicația va afișa un ecran cu informațiile ce urmează a fi șterse sau răscumpărate în vederea conformării operațiunii de către utilizator</p>	<p>Se încearcă răscumpărarea sau ștergerea unui titlu de creanță și se verifică dacă aplicația afișează un mesaj solicitând utilizatorului să confirme operațiunea</p>
--	--	--

FIGURA 1: AUDITURI ALE DATORIEI PUBLICE EFECTUATE DE SAI-URI: CAZUL BRAZILIEI

Audit efectuat în 2014 de către Curtea de Audit a Braziliei pe marginea Sistemului Integrat de Administrare a Datoriei (SID) al Guvernului Federal din Brazilia

Ținând cont de faptul că SID este testat în ce privește datoria internă securitizată, echipa de audit a ales să se concentreze exclusiv pe testarea proceselor specifice administrării datoriei externe (directă și garantată). Observațiile și constatările auditului au fost după cum urmează:

Strategia privind administrarea și gestionarea Sistemului IT

Potrivit Manualului său de Utilizare, după implementarea sa integrală, SID va asigura următoarele funcții:

- a) o gamă diversă de calcule, precum valoarea nominală actualizată, prețul de emisiune, stocul datoriei publice (de titluri de creanță contractuale și securitizate), planificarea financiară a contractelor, precum și stabilirea prețurilor de emisiune pentru titlurile de stat subscribe și a datelor scadențelor;
- b) o varietate de căutări și rapoarte privind înregistrarea datelor și rezultatele calculelor;
- c) operațiuni financiare, precum emisiuni de obligațiuni, scadența, răscumpărare și transfer, printre altele; și
- d) un registru de informații utilizat la potențial maxim în diversele module de activități economice.

Cu privire la strategia de administrare și gestionare a sistemului IT, principalele observații și constatări de audit au fost după cum urmează:

- Nu există niciun program de instruire pentru cel mai frecvent utilizate sisteme de administrare a datoriei publice, Seorfi și SID.
- Nu există o dată preconizată pentru implementarea integrală a SID, inclusiv cu privire la datoria internă garantată.
- Unele operațiuni importante, precum intrarea în efectivitate a contractului, rambursări, plăți anticipate, modificări ale ratelor de dobândă sau modificări ale valorii contractului, sunt efectuate de o singură persoană. Sistemul nu solicită aprobare sau dublă autorizare. Siguranța operațiunilor depinde strict de gradul de adecvare al profilului, generând o problemă privind separarea atribuțiilor.
- O altă problemă privind separarea atribuțiilor este lipsa personalului dedicat dezvoltării SID; personalul DMO dezvoltă sistemul, îndeplinind în paralel funcțiile obișnuite ale oficiului.
- Evaluarea vulnerabilității proceselor IT la riscuri operaționale este finalizată, însă evaluarea mecanismelor de atenuare a acestor riscuri încă nu a avut loc.

Controale de Securitate și de Mediu

Cu referire la controale de securitate și de mediu, principalele observații și constatări de audit au fost după cum urmează:

- DMO nu a desemnat un Director de Comunicare și Securitate a Informației, iar Comitetul de Securitate a Informației, însărcinat cu numirea în funcție a directorului, nu și-a început efectiv activitatea.
- Nu există un BCP oficial, iar procesele funcționale de administrare a datoriei publice sunt în curs de analiză în scopul întocmirii unui plan BCP.
- Analizele echipei de audit au remarcat existența unui număr de trei utilizatori generici, ceea ce îngreunează bunele practici IT, dat fiind articolul 11.2.1 din ISO / IEC 27002: 2005, care recomandă utilizarea unui identificator unic pe utilizator pentru a asigura responsabilizarea fiecărui utilizator în sistem.

- În ciuda faptului că definirea accesului la SID ar trebui realizată exclusiv printr-un certificat digital A3, iar accesul pe bază de cod numeric personal și parolă ar trebui să constituie o excepție, analiza bazei de date cu utilizatori ai SID indică faptul că nu există niciun termen limită de utilizare a excepției.
- Analiza bazei de date cu utilizatori ai SID indică disfuncționalități în procesul de revizuire a accesului utilizatorilor.
- Echipa de audit a detectat disfuncționalități și la nivelul mentenanței de rutină a bazei de date cu utilizatori ai SID.
- SID nu înregistrează piste de audit pentru majoritatea tranzacțiilor sale și, drept rezultat DMO nu efectuează evaluări periodice ale pistelor de audit generate de sistem, la fel cum nu monitorizează tranzacțiile SID.
- SID nu dispune de o funcție de auditare care să genereze, să stocheze și să analizeze în mod curent jurnalul de sistem.
- Echipa de audit a remarcat lipsa unui plan de testare și a rezultatelor sale aferente la nivelul sistemelor utilizate frecvent de către DMO, Seorfi și SID.
- Echipa de audit nu a primit confirmarea faptului că o echipă de intervenție în caz de incidente a fost creată pentru rețelele informatice, având sarcina de a recepționa, evalua incidente de securitate și a interveni în urma acestora.
- Echipa de audit a remarcat lipsa unui plan de continuitate a serviciilor IT, acesta fiind documentul oficial corespunzător care descrie inițiativele de continuitate pentru toate serviciile IT administrate de agenție sau entitate.

Controale Operaționale și Documentație

Cu referire la controalele operaționale și documentație, principalele observații și constatări de audit au fost după cum urmează:

- Interfața nu este foarte prietenoasă, din acest motiv utilizatorii SID necesitănd un volum mai mare de cunoștințe prealabile despre sistem.
- Nu există un manual de utilizare al SID.

- Viteza prelucrării calculelor este scăzută. Acest lucru împiedică generarea simultană a unor calcule și rapoarte. Întrucât există mai mulți utilizatori simultani ai sistemului, această problemă ar putea reduce eficiența sistemului.

Echipa de audit a sugerat DMO să evalueze îmbunătățirile pentru a spori capacitatea de prelucrare a sistemului.

Controale de Aplicații

După ce echipa de audit a testat la nivelul SID controalele privind intrările, prelucrarea și ieșirile aferente administrării datoriei publice externe, constatările și observațiile auditului au fost după cum urmează:

- Numeroase mesaje de eroare nu sunt clare și, uneori, nu sunt afișate utilizatorului.
- Prin intermediul testelor pe controalele de aplicații privind intrările de date, echipa de audit a identificat o serie de mesaje de eroare ce nu explicau cauza erorii.
- Prin intermediul testelor pe controalele de aplicații privind prelucrarea datelor aferente datoriei directe externe, echipa de audit a identificat o diferență între valorile din Raportul Financiar al Fluxurilor de Numerar, diferență cauzată de efectuarea unei plăți anticipate care nu a fost luată în considerare în raport.
- Cu ocazia testelor pe controalele de aplicații privind ieșirile de date, echipa de audit a constatat că, dacă datele introduse nu sunt corecte, aplicația nu generează unele rapoarte privind datoria publică directă, conform așteptărilor, la fel cum nu reușește să atragă atenția utilizatorului asupra erorii.
- Prin intermediul testelor pe controalele de aplicații privind ieșirile, echipa de audit a identificat erori în rapoarte privind datoria publică directă cauzate de utilizarea de către sistemul IT a unor indici neactualizați.
- Unele rapoarte privind datoria publică directă au fost emise cu informații incomplete.

Recomandări

Ținând cont de constatările și observațiile auditului, echipa de audit a recomandat ca, în termen de 90 zile, Secretariatul Trezoreriei Naționale să formuleze un plan de acțiune ce conține graficul de implementare pentru următoarele:

- Stabilirea unei date așteptate pentru implementarea totală a SID, inclusiv privind datoria internă garantată .
- Desemnarea Directorului de Comunicare și Securitate a Informației și a membrilor Comitetului de Securitate a Informației.
- Oficializarea planului BCP.
- Oficializarea Planului de Continuitate a Serviciilor IT.
- Crearea unei Echipe de Intervenție în caz de Incidente pentru Rețele Informaticе.
- Evaluarea și atenuarea riscurilor operaționale IT.
- Analiza mentenanței automate zilnice de rutină a bazei de date cu utilizatori ai SID.
- Analiza procesului de evaluare a accesului utilizatorilor SID.
- Analiza procesului generic de acordare a accesului pentru utilizatorii SID.
- Stabilirea procedurilor pentru analiza periodică a pistelor de audit generate de SID.
- Furnizarea înregistrărilor din jurnalului aplicației generate de SID.
- Analiza mesajelor de eroare din SID.
- Dezvoltarea manualului de utilizare al SID.
- Analiza rutinei de raportare a SID.

FIGURA 2: AUDITURI ALE DATORIEI PUBLICE EFECTUATE DE SAI-URI: CAZUL MOLDOVEI

Evaluarea controalelor din aplicație efectuată de către Curtea de Conturi a Republicii Moldova

Aplicația DMFAS dispune de suficiente controale integrate care verifică în mod automat dacă introducerea datelor s-a efectuat cu acuratețe. Există, totuși, anumite aspecte care generează motive de îngrijorare și necesită soluționare: operatorii pot introduce date în clasificatorii sistemului și în alte tabele ale sistemului, ceea ce poate afecta acuratețea și integritatea datelor prin duplicarea sau ștergerea înregistrărilor.

Recomandarea nr. 15: Se vor revizui drepturile operatorilor de a introduce, modifica sau șterge date în clasificatorul bazei de date DMFAS sau se vor identifica operațiuni de acest gen având ca rezultat duplicarea datelor sau intrări eronate de date.

Pe lângă rapoartele standard implementate în aplicația DMFAS, un număr semnificativ de rapoarte generice a fost dezvoltat în Excel, incluzând cele mai multe dintre aspectele necesare. Nu toate tipurile de rapoarte sunt utilizate sistematic. Majoritatea rapoartelor necesare sunt generate în Excel. Totuși, există anumite rapoarte generate manual pe baza unor date obținute din alte rapoarte. De interes în acest sens este reînnoirea datelor în rapoarte generate în Excel. Generarea rapoartelor reprezintă o procedură complicată, care ar putea fi drastic afectată de erori umane. De asemenea, rapoartele generate ar putea fi modificate fără autorizație, iar asemenea erori se pot produce în alte rapoarte centralizatoare importante, care ar trebui să beneficieze de securizare maximă și să reprezinte activitatea principală a Diviziei Generale privind Datoria Publică.

Drept urmare, anumite deficiențe minore ar putea afecta în mod decisiv credibilitatea și acuratețea datelor din rapoarte importante privind activitatea Diviziei Generale privind Datoria Publică.

Recomandarea nr. 16: Se vor lua în considerare optimizarea sau automatizarea procesului de modificare a rapoartelor ce urmează a fi generate. Se va identifica o modalitate de generare automată a rapoartelor centralizatoare, eliminând posibilitatea producerii erorilor umane. Se va lua în considerare migrarea către versiunea 6.0.

BIBLIOGRAFIE

Organizația Asiatică a Instituțiilor Supreme de Audit. Proiect de cercetare. *IT Audit Guidelines – 6th Edition (Ghiduri privind Auditul IT – a 6-a ediție)*. Septembrie 2003

Gallegos, Frederick, Sandra Senft, Daniel P. Manson și Carol Gonzales. *Information Technology Control and Audit. (Controlul și Auditul Tehnologiei Informației)* Auerbach Publications. SUA, 2004

Oficiul Indian al Controlerului și al Auditorului General. *Information Technology Audit – General Principles (IT Audit Monograph Series # 1) (Auditul Tehnologiei Informației – Principii Generale (Seria Monografică nr. 1 privind Auditul IT))*.

Fondul Monetar Internațional și Banca Mondială. *Ghiduri privind Administrarea Datoriei Publice*. 1 aprilie 2014

Organizația Internațională a Instituțiilor Supreme de Audit. *ISSAI 300 – Principiile Auditului Performanței*. Septembrie 2019.

Organizația Internațională a Instituțiilor Supreme de Audit. *ISSAI 3000 – Standardul Auditului Performanței*. Septembrie 2019

Inițiativa de Dezvoltare a INTOSAI. WGITA, *IDI Handbook on IT Audit for Supreme Audit Institutions (Manual IDI privind Auditul IT, destinat Instituțiilor Supreme de Audit)*. Februarie 2014.

Parker, Xenia Ley. *Information Technology Audits (Auditurile Tehnologiei Informației)*. CCH Incorporated. SUA 2006.

Site-ul web al Departamentului de Securitate Internă al Statelor Unite web site:
<http://www.dhs.gov>.

Biroul pentru Responsabilitate Guvernamentală al Statelor Unite. *Federal Information System Controls Audit Manual (FISCAM) (Manual de Audit al Controalelor Sistemului Informatic Federal)*. GAO-09-232G. Februarie 2009.