REGULI SI PROCEDURI PRIVIND GESTIONAREA RISCURILOR

Număr cod intern: P – 02, ed.1, rev.16
Număr cod ASF: 0002

Exemplarul nr. _
☐ Exemplar controlat
☐ Exemplar necontrolat

APROBAT - Director General – Adrian SIMIONESCU

REVIZUIT - Ofiţer Conformitate – Andi BRĂDICEANU

Data intrării în vigoare: 01.04.2019

LISTA DE CONTROL A REVIZIILOR

Identificarea documentului:

1	Denumire	***REGULI SI PROCEDURI privind gestionarea riscurilor***
2	Cod	***P – 02***
3	Ediţie	***1***
4	Revizie	***16***

Identificarea reviziei:

Nr. ediţie/ revizie	Dată revizie	Pagini revizuite	Revizuit de :	Aprobat de :	Conţinutul reviziei
1/15	19.04.2018	33	Miu Mihaela	Adrian Simionescu	Revizie periodică: - introducere Listă de control a reviziilor; - revizuire conţinut.
1/16	26.02.2019	integral	Brădiceanu Andi	Adrian Simionescu	Revizie periodică: - redenumire procedură; - actualizare reglementări incidente; - revizuire conţinut Procedură.

1. SCOP

Procedura stabileşte regulile și procedurile privind identificarea, evaluarea, monitorizarea, gestionarea și raportarea riscurilor ce pot avea un impact negativ asupra situaţiei financiare, patrimoniale şi/ sau reputaţionale ale S.S.I.F. Vienna Investment Trust S.A..

2. DOMENIU DE APLICARE

Procedura este aplicabilă întregului personal implicat în procesul de identificare, evaluare, monitorizare, gestionare și raportare a riscurilor.

3. DOCUMENTE DE REFERINŢĂ

Legea nr.126/2018 privind pieţele de instrumente financiare (**Legea nr.126/2018**)
Regulamentul A.S.F. nr.3/2014 privind unele aspecte legate de aplicarea Ordonanței de urgență a Guvernului nr. 99/2006 privind instituţiile de credit şi adecvarea capitalului și a Regulamentului (UE) nr.575/2013 al Parlamentului European şi al Consiliului din 26 iunie 2013 privind cerinţele prudenţiale pentru instituţiile de credit şi firmele de investiţii şi de modificare a Regulamentului (UE) nr.648/2012, cu modificările şi completările ulterioare (**Regulamentul nr.3/2014**)
Regulamentul A.S.F. nr.1/2019 privind evaluarea şi aprobarea membrilor structurii de conducere şi a persoanelor care deţin funcţii-cheie în cadrul entităţilor reglementate de A.S.F. (**Regulamentul nr.1/2019**)
Norma nr.4/2018 privind gestionarea riscurilor operaționale generate de sistemele informatice utilizate de entitățile autorizate/avizate/înregistrate și/sau supravegheate de A.S.F., cu modificările şi completările ulterioare (**Norma nr.4/2018**)
Regulamentul (UE) nr.575/2013 al Parlamentului European şi al Consiliului privind cerinţele prudenţiale pentru instituţiile de credit şi societăţile de investiţii şi de modificare a Regulamentului (UE) nr.648/2012, cu modificările şi completările ulterioare (**Regulamentul UE 575/2013**)
Regulamentul (UE) nr. 648/2012 al Parlamentului European şi al Consiliului privind instrumentele financiare derivate extrabursiere, contrapărţile centrale şi registrele centrale de tranzacţii (EMIR), cu modificările şi completările ulterioare (**Regulamentul UE nr.648/2012**)
Directiva 2014/65/UE a Parlamentului European și a Consiliului din 15 mai 2014 privind piețele instrumentelor financiare și de modificare a Directivei 2002/92/CE și a Directivei 2011/61/UE (MiFID II)
Regulamentul (UE) nr. 600/2014 al Parlamentului European și al Consiliului din 15 mai 2014 privind piețele instrumentelor financiare și de modificare a Regulamentului (UE) nr. 648/2012, cu modificările şi completările ulterioare (MiFIR)
Regulamentul A.S.F. nr.2/2016 privind aplicarea principiilor de guvernanţă corporativă de către entităţile autorizate, reglementate şi supravegheate de A.S.F. (**Regulamentul nr.2/2006**)
Acte normative aplicabile, în vigoare.

4. DEFINIŢII. ABREVIERI

4.1 Definiții

Definiţiile termenilor utilizaţi sunt preluate din actele normative aplicabile.
Organ de conducere - organul sau organele de administrare şi de conducere ale unei firme de investiţii, ale unui operator de piaţă sau ale unui furnizor de servicii de raportare a datelor, care sunt numite în conformitate cu prevederile Legii societăţilor nr. 31/1990, republicată, cu modificările şi completările ulterioare, abilitate să stabilească strategia, obiectivele şi direcţia generală a entităţii, care supervizează şi monitorizează procesul decizional şi din care fac parte şi persoanele care conduc efectiv activitatea entităţii;
Organ de conducere în funcţia sa de supraveghere - organul de conducere al unei firme de investiţii care îşi îndeplineşte rolul de supraveghere şi monitorizare a procesului decizional de conducere şi care este reprezentat de consiliul de administraţie, în cadrul sistemului unitar de administrare, şi de consiliul de supraveghere, în cadrul sistemului dualist de administrare;
Conducere executivă/conducere superioară – persoane care, potrivit actelor constitutive şi/sau hotărârii structurilor statutare ale entității reglementate, sunt împuternicite să conducă şi să coordoneze activitatea curentă a acesteia şi au competența de a angaja răspunderea societăţii, respectiv, directorii, în cazul administrării în sistem unitar sau directoratul, în cazul administrării în sistem dualist; nu se includ în această categorie persoanele care asigură conducerea nemijlocită a compartimentelor și a sediilor secundare din cadrul entității reglementate;

Conducere superioară - persoanele fizice care exercită funcţii executive în cadrul unei firme de investiţii, al unui operator de piaţă sau al unui furnizor de servicii de raportare a datelor şi care răspund în faţa organului de conducere pentru managementul activităţilor curente ale entităţii, inclusiv pentru implementarea politicilor privind distribuţia de servicii şi produse clienţilor de către entitate şi personalul acesteia;
Profil de risc - suma expunerilor unei S.S.I.F. la riscuri reale şi potenţiale;
Apetit la risc - nivelul absolut al riscurilor pe care o S.S.I.F. este pregătită să şi-l asume în mod aprioric;
Proces intern de evaluare a adecvării capitalului la riscuri - componentă a cadrului de administrare a activităţii S.S.I.F, care vizează ca organul de conducere al acestora să asigure identificarea, măsurarea, agregarea şi monitorizarea în mod adecvat a riscurilor S.S.I.F, deţinerea unui capital intern adecvat la profilul de risc şi utilizarea şi dezvoltarea unor sisteme solide de administrare a riscurilor;
Risc reputaţional - riscul actual sau viitor de afectare negativă a profiturilor şi capitalului determinat de percepţia nefavorabilă asupra imaginii unei S.S.I.F de către clienţi, contrapartide, acţionari, investitori sau autorităţi de supraveghere;
Risc strategic - riscul actual sau viitor de afectare negativă a profiturilor şi capitalului determinat de schimbări în mediul de afaceri sau de decizii de afaceri defavorabile, de implementarea inadecvată a deciziilor sau de lipsa de reacţie la schimbările din mediul de afaceri;
Risc operațional - riscul de pierdere care rezultă fie din utilizarea unor procese, persoane sau sisteme interne inadecvate sau care nu și-au îndeplinit funcția în mod corespunzător, fie din evenimente externe, și care include riscul juridic;
Risc aferent tehnologiei informaţiei (IT) - subcategorie a riscului operaţional care se referă la riscul actual sau viitor de afectare negativă a profiturilor şi capitalului, determinat de inadecvarea strategiei şi politicii IT, a tehnologiei informaţiei şi a procesării informaţiei, cu referire la capacitatea de gestionare, integritatea, controlabilitatea şi continuitatea acesteia sau de utilizarea necorespunzătoare a tehnologiei informaţiei;
Riscuri semnificative - riscuri cu impact însemnat asupra situaţiei financiare, patrimoniale şi/sau reputaţionale ale S.S.I.F.;
Risc de piaţă - riscul de a înregistra pierderi aferente poziţiilor din bilanţ şi din afara bilanţului datorită fluctuaţiilor nefavorabile pe piaţă ale preţurilor (cum ar fi, de exemplu, preţurile acţiunilor, ratele de dobândă, cursurile de schimb valutar);
Risc de credit - riscul actual sau viitor de afectare negativă a profiturilor şi capitalului ca urmare a neîndeplinirii de către debitor a obligaţiilor contractuale sau a eşecului acestuia în îndeplinirea celor stabilite;
Risc de lichiditate - riscul actual sau viitor de afectare negativă a profiturilor şi capitalului, determinat de incapacitatea S.S.I.F de a-şi îndeplini obligaţiile la scadenţa acestora;
Risc sistemic - riscul de afectare a unei zone importante a sistemului financiar sau a unei pieţe financiare, cu potenţial de consecinţe negative serioase pentru piaţa internă şi economia reală, instabilitate a sistemului financiar, posibil catastrofică, cauzată sau accentuată de evenimente idiosincratice sau de condiţii ale entităţilor;
Analiză de risc - analiza scenariilor de ameninţări semnificative, pentru a evalua probabilitatea materializării acestora şi impactul potenţial pe care un astfel de eveniment l-ar avea asupra entităţii şi operaţiunilor acesteia;
Atac etic/test de penetrare - test al sistemelor informatice realizat printr-o simulare a unui atac real asupra reţelelor, sistemelor şi programelor informatice utilizate de entitatea testată sau auditată, după caz;
Bază de date – structură de organizare a informaţiei în unul sau mai multe domenii de aplicare, cu scopul de a o face accesibilă în permanenţă către utilizatori prin ansamblul de programe informatice;
Centru de date - spaţiu securizat, dotat cu tehnică de calcul şi echipamente de comunicaţii prin intermediul cărora se primesc, se stochează şi se transmit date în formă electronică, care se implementează respectând standardele specifice, utilizând conceptul de nivel sau un echivalent al acestuia, precum, dar fără a se limita la, standardele SR EN 50600 (European Standard - Data Centers Facilities and Infrastructures) sau TIA-942 (Telecommunications Industry Association);
Date (informatice) - orice reprezentare a unor fapte, informaţii sau concepte într-o formă care poate fi prelucrată printr-un sistem informatic, incluzându-se şi orice program informatic care poate determina realizarea unei funcţii similare de către un sistem informatic;
Vulnerabilități - stări de fapt, procese şi/sau fenomene care diminuează capacitatea de reacţie a sistemelor informatice la riscurile existente ori potenţiale sau care favorizează apariţia şi dezvoltarea lor, cu consecinţe în planul funcţionalităţii şi utilităţii.

4.2 Abrevieri

A.S.F. – Autoritatea de Supraveghere Financiară
S.S.I.F. – Societate de Servicii de Investiții Financiare

5. PROCEDURA

5.1. Atribuţiile structurilor organizatorice cu privire la activităţile specifice administrării riscurilor

Art.1.(1). Departamentul de Administrare Riscuri (Risk Management), împreună cu Compartimentul de Conformitate, Auditul Intern, Comitetul de Audit şi Comitetul de risc, se asigură că toate activităţile desafăşurate în cadrul S.S.I.F. Vienna Investment Trust S.A. respectă cadrul legal aplicabil şi procedurile, politicile şi regulile interne.

(2) Activitatea de administrare a riscurilor reprezintă suma activităţilor desfăşurate şi a rezultatelor tuturor structurilor organizatorice ale S.S.I.F. Vienna Investment Trust S.A..

(3) Activitatea de administrare a riscurilor este realizată la nivelul tuturor structurilor organizatorice cu atribuţii de control, de analiză a procedurilor şi a cadrului legislativ aplicabil, de monitorizare a proceselor şi de prevenire a producerii de evenimente cu impact negativ.-

Art.2.(1) În vederea administrării eficiente a riscurilor, la nivelul societăţii sunt implementate trei nivele:

i) Nivelul I: identificarea şi evaluarea riscurilor se realizează la nivelul fiecărei structuri organizatorice, pe baza procedurilor operaţionale. La nivelul fiecărei structuri organizatorice sunt desemnaţi responsabili cu identificarea şi evaluarea riscurilor operaţionale. Persoanele desemnate sunt comunicate Departamentului de Administrare Riscuri (Risk Management). Activităţi specifice nivelului I: identificarea şi gestionarea riscurilor utilizând instrumente de gestiune a riscului operaţional; evaluarea şi îmbunătăţirea continuă a controalelor şi alertelor; monitorizarea şi raportarea profilului de risc operaţional, asigurându-se că profilul de risc operaţional respectă apetitul de risc stabilit, precum şi nivelul de toleranţă.

ii) Nivelul II: identificarea, analiza şi monitorizarea riscurilor se realizează de către responsabilul cu administrarea riscului din cadrul Departamentului de Administrare Riscuri. Această activitate foloseşte atât informaţiile provenite de la structurile organizatorice, cât şi cele obţinute din activitatea de monitorizare şi analiză. Departamentul de Administrare Riscuri dezvoltă şi implementează politici, proceduri, propune măsuri şi instrumente de gestionare a riscurilor şi se asigură că se urmăreşte identificarea riscurilor, stabilirea şi, dacă este cazul, testarea metodelor de evaluare ale acestora, monitorizarea şi raportarea riscurilor. Activităţi specifice nivelului II: proiectarea unor instrumente operaţionale de administrare a riscurilor în vederea identificării şi administrării riscurilor; simularea unor situaţii de atac real; utilizarea instrumentelor de administrare a riscului operaţional; dezvoltarea şi menţinerea unor proceduri adecvate în vederea monitorizării şi raportării profilului de risc operaţional; instruirea personalului cu privire la riscurile operaţionale.

iii) Nivelul III: evaluarea riscurilor realizată de auditul intern, auditul extern (financiar / IT) şi Compartimentul de Conformitate. Nivelul III se asigură, de fapt, că procesele aferente nivelelor I şi II operează efectiv. În acest sens, auditul intern, auditul extern şi/sau Compartimentul de Conformitate realizează evaluarea independentă a procedurilor interne, confirmă gradul de conformitate a acestora cu normele aplicabile şi formulează recomandări privind îmbunătăţirea proceselor şi remedierea deficienţelor. Activităţi specifice: verificarea în mod independent că regulile şi procedurile de administrare a riscului sunt suficient de bine concepute şi puse în aplicare; revizuirea scenariilor de simulare a unor situaţii de atac real; revizuirea proceselor de monitorizare, raportare şi guvernanţă; controale cu privire la activitatea agenţilor pentru servicii de investiţii financiare, verificări periodice cu clienţii pentru confirmarea activităţii, verificări inopinate cu clienţii în legătură cu tranzacţii de valori mari.

(2) Cele 3 nivele menţionate la alin. (1) furnizează, individual sau prin cooperarea cu administratorul de risc, informaţii şi rapoarte către conducerea executivă şi către Consiliul de Administraţie, pentru a le permite monitorizarea eficientă a activităţii societăţii.-

Art.3. Consiliul de Administraţie al S.S.I.F. Vienna Investment Trust S.A. aprobă prezentele reguli şi proceduri privind identificarea, evaluarea, monitorizarea, gestionarea și raportarea riscurilor, inclusiv modificările acestora, decide cu privire la măsurile necesare diminuării impactului potenţial negativ, analizează adecvarea, eficienţa şi actualizarea sistemului de administrare a riscurilor în vederea gestionării eficiente a activelor, precum şi a modului de administrare a riscurilor şi stabileşte profilul de risc al societăţii, stabilind apetitul şi limitele de toleranţă pentru fiecare categorie de risc. Limitele de toleranţă sunt supuse analizării şi revizuirii anual şi ori de câte ori este necesar.-

Art.4.(1) Departamentul de Administrare Riscuri este structura cu rol în colectarea şi analiza datelor şi informaţiilor privind riscurile ce pot afecta negativ patrimoniul sau reputaţia S.S.I.F. Vienna Investment Trust S.A.

(2) Atribuţiile Departamentului de Administrare Riscuri:

i) monitorizarea şi evaluarea impactului modificărilor legislative şi a deciziilor organului de conducere;

ii) monitorizarea nivelului riscurilor şi a limitelor acestora – Comitetul de risc, pe baza propunerilor Departamentului de Administrare a Riscului şi împreună cu acesta, recomandă revizuirea limitelor de toleranţă, dacă este cazul, cel puţin anual. Monitorizarea limitelor stabilite pentru adecvarea capitalului se realizează permanent de către Departamentul Financiar-Contabil împreună cu Departamentul de Administrare Riscuri. Monitorizarea riscurilor curente şi a celor potenţiale se realizează pe baza rapoartelor şi informaţiilor furnizate de către departamentele operaţionale. Departamentul de Administrare Riscuri, împreună cu departamentele operaţionale, identifică şi evaluează periodic riscurile asociate activităţilor operaţionale şi propun măsuri de diminuare şi control. Propunerile sunt prezentate organului de conducere al societăţii şi Comitetului de Risc;

iii) implementarea regulilor şi procedurilor privind gestionarea riscurilor – Departamentul de Administrare riscuri, împreună cu departamentele operaţionale şi Compartimentul de Conformitate, stabileşte modalităţile de revizuire şi testare a procedurilor de administrare a riscurilor. În cazul în care se impune actualizarea conţinutului acestor proceduri ca urmare a unor modificări legislative, operaţionale, organizatorice, monitorizarea procesului de actualizare şi modificare va fi realizată de către Compartimentul de Conformitate, în colaborare cu Departamentul Administrare Riscuri. În vederea evaluării şi testării eficienţei procedurilor interne, se vor avea în vedere rapoartele şi constatările Compartimentului de Conformitate şi Auditului Intern;

iv) actualizarea Planului de Continuitate Operaţională – la nivelul societăţii este implementat un Plan de Asigurare a Continuităţii şi un Plan de recuperare a datelor în caz de dezastru. Aceste planuri se vor revizui ori de câte ori apar modificări în structura organizaţională ori în sistemele utilizate în cadrul S.S.I.F. Vienna Investment Trust S.A. Administratorul de risc, împreună cu toate departamentele operaţionale, identifică funcţiile şi activităţile importante pentru asigurarea funcţionării minimului de operaţiuni pentru clienţi. Eficacitatea planului de asigurare a continuităţii şi a planului de recuperare în caz de dezastru se analizează pe baza rezultatelor testelor anuale realizate la nivel intern, sub coordonarea Departamentului IT;

v) participarea la adoptarea măsurilor de control al riscurilor – Administratorul de Risc poate participa la şedinţele Consiliului de Administraţie în vederea abordării unor problematici specifice acestui departament şi atunci când adresează, împreună cu Comitetul de Risc sau alte comitete, recomandări Consiliului de Administraţie cu privire la măsurile care pot influenţa gestionarea riscurilor. De asemenea, participă activ la adoptarea măsurilor de management al situaţiilor de criză. Administratorul de risc poate participa, de asemenea, la şedinţele Consiliului de Administraţie în care se analizează rapoartele privind administrarea riscurilor sau alte evenimente şi situaţii cu posibil impact negativ asupra societăţii şi, în măsura în care este necesar, vor putea participa şi directorii departamentelor operaţionale implicate şi/sau afectate;

vi) raportarea – Administratorul de Risc întocmeşte analize, rapoarte şi recomandări, astfel:

a. Raportează conducerii executive şi Consiliului de Administraţie, trimestrial şi ori de câte ori este necesar, despre aplicarea regulilor şi procedurilor privind identificarea, evaluarea, monitorizarea, gestionarea și raportarea riscurilor, din proprie initiaţivă sau la solicitarea Consiliului de Administraţie sau a conducerii executive;

b. Raportează semestrial Consiliului de Administraţie şi conducerii executive în vederea analizării şi evaluării eficienţei sistemului de management al riscurilor în funcţie de politicile, procedurile și controalele efectuate.

c. Raporteaza imediat Directorului general, precum şi Comitetului de Risc şi/sau Consiliului de Administraţie, dacă este cazul, identificarea unor nereguli şi/sau posibile prejudicii, precum şi a unor situaţii cu posibil impact semnificativ asupra societăţii;
d. Realizează analize cu privire la impactul pe care îl poate avea implementarea unor măsuri, procese, reguli şi le aduce la cunoştinţa Conducerii executive, a directorilor departamentelor implicate/afectate, precum şi a Comitetului de Risc / Consiliului de Administraţie, după caz.

vii) să monitorizeze, împreună cu persoana numită în funţia de conformitate, încadrarea în suma maximă admisă în situaţia alimentării de către societate a contului de disponibilităţi al clienţilor cu sume proprii necesare pentru finalizarea tranzacţiilor aflate în decontare, precum şi demersurile efectuate de S.S.I.F. pentru recuperarea debitelor; suma maximă admisă nu poate depăşi valoarea activelor lichide aparţinând clientului pentru care S.S.I.F. a acoperit necesarul de decontare, aflate în custodia societăţii.

(3) Rapoartele şi analizele întocmite în cadrul Departamentului de Administrare Riscuri vor cuprinde cel puţin următoarele informaţii: perioada la care se referă raportul/analiza, tipul riscurilor analizate, identificate şi/sau monitorizate, impactul potenţial al respectivelor riscuri asupra activităţilor curente sau viitoare (a unui departament, funcţie etc.), contribuţia unui alt departament operaţional, dacă este necesar, măsurile propuse pentru remedierea situaţiei identificate sau pentru preîntâmpinarea producerii unor evenimente cu impact negativ asupra patrimoniului societăţii.-

Art.5.(1) Administratorul de risc va monitoriza, de asemenea, riscurile operaţionale ce decurg din eventualele erori de tranzacţionare. În astfel de situaţii, se vor propune conducătorilor măsuri de remediere a situaţiei.
(2) Funcţia de administrare a riscurilor raportează conducerii executive/conducerii superioare riscurile identificate ca fiind potențial semnificative în conformitate cu prezentele reguli şi proceduri.
(3) Funcţia de administrare a riscurilor va raporta cu privire la zonele de risc identificate atât din proprie iniţiativă, cât şi la cererea consiliului sau a conducerii executive/conducerii superioare.
(4) Riscurile operaţionale din cadrul tranzacţiilor electronice vor fi gestionate prin măsuri adecvate şi proporţionale de guvernanţă, controale interne şi sisteme interne de raportare, luând în considerare, după caz, Orientările Autorităţii bancare europene (ABE) privind gestionarea riscurilor operaţionale în activităţi de piaţă.-

Art.6. Departamentul Back-Office monitorizează continuu corectitudinea înregistrării tranzacţiilor, depunând toate eforturile pentru a remedia orice inadvertenţă apărută. Astfel, departamentul va efectua:

- Verificarea corectitudinii tranzacţiilor efectuate prin confruntarea evidenţelor societăţii, respectiv ordinele iniţiale cu documentele primite din partea instituţiilor abilitate pentru tranzacţiile executate;
- Urmărirea corelării dintre evidenţa contului (portofoliului) SSIF la Depozitarul Central şi înregistrările în softul de evidenţă şi gestionarea a instrumentelor financiare;
- Verificarea corectitudinii transferurilor de instrumente financiare efectuate prin confruntarea evidenţelor societăţii cu documentele primite de la Depozitarul Central;
- Corelarea armonizării decontărilor şi compensărilor zilnice cu instituţiile de decontare.-

5.2. Cerinţe prudenţiale

Art.7.(1) S.S.I.F. va raporta în scopuri de supraveghere, Autorității de Supraveghere Financiare, următoarele:

a) cerințele de fonduri proprii și informațiile financiare, în conformitate cu art.99 din Regulamentul (UE) nr.575/2013;
b) pierderile care decurg din împrumuturi garantate cu bunuri imobile, în conformitate cu art.101 alin.(4) lit.(a) din Regulamentul (UE) nr.575/2013;
c) expunerile mari și alte cele mai mari expuneri, în conformitate cu art.394 alin.(1) din Regulamentul (UE) nr.575/2013;
d) indicatorul efectului de levier, în conformitate cu art.430 din Regulamentul (UE) nr.575/2013;
e) cerințele de acoperire a necesarului de lichiditate și cerințe de finanțare stabilă netă, în conformitate cu art.415 din Regulamentul (UE) nr.575/2013;
f) grevarea cu sarcini a activelor, în conformitate cu articolul 100 din Regulamentul (UE) nr. 575/2013.

Societatea a desemnat o persoană din cadrul Departamentului Financiar-Contabil responsabilă cu întocmirea acestor raportări. De asemenea o persoană din cadrul compartimentului de Conformitate este desemnată responsabilă cu identificarea, monitorizarea și administrarea riscurilor.
(2) S.S.I.F. transmite raportări către A.S.F. respectând următoarele datele de referință:

a) raportare lunară: ultima zi a fiecărei luni;
b) raportare trimestrială: 31 martie, 30 iunie, 30 septembrie și 31 decembrie;
c) raportare bianuală: 30 iunie și 31 decembrie;
d) raportare anuală: 31 decembrie.

(3) S.S.I.F. transmite raportări către A.S.F. până la sfârșitul programului de lucru, la următoarele date de transmitere:

a) raportare lunară: a 15-a zi calendaristică de la data de referință a raportării;
b) raportare trimestrială: 12 mai, 11 august, 11 noiembrie și 11 februarie;
c) raportare bianuală: 11 august și 11 februarie;
d) raportare anuală: 11 februarie.

(4) În cazul în care data de transmitere a raportărilor este o sărbătoare legală sau o zi de sâmbătă ori de duminică, informațiile sunt transmise în ziua lucrătoare următoare.
(5) S.S.I.F. transmite fără întârziere către A.S.F. orice alte corecții ale rapoartelor prezentate.-

Art.8. Informațiile cu privire la cerința de acoperire a necesarului de lichiditate, conform art.15 din Regulamentul (UE) nr.680/2014, se vor raporta către A.S.F. cu o frecvență lunară, data de transmitere fiind a 15-a zi calendaristică de la data de referință a raportării.-

Art.9.(1) Informațiile privind fondurile proprii și cerințele de fonduri proprii, în conformitate cu art.5 din Reglamentul (UE) nr. 680/2014 se vor raporta către A.S.F. cu o frecvență trimestrială, la datele de transmitere prevăzute la art.7, alin.(3) lit.b) și cu o frecvență bianuală, la datele de transmitere prevăzute la art.7, alin.(3) lit.c).
(2) În conformitate cu art.99 din Regulamentul (UE) nr. 575/2013, S.S.I.F. prezintă următoarele informații cu o frecvență trimestrială:

1. informațiile privind toate expunerile din securitizări, astfel cum se specifică în formularul 14 din anexa I, în conformitate cu instrucțiunile de la punctul 3.9 partea II din anexa II;
2. informațiile privind expunerile la riscul de credit și la riscul de credit al contrapărții care sunt tratate în conformitate cu abordarea standardizată, astfel cum se specifică în formularul 7 din anexa I, în conformitate cu instrucțiunile din partea II punctul 3.2 din anexa II;
3. informațiile privind expunerile la riscul de credit și la riscul de credit al contrapărții care sunt tratate în conformitate cu abordarea pe baza ratingurilor interne, astfel cum se specifică în formularul 8 din anexa I, în conformitate cu instrucțiunile din partea II punctul 3.3, anexa II;
4. informațiile privind distribuția geografică a expunerilor pe țări, astfel cum se specifică în formularul 9 din anexa I, în conformitate cu instrucțiunile din partea II punctul 3.4 din anexa II, în cazul în care expunerile inițiale altele decât expunerile interne din toate celelalte țări „altele decât țara proprie” în toate clasele de expuneri, astfel cum sunt raportate în rândul 850 din formularul 4 din anexa I, sunt egale sau mai mari de 10 % din totalul expunerilor inițiale, atât interne, cât și altele decât interne, astfel cum sunt raportate în rândul 860 din formularul 4 din anexa I. În acest scop, expunerile sunt considerate a fi interne atunci când reprezintă expuneri față de contrapărți situate în statul membru în care este situată instituția. Se aplică criteriile de intrare și de ieșire prevăzute la articolul 4;
5. informațiile privind expunerile provenind din titluri de capital care sunt tratate în conformitate cu abordarea pe baza ratingurilor interne, astfel cum se specifică în formularul 10 din anexa I, în conformitate cu instrucțiunile din partea II punctul 3.5 din anexa II;
6. informațiile privind riscul de decontare, astfel cum se specifică în formularul 11 din anexa I, în conformitate cu instrucțiunile din partea II punctul 3.6 din anexa II;
7. informațiile privind expunerile din securitizări care sunt tratate în conformitate cu abordarea standardizată, astfel cum se specifică în formularul 12 din anexa I, în conformitate cu instrucțiunile din partea II punctul 3.7 din anexa II;
8. informațiile privind expunerile din securitizări care sunt tratate în conformitate cu abordarea pe baza ratingurilor interne, astfel cum se specifică în formularul 13 din anexa I, în conformitate cu instrucțiunile din partea II punctul 3.8 din anexa II;

9. informațiile privind cerințele de fonduri proprii și pierderile legate de riscurile operaționale, astfel cum se specifică în formularul 16 din anexa I, în conformitate cu instrucțiunile din partea II punctul 4.1 din anexa II;
10. informațiile privind cerințele de fonduri proprii legate de riscul de piață, astfel cum se specifică în formularele 18-24 din anexa I, în conformitate cu instrucțiunile din partea II punctele 5.1-5.7 din anexa II;
11. informațiile privind cerințele de fonduri proprii legate de riscul de ajustare a evaluării creditului, astfel cum se specifică în formularul 25 din anexa I, în conformitate cu instrucțiunile din partea II punctul 5.8 din anexa II.

(3) În conformitate cu art.99 din Regulamentul (UE) nr. 575/2013, S.S.I.F. prezintă următoarele informații cu o frecvență bianuală:

1. informațiile privind expunerile din securitizări, astfel cum se specifică în formularul 14 din anexa I, în conformitate cu instrucțiunile din partea II punctul 3.9 din anexa II;
2. informațiile privind pierderile materiale legate de riscurile operaționale, în următorul mod:
    a) instituțiile care calculează cerințele de fonduri proprii legate de riscurile operaționale în conformitate cu partea a 3-a titlul III capitolul 3 sau capitolul 4 din Regulamentul (UE) nr. 575/2013 raportează aceste informații astfel cum se specifică în formularul 17 din anexa I, în conformitate cu instrucțiunile din partea II punctul 4.2 din anexa II;
    b) instituțiile care calculează cerințele de fonduri proprii legate de riscurile operaționale în conformitate cu partea a 3-a titlul III capitolul 3 din Regulamentul (UE) nr. 575/2013 și pentru care totalul bilanțului individual reprezintă o pondere mai mică de 1 % din suma totalurilor bilanțurilor individuale ale tuturor instituțiilor din același stat membru pot raporta numai informațiile specificate în formularul 17 din anexa I, în conformitate cu instrucțiunile de la punctul 124 din partea II din anexa II. Totalul cifrelor din bilanț se bazează pe cifrele de la sfârșitul exercițiului pentru anul anterior anului care precedă data de referință de raportare. Se aplică criteriile de intrare și de ieșire prevăzute la articolul 4;
    c) instituțiile care calculează cerințele de fonduri proprii legate de riscurile operaționale în conformitate cu partea a 3-a titlul III capitolul 2 din Regulamentul (UE) nr. 575/2013 sunt pe deplin exceptate de la obligația de a raporta informațiile menționate în formularul 17 din anexa I și la punctul 4.2 din partea II din anexa II.-

Art.10. Informațiile privind expunerile mari, în conformitate cu art.13 din Reglamentul (UE) nr. 680/2014 se vor raporta către A.S.F. cu o frecvență trimestrială, la datele de transmitere prevăzute la art.7, alin.(3) lit.b).-

Art.11. Informațiile privind indicatorul efectului de levier, în conformitate cu art.14 din Regulamentul (UE) nr.680/2014 se vor raporta către A.S.F. cu o frecvență trimestrială, la datele de transmitere prevăzute la art.7, alin.(3) lit.b).-

Art.12.(1) Societatea raportează Autorității de Supraveghere Financiară informațiile prevăzute la art.7-11 precum şi orice element component aferent acestora solicitat de autoritatea competentă.
(2) Conform prevederilor art.104 alin.(1), lit.j) din Directiva UE nr.36/2013, A.S.F. poate impune S.S.I.F. cerințe de raportare suplimentare sau cu o frecvență mai mare a raportării, inclusiv raportarea privind situația fondurilor proprii și a cerințelor de fonduri proprii.
(3) În situația în care A.S.F. va decide cerințe suplimentare sau o frecvență mai mare a raportărilor privind cerințele prudențiale, acest lucru va fi adus la cunoștința S.S.I.F.
(4) Societatea va informa autorităţile competente cu privire la riscurile semnificative care pot afecta tranzacţionarea corectă şi ordonată, precum şi incidentele majore, în cazul materializării acestor riscuri.-
Art.13.(1) Funcţia de administrare a riscurilor se asigură că toate riscurile semnificative sunt identificate, măsurate şi raportate în mod corespunzător.
(2) Funcţia de administrare a riscurilor se implică în mod activ la elaborarea strategiei S.S.I.F. privind administrarea riscurilor şi în toate deciziile privind administrarea riscurilor semnificative.
(3) În cazul în care este necesar, funcţia de administrare a riscurilor trebuie să poată raporta direct organului de conducere, în funcţia sa de supraveghere, independent de raportarea către conducerea superioară, să poată face sesizări şi să poată avertiza acest organ, atunci când este cazul, dacă au loc

evoluţii specifice ale riscurilor care afectează sau ar putea să afecteze instituţia, fără a aduce atingere responsabilităţilor pe care le are organul de conducere în funcţiile sale de supraveghere şi/sau de conducere în conformitate cu prevederile Ordonanţei de urgenţă a Guvernului nr. 99/2006, aprobată cu modificări şi completări prin Legea nr. 227/2007, cu modificările şi completările ulterioare, Regulamentului A.S.F. nr.3/2014, cu modificările și completările ulterioare, şi Regulamentului (UE) nr. 575/2013.
(4) Coordonatorul funcţiei de administrare a riscurilor trebuie să fie un membru independent al conducerii superioare, cu responsabilităţi distincte privind funcţia de administrare a riscurilor. În cazul în care natura, extinderea şi complexitatea activităţilor S.S.I.F. nu justifică numirea unei persoane distincte, o altă persoană dintre membrii conducerii superioare din cadrul S.S.I.F. poate îndeplini funcţia respectivă, cu condiţia să nu existe niciun conflict de interese.
(5) Coordonatorul funcţiei de administrare a riscurilor nu poate fi demis fără aprobarea prealabilă a organului de conducere în funcţia sa de supraveghere şi trebuie să poată avea acces direct la organul de conducere, în funcţia sa de supraveghere, atunci când este necesar.
(6) Coordonatorul funcţiei de administrare a riscurilor raportează în mod direct conducerii executive/conducerii superioare riscurile identificate ca fiind potenţial semnificative, în conformitate cu prezenta procedura.
(7) Coordonatorul funcţiei de administrare a riscurilor are obligaţia să raporteze cu privire la zonele de risc specifice atât din proprie iniţiativă, cât şi la cererea consilului sau a conducerii executive/conducerii superioare.
(8) În cazul în care funcţia de administrare a riscului nu este exercitată în mod independent, iar S.S.I.F. nu se încadrează în categoria S.S.I.F. semnificative în conformitate cu prevederile art. 7 din Regulamentul nr. 3/2014, funcția de administrare a riscului poate fi exercitată de un angajat al S.S.I.F. care nu îndeplinește o funcție operațională.
(8[1]) În sensul alin. (2) și al art. 22 alin. (3) din Regulamentul nr. 3/2014, în categoria funcțiilor operaționale se includ: agentul pentru servicii de investiții financiare, agentul delegat, analistul financiar, administratorul de portofoliu, persoana responsabilă cu administrarea sancțiunilor internaționale, persoane care au responsabilități în aplicarea prevederilor legale referitoare la prevenirea și combaterea spălării banilor și a finanțării actelor de terorism (ofițer de conformitate și persoană responsabilă), precum și persoanele cu funcții de conducere și supraveghere a acestora.” .
(9) Persoana care asigură funcţia de administrare a riscului trebuie să fie autorizată de A.S.F. şi înscrisă în Registrul A.S.F., să fi participat la stagiile de pregătire şi să fi promovat testul privind cunoaşterea legislaţiei în vigoare organizat de către organismele de formare profesională atestate de A.S.F. şi să fie angajată cu contract individual de muncă şi să aibă atribuţii de administrare a riscului numai în cadrul societăţii -

5.3. Managementul riscurilor
Secţiunea 1 - Riscul de credit

Art.14.(1) Riscul de credit reprezintă riscul actual sau viitor de afectare negativă a profiturilor şi capitalului ca urmare a neîndeplinirii de către debitor a obligaţiilor contractuale sau a eşecului acestuia în îndeplinirea celor stabilite.
(2) S.S.I.F. evaluează riscul de credit al expunerilor faţă de debitori individuali, titluri de valoare sau poziţiile din securitizare, precum şi riscul de credit la nivelul portofoliului.
(3) Departamentul Back-Office verifică în permanenţă contul de marjă al clienţilor şi transmite Departamentului Front Office & Tranzacţionare atenţionări privind nerespectarea nivelului minim al acestuia, informând concomitent conducerea societăţii.
(4) S.S.I.F. gestionează şi monitorizează permanent portofoliile purtătoare de risc de credit şi diferitele expuneri ale acesteia, inclusiv pentru identificarea şi gestionarea creditelor problematice şi pentru efectuarea ajustărilor de valoare şi constituirea unor provizioane adecvate.
(5) Acordarea de credite se face pe baza unor criterii solide şi bine definite, iar procesul de aprobare, modificare, reînnoire şi refinanţare a creditelor se stabileşte cu claritate, pentru fiecare caz în parte.
(6) S.S.I.F. se asigură că diversitatea portofoliilor de credite este adecvată în funcţie de pieţele-ţintă şi strategiile globale de creditare ale instituţiei.
(7) S.S.I.F. dispune de criterii, politici şi procese solide şi bine definite privind aprobarea noilor expuneri - inclusiv standarde prudente de asumare a expunerilor, operaţiunile de modificare, reînnoire şi refinanţare a expunerilor existente şi identificarea competenţei de aprobare corespunzătoare dimensiunii şi

complexităţii expunerilor.
(8) Administratorul de risc monitorizează activitatea departamentelor de mai sus.-

Art.15. Departamentul Back-Office, împreună cu Departamentul Financiar-Contabil, monitorizează respectarea obligaţiilor tuturor debitorilor societăţii (de ex. emitenţii de obligaţiuni). Ori de câte ori se constată întârzieri în respectarea acestora, se parcurg următoarele etape:

- informarea conducătorilor;
- corespondenţă cu emitentul;
- informarea Departamentului Juridic pentru declanşarea procedurilor legale în situaţia în care rezolvarea pe care amiabilă nu a fost posibilă.-

Secţiunea 2 - Riscurile financiare

Art.16.(1) Departamentul Back-Office, împreună cu Departamentul Financiar-Contabil, vor conduce evidenţele solicitate de actele normative aplicabile privind adecvarea capitalului unei S.S.I.F. și cerințele prudențiale.
(2) Administratorul de risc va monitoriza această activitate a celor două departamente.
(3) Administratorul de risc şi persoana care îndeplineşte funcţia de conformitate vor raporta conducerii societăţii ori de câte ori se constată abateri de la prevederile legale, propunând totodată măsuri de remediere a situaţiei.
(4) Pentru evaluarea adecvării capitalului la riscuri şi administrarea riscului derivat din nivelul ridicat al valorii activelor clienţilor deţinute în custodie, administratorul de risc împreună cu persoana care îndeplineşte funcţia de conformitate şi/sau auditul intern, respectiv auditul extern (financiar/IT) vor efectua activităţi de verificare cum ar fi: controale cu privire la activitatea agenţilor pentru servicii de investiţii financiare, verificări periodice cu clienţii pentru confirmarea activităţii, verificări inopinate cu clienţii în legătură cu tranzacţii de valori mari.-

Art.17. În scopul diminuării impactului riscului specific şi al riscului de piaţă asupra portofoliului de instrumente financiare deţinut de societate în contul „House", Departamentul Analiză Financiară transmite Administratorului de risc, Departamentului Front-Office & Tranzacţionare şi conducătorilor societăţii, rapoarte periodice de analiză a emitenţilor şi pieţei în ansamblul său.-

Secţiunea 3 - Riscuri operaţionale

Art.18.(1) S.S.I.F. identifică toate sistemele informatice importante utilizate pe ambele componente, respectiv infrastructura hardware şi software, care sunt esenţiale în activitatea desfăşurată de către acestea.
(2) Sistemele informatice importante prevăzute la alin. (1) cuprind, în funcţie de activitatea desfăşurată, cel puţin următoarele, fără a se limita la acestea:
a) sistemele informatice necesare pentru derularea în bune condiţii a activităţii autorizate/avizate de A.S.F.;
1. sisteme de tranzacţionare/sisteme alternative de tranzacţionare;
2. sisteme de compensare, decontare, depozitare şi custodie;
3. platforme/aplicaţii de tranzacţionare sau distribuţie prin internet sau telefon;
4. sisteme de gestiune asiguraţi;
5. sisteme de gestiune şi subscriere contracte de asigurare;
6. sisteme de înregistrare şi gestiune a dosarelor de daună;
7. platforme de emitere a contractelor de asigurare;
8. sisteme de calcul al comisioanelor;
9. sisteme de gestiune a contractelor de reasigurare;
10. sisteme de gestiune a participanţilor la fondurile de pensii private;
11. sisteme de administrare a portofoliilor de instrumente financiare ale fondurilor de pensii private;
12. sisteme de call-center;
13. aplicaţii online utilizate în scopul de distribuţie şi informare a clienţilor, precum accesarea conturilor online;
14. sisteme informatice de back-office, altele decât cele care se încadrează la pct. 1-13;
b) sisteme interne pentru asigurarea raportărilor către A.S.F. şi alte instituţii/entităţi ale pieţei financiare;
c) sisteme informatice folosite în activitatea financiar- contabilă a entităţii, cum ar fi programele de contabilitate;

d) sisteme electronice de vot şi alte sisteme informatice cu implicaţii semnificative asupra sistemului de guvernanţă al
entităţii, precum sisteme de tip teleconferinţă/videoconferinţă utilizate pentru desfăşurarea la distanţă a şedinţelor
consiliului de administraţie/consiliului de supraveghere;
e) sisteme informatice cu impact asupra planului pentru continuitatea afacerii şi redresării activităţii în caz de dezastre;
f) aplicaţii centrale de business, altele decât cele care se încadrează la lit. a)-e);
g) infrastructura informatică utilizată pentru sistemele informatice importante găzduite în locaţiile de centre de date.
(3) Societatea întocmşte şi actualizează permanent un registru cu sistemele informatice importante identificate în conformitate cu prevederile alin. (1) şi (2).
(4) Registrul întocmit în conformitate cu prevederile alin. (3) este supus verificării de către auditorul IT .-

Art.19.(1) Societatea va testa sistemele/programele informatice importante înainte de prima utilizare și la orice modificare în cadrul ciclului de viață al acestora, indiferent dacă sunt realizate cu resurse interne sau de către furnizori externi.
(2) Rezultatul testărilor prevăzute la alin. (1) se consemnează într-un raport de testare IT care cuprinde cel puțin următoarele elemente:

a) echipa de testare;
b) scopul testării;
c) perioada testării;
d) descrierea programului informatic testat;
e) identificarea aplicaţiilor utilizate şi a persoanelor implicate;
f) analiza riscurilor implicate de achiziţia sau modificarea programului informatic, a posibilelor vulnerabilităţi şi a măsurilor de reducere a riscurilor asociate, prin controale de sistem sau de program informatic;
g) descrierea modului în care s-au efectuat testele, scenariile de test, eventualele norme sau standarde aplicate şi rezultatul testării;
h) concluzia echipei de testare;
i) semnătura membrilor echipei de testare. -

Art.20.(1) S.S.I.F. Vienna Investment Trust S.A. evaluează anual şi monitorizează continuu riscurile operaţionale generate de utilizarea sistemelor informatice, prioritizează resursele, implementează măsuri de securitate informatică şi monitorizează eficacitatea acestora prin aplicarea managementului de risc.
(2) Raportul privind evaluarea internă a riscurilor operaţionale efectuată în conformitate cu prevederile alin. (1), este transmisă A.S.F. anual, până la data de 31 martie a anului curent .
(3) Societatea va transmite A.S.F., până la data de 31 martie a anului curent, pentru anul anterior, raportarea Indicatorilor de raportare electronică anuală, în măsura în care aceşti indicatori sunt aplicabili şi sunt aferenţi sistemelor informatice importante. -

Art.21.(1) În funcţie de categoria de risc în care se încadrează societatea în funcţie de natura, dimensiunea şi complexitatea activităţii, precum şi de riscurile pe care le poate induce, respectiv *risc major/risc important/risc mediu/risc scăzut*, societatea are obligaţia de a audita IT sistemele informatice importante, extern sau cu resurse interne certificate, anual / o dată la 2 ani / o dată la 3 ani / o dată la 4 ani, începând cu prima lună ianuarie după data sfârşitului perioadei supuse auditului IT anterior.
(2) Raportul de audit IT va fi transmis A.S.F. până la 30 iunie a anului curent, după ultimul an din perioada supusă auditului, însoţit de copia certificatului de auditor IT semnată pentru conformitate cu originalul valabil la momentul întocmirii raportului de audit .
(3) În cazul în care au fost identificate deficienţe/vulnerabilităţi, raportul de audit IT se transmite A.S.F. însoţit de planul de acţiune din care să rezulte modalitatea de remediere a deficienţelor/vulnerabilităţilor identificate de auditorul IT. -

Art.22. S.S.I.F. Vienna Investment Trust S.A. va desfăşura activităţile precizate în Anexa nr.1, conform categoriei/categoriilor de risc corespunzătoare. -

❖ ***Monitorizarea riscurilor operaţionale***

Art.23.(1) Procesul de monitorizare a riscurilor în cadrul S.S.I.F. Vienna Investment Trust S.A. se realizeaza prin intermediul următoarelor instrumente:

a) Alertă la risc;
b) Registrul de riscuri operaţionale;
c) Indicatori cheue de risc (Key Risk Indicators).

(2) Orice persoană, din cadrul oricărui department, care identifică un risc, analizează preliminar riscul identificat, procedând, pentru documentarea procesului de evaluare, la completarea formularului „**Alertă la risc**" – Anexa nr.2 la prezenta Procedură, respectând următoarele etape:

1. descrierea nartativă a riscului, cu respectarea următoarelor reguli:

- riscul este o situaţie, eveniment, care poate să apară. Riscul este o incertitudine şi nu ceva sigur;
- nu se identifică riscuri care nu afectează organizația;
- problemele dificile identificate nu trebuie ignorate. Ele pot deveni riscuri în situaţii repetitive din cadrul aceleiaşi structuri organizatorice sau pentru alte structuri organizatorice în care astfel de riscuri nu s-au materializat;
- riscurile nu trebuie definite numai prin impactul lor asupra activităților organizației. Impactul nu este risc, ci consecinţa exploatării unei vulnerabilități;
- riscurile nu se descriu prin negarea unei situații;
- problemele care vor apărea cu siguranţă, nu constituie riscuri, ci certitudini;
- problemele a căror apariţie este imposibilă, nu constituie riscuri, ci ficţiuni.

2. prezentarea preliminară a cauzelor, descrierea circumstanţelor şi a factorilor care favorizează apariţia riscului.

3. analizarea preliminară a consecinţelor asupra activităților şi operațiunilor, în cazul materializării riscului.

4. evaluarea preliminara a expunerii la risc se realizează prin:

a) stabilirea valorii resursei/operațiunii, pe o scală în trei trepte, ca fiind: puțin importantă (valoare=1), necesară (valoare=2) sau vitală (valoare=3).
b) estimarea probabilităţii de apariţie a riscului, pe o scală în trei trepte, ca fiind: neglijabilă (valoare=1), medie (valoare=2) sau mare (valoare=3).
c) estimarea vulnerabilității sistemului informatic, pe o scală în trei trepte, ca fiind: neglijabilă (valoare=1), medie (valoare=2) sau mare (valoare=3).
d) evaluarea preliminară a nivelului riscului, conform matricei de risc, pe o scală cu trei trepte, ca fiind: scăzut, mediu sau mare.
e) evaluarea preliminară a valorii riscului se realizează prin adunarea valorii resursei, cu valoarea probabilității și cu cea a vulnerabilității. Valoarea maximă a riscului este 9 (3+3+3 = 9 – resursa este vitală, probabilitatea este mare și vulnerabilitatea este mare).

5. formularea unei opinii cu privire la măsurile de tratare (controalele de risc) ce ar trebui întreprinse pentru a gestiona riscul în mod adecvat, astfel încât să se încadreze în limitele de toleranță.

6. formularul "Alertă la risc" completat corespunzător este trimis coordonatorului stucturii organizatorice.

(3) Coordonatorul structurii organizatorice analizează fiecare formular "*Alertă la risc",* primit de la persoanele care au efectuat analiza preliminară a riscurilor, propunând:

1. clasarea formularului "*Alertă la risc"*, dacă riscul este nerelevant;
2. înregistrarea riscului ca aparţinând activității sau operațiunii care se bazează pe sistemul informatic utilizat/administrat de structura organizatorică, caz în care confirmă existența riscului la nivelul structurii organizatorice, stabilește/confirmă nivelul riscului și propune cel puțin o măsură de tratare a acestuia.

(4) După finalizarea acţiunii de analiză preliminară a riscurilor, conducătorul structurii organizatorice centralizează rezultatele analizei datelor/informaţiilor cuprinse în formularele "Alertă la risc", la care anexează documentaţia privind riscurile nou-identificate.

(5) În cadrul analizei „alertelor la risc" conducătorul structurii organizatorice desfăşoară următoarele acţiuni:

1. deliberează asupra tuturor riscurilor şi stabileşte riscurile pentru care să fie luată decizia de "reţinere pentru gestionare" în cadrul structurii organizatorice;
2. propunere **clasare** pentru riscurile considerate nerelevante;
3. deliberează asupra riscurilor propuse spre includere în Registrul Riscurilor şi face propuneri de completare a Registrului Riscurilor, cel puţin în următoarele situaţii:

a) măsurile prin care se realizează un control satisfăcător al riscurilor exced competenţele decizionale ale structurii organizatorice;
b) resursele structurii organizatorice sunt insuficiente;
c) se identifică riscuri externe structurii organizatorice, dar al căror impact afectează obiectivele stabilite pentru acesta.

4. efectuează, pentru fiecare risc identificat şi evaluat, o comparare a expunerii la risc cu limitele de toleranţă aprobate de conducerea societăţii;

5. analizează rapoartele de audit, reţinând riscurile identificate prin acestea şi măsurile de control recomandate a fi implementate;

6. formulează propuneri pentru conducerea societăţii, pentru fiecare risc identificat şi evaluat, cu privire la tipul de răspuns (strategia adoptată) considerat cel mai adecvat dintre cele de mai jos, decizia finală cu privire la acest aspect aparţinând conducerii societăţii:

a) **acceptarea (tolerarea) riscului**, în cazul riscurilor cu expunere scăzută sau atunci când aplicarea unei strategii de răspuns la risc nu este posibilă;
b) **monitorizarea riscului**, în cazul riscurilor cu impact semnificativ, dar cu probabilitate mică de apariţie;
c) **evitarea riscului**, cu precizarea că aplicarea acestei strategii este limitată în cazul activităţilor care ţin de obiectul de activitate al societăţii și de deciziile conducerii acesteia;
d) **transferarea (externalizarea) riscului**, îndeosebi în cazul riscurilor pentru care se înregistrează doar cheltuieli financiare care pot fi acoperite prin produse de asigurare;
e) **tratarea (atenuarea) riscului**, caz în care se identifică măsurile posibile ce pot fi luate astfel încât riscurile să fie controlate satisfăcător, se grupează în variante alternative, se alege varianta cea mai avantajoasă din perspectiva raportului cost/beneficiu.

7. stabilește ordinea de priorităţi în tratarea riscurilor reţinute pentru gestionare, astfel încât expunerea la riscurile reziduale să se situeze în limitele de toleranţă aprobate;

8. stabilește măsurile de control ce trebuie luate în vederea reducerii nivelului riscurilor (reducerea probabilității sau a impactului), termenele-limită până la care acestea trebuie implementate, precum şi persoanele responsabile cu implementarea lor prin elaborarea unui plan pentru implementarea măsurilor de control.

(6) Conducerea societăţii și persoana/comitetul desemnată/desemnat de aceasta cu r*esponsabilități pentru gestionarea riscurilor, dacă există,* desfăşoară următoarele acţiuni:

1. primește formularele “Alertă la risc” şi documentaţia aferentă pentru riscurile semnalate de către fiecare structură organizatorică;

2. transmite persoanelor responsabile cu implementarea măsurilor de control, modificarea măsurilor sau a termenelor pentru riscurile aflate deja în faza de implementare a măsurilor de Conformitate;

3. iniţial intocmeşte şi ulterior completează, ori actualizează, după caz, Registrul Riscurilor cu datele/informaţiile despre riscurile care sunt sau care urmează a fi gestionate la nivelul tuturor structurilor organizatorice;

4. în vederea asigurării unui proces formalizat în mod transparent de gestionare a riscurilor, se va proceda la completarea Formularului “Planul de acţiune împotriva riscurilor” (Anexa nr.3) şi Formularului “Fişă de urmărire a riscurilor“ (Anexa nr.4).

(7) Evaluarea de risc se efectuează regulat, dar cel puţin anual. Funcția de administrare a riscului integrează toate riscurile semnificative pentru entitate pe o hartă ce reprezintă profilul de risc al S.S.I.F. Vienna Investment Trust S.A. Profilul de risc este analizat şi discutat oricând au loc schimbări importante în societate. –

Art.24.(1) Monitorizarea riscurilor se face de către administratorul de risc pe baza informaţiilor cuprinse în ***Registrul centralizat al riscurilor operaţionale*** (monitorizare statică), precum şi prin intermediul Indicatorilor cheie de risc - KRI (monitorizare dinamică).

(2) Datele şi informaţiile cuprinse în registrele departamentelor operaţionale sunt centralizate într-un singur registru, Registrul centralizat la riscurilor operaţionale, ţinut şi actualizat de către administratorul de risc.

(3) Informaţiile cuprinse în registrele departamentelor operaţionale sunt actualizate cel puţin semestrial la nivelul fiecărui departament şi apoi agreate la nivelul Departamentului de Administrare Riscuri.

(4) În măsura în care sunt identificate riscuri noi ce nu au fost notificate prin formularul "Alertă la risc" sau se constată modificarea impactului şi/sau a probabilităţii de producere a riscurilor deja identificate, se vor actualiza în mod corespunzător registrele fiecărui departament în termen de cel mult 15 zile de la apariţia evenimentului care determină modificarea acestora, împreună cu posibile măsuri de remediere.
(5) Informaţiile actualizate sunt transmise administratorului de risc, acesta din urmă centralizând şi analizând informaţiile şi registrele actualizate, întocmind **matricea riscurilor** pentru fiecare departament, precum şi **matricea riscurilor agregată** şi, pe baza acestora, formulează propuneri de măsuri în vederea diminuării riscurilor potenţiale identificate. –

Art.25.(1) S.S.I.F. Vienna Investment Trust S.A. își evaluează intern riscurile operaţionale generate de utilizarea tehnologiei informaţiilor și comunicaţiilor în conformitate cu cerinţele legale și în funcţie de securitatea informațiilor activității organizației, precum și cele mai bune practici în domeniu și ţine un Registru al riscurilor operaţionale generate de utilizarea sistemelor informatice, conţinând cel puţin elementele prevăzute în Anexa nr.5 la prezenta procedură.
(2) Societatea identifică toate categoriile relevante de risc, pe care le menționează în registrul riscurilor pe patru categorii: oameni, procese, sisteme/tehnologii și mediul extern, ținând cont de riscurile activităților externalizate către furnizorii de produse şi servicii informatice și de comunicaţii.
(3) Riscuri aferente **oamenilor** pot fi, fără a se limita la:

- nerespectarea proceselor, procedurilor sau a instrucțiunilor de lucru;
- erori de introducere manuală sau de utilizare neadecvată a sistemelor informatice;
- cunostințe, experiență și pregătire insuficientă a personalului care utilizează sau deservește sistemele informatice;
- personal insuficient;
- dependența de angajați cheie;
- lipsă de comunicare și cooperare între angajați;
- neraportarea erorilor sau greșelilor aferente sistemelor informatice;
- alterarea datelor;
- modificarea informațiilor sau a datelor din rapoarte, fără documentarea adecvată;
- conflict de interese între personalul care dezvoltă și cel care administrează sistemele informatice ori între utilizatorii acestora;
- lipsa unei delimitări clare între rolurile persoanelor care accesează/administrează/ dezvoltă sistemele informatice;
- automulțumire;
- fraudă;
- operațiuni suspecte de spălarea banilor și finanțarea actelor de terorism;
- nerespectarea regimului de sancțiuni internaționale.

(4) Riscuri aferente **proceselor** pot fi, fără a se limita la:

a) ***Riscuri de model:*** lipsa proceselor organizatorice (cel puţin referitoare la managementul schimbării, al incidentelor, al problemelor, al nivelurilor de servicii, al versionărilor, al capacităţii, al disponibilităţii și al proiectelor), erori de metodologie sau de model, erori de evaluare, disponibilitatea rezervelor pentru acoperirea pierderilor, complexitatea modelelor, control inadecvat al proceselor, software neadecvat obiectivelor de activitate, insuficienţa guvernanţei corporative în domeniu;

b) ***Riscuri tranzacționale:*** erori de execuție, erori de înregistrare, managementul inadecvat al datelor și informațiilor, erori de matching, compensare, colateral, complexitatea produselor, riscuri de capacitate, riscuri de evaluare, riscuri de confidențialitate, fraude;

c) ***Riscuri aferente controlului operațiunilor:*** lipsa separării drepturilor și atribuțiilor, depășirea limitelor, riscuri de volum, riscuri de securitate, riscuri de raportare, riscuri de înregistrări contabile neadecvate, control inadecvat al activităților externalizate, întreruperea furnizării serviciilor, neidentificarea operațiunilor în speță în funcție de indicatorii de risc și variabile analitice prestabilite.

(5) Riscuri aferente **sistemelor/tehnologiei** pot fi, fără a se limita la:

- sistem inadecvat de management al tehnologiei și securității;
- lipsa metodologiilor de dezvoltare si testare;
- capacitate insuficientă de procesare;
- întreruperi în funcționarea sistemelor (hardware, software, stocare, telecomunicații);

- căderi de rețea;
- întreruperi în furnizarea serviciilor prestate de furnizorii externi;
- sisteme inadecvate;
- protecție inadecvată împotriva malware;
- riscuri de compatibilitate;
- riscuri generate de furnizori/vânzători;
- erori de programare;
- coruperea datelor;
- riscuri de recuperare după dezastre;
- testare necorespunzătoare a recuperării în caz de dezastru;
- sistem inadecvat de actualizare tehnologică;
- sisteme învechite;
- servicii necorespunzătoare de suport pentru sisteme.

(6) Riscuri aferente **mediului extern** pot fi, fără a se limita la:

- pierderi datorate evenimentelor catastrofice/dezastrelor naturale sau generate de oameni ori factori din afara organizației;
- întreruperi în furnizarea serviciilor prestate de furnizori externi;
- fraude și activități criminale externe;
- expuneri externe ale securității sistemelor;
- atacuri teroriste clasice sau informatice;
- criminalitate economică și/sau informatică;
- căderi ale alimentării cu electricitate. -

Art.26. ***Indicatorii cheie de risc (Key Risk Indicators)*** sunt utilizaţi în monitorizarea şi previzionarea riscurilor operaţionale prin cuantificarea unor situaţii specifice într-o perioadă dată sau pentru un anumit interval, constituind un instrument de avertizare a posibilelor expuneri la riscuri.-

Art.27. S.S.I.F. Vienna Investment Trust S.A. își defineşte apetitului la risc prin definirea unor limite la care indicatorii de risc sunt folosiți ca suport. Societatea asigură procesul de monitorizare și măsură prin indicatorii cheie de risc (KRI), identificând pierderile operaționale potențiale cauzate de deficiențele legate de IT și comunicații.-

Art.28.(1) Societatea a stabilit, prin P-03 (Reguli şi proceduri pentru securitatea şi controlul sistemelor informatice), un set de indicatori cheie de risc aferenți naturii, dimensiunii și complexității acesteia.
(2) Metodologia de determinare şi utilizare a indicatorilor cheie este supusă revizuirii anuale, fiind modificată/completată corespunzător cu natura şi evoluţia activităţilor S.S.I.F. Vienna Investment Trust.-

Art.29. S.S.I.F. Vienna Investment Trust S.A. efectuează, ca urmare a evaluărilor proprii și când este cazul, controale preventive şi controale de avertizare. -

Art.30.(1) Societatea controlează riscurile generate de utilizarea sistemelor informatice prin:

- stabilirea de obiective de control;
- implementarea de puncte de control;
- monitorizarea punctelor de control și a indicatorilor cheie de risc.

(2) În acest scop, se efectuează atât controale generale la nivelul sistemului informatic, cât şi controale specifice la nivelul fiecărei componente a acestuia, după caz. Informaţiile din punctele de control sunt colectate periodic la alegerea societăţii sau când este cazul și vor fi păstrate la dispoziţia S.S.I.F. Vienna Investment Trust S.A. și raportate către A.S.F. pe baza cerințelor de raportare.-

❖ ***Măsuri preventive***

Art.31.(1) Pentru a stabili măsuri preventive corespunzătoare riscurilor identificate şi impactului pe care acestea l-ar putea avea, registrul riscurilor se revizuieşte periodic şi ori de câte ori este necesar, atât la nivelul fiecărui departament, cât şi la nivel centralizat.
(2) În cadrul procesului de revizuire, se analizează dacă:

1. riscurile persistă;
2. au apărut riscuri noi;

3. impactul şi probabilitatea riscurilor au suferit modificări, caz în se revizuiesc nivelurile riscurilor;
4. sunt necesare noi măsuri de control al riscului şi termene pentru implementarea acestora;
5. se impune reprioritizarea riscurilor.

(3) În cadrul procesului de gestionare şi revizuire a riscurilor se analizează cel puţin următoarele:
1. activităţile desfăşurate în perioada pentru care se realizează modificarea/actualizarea/ completarea registrului riscurilor;
2. riscurile noi identificate, tipul de răspuns şi măsurile de control instituite/propuse;
3. rezultatele reevaluării riscurilor, dacă este cazul;
4. orice alte aspecte considerate relevante în legătură cu gestionarea riscurilor.-

Art.32.(1) S.S.I.F. Vienna Investment Trust S.A. recunoaște expunerile sale la riscuri rezultate din operațiunile zilnice, precum și din realizarea obiectivelor sale strategice.
(2) Gestionarea eficientă a riscurilor este considerată vitală în vederea atingerii obiectivelor strategice. În acest context, strategia societății privind administrarea riscurilor semnificative asigură cadrul pentru identificarea, evaluarea, monitorizarea, gestionarea și raportarea riscurilor semnificative, în vederea menținerii lor la niveluri acceptabile în funcție de apetitul la risc al societății și de capacitatea ei de a acoperi (absorbi) aceste riscuri.-

↳ Limitele de toleranţă

Art.33. Strategia de risc a S.S.I.F. Vienna Investment Trust S.A. este bazată pe trei parametri:
- **Apetitul la risc** indică nivelul riscului pe care societatea este dispusă să îl accepte.
- **Profilul de risc** reprezintă totalitatea riscurilor la care societatea este expusă în funcție de obiectivele strategice și, în mod corespunzător, de apetitul la risc. Profilul de risc, evaluat potrivit matricei de risc, nu este o măsură statică, ci o evaluare a riscurilor în evoluție, cu o frecvență predeterminată. Rolul său este acela de a determina dimensiunea fiecărui risc semnificativ și a nivelului general de risc, pe baza unor indicatori.
- **Toleranța la risc** reprezintă capacitatea societății de a accepta sau absorbi riscurile.-

Art.34.(1) Consiliul de administrație aprobă apetitul și limitele de toleranță la risc ale societații, precum și prezentele reguli şi proceduri, pe baza propunerilor formulate de către administratorul de risc şi persoana care îndeplineşte funcţia de conformitate, ulterior prezentării acestora conducerii executive şi Comitetului de Risc şi cu luarea în considerarea a recomandărilor şi observaţiilor formulate în acest sens.
(2) Consiliul de administrație va evalua semestrial, în funcţie de politicile, procedurile și controalele efectuate, eficienţa sistemului de administrare/management a/al riscurilor implementat, în baza raportului de risc.
(3) Propunerile privind introducerea unor noi limite de toleranţă sau revizuirea celor existente se realizează de către administratorul de risc împreună cu şi pe baza informaţiilor primite de la departamentele operaţionale, cel puţin anual.
(4) Toate riscurile vor fi controlate astfel încât expunerea la risc să se încadreze în limitele de toleranţă aprobate. Limitele de toleranţă la risc trebuie respectate de către toate departamentele operaţionale, acestea urmărind diminuarea riscurilor identificate şi a factorilor care pot conduce la apariţia riscurilor, şi au aplicabilitate până la o nouă revizuire.-

Art.35. Obiectivele strategiei privind administrarea riscurilor semnificative sunt:
- determinarea riscurilor semnificative ce pot interveni în cursul normal al activității și formalizarea unui cadru adecvat de administrare și control al acestora, prin adoptarea celor mai bune practici, adaptate dimensiunii, profilului de risc și strategiei de risc a societății;
- dezvoltarea unui registru de riscuri cât mai detaliat care să faciliteze identificarea acestora la nivel de tranzacție și de portofoliu și care să le structureze și să le ierarhizeze în funcție de impactul posibil asupra activității curente a societății;
- delimitarea nivelului de risc acceptat pentru fiecare activitate semnificativă și pentru ansamblul activităților, în raport cu liniile strategice generale stabilite la nivelul structurii de conducere;
- promovarea unei culturi de conștientizare și gestionare a riscurilor la nivelul tuturor departamentelor.-

↳ Controlul activităţilor/sistemelor, măsuri de reducere a riscurilor

Art.36.(1) Administratorul de risc, împreună cu şi pe baza măsurilor de gestionare şi monitorizare primite de la fiecare departament operaţional, precum şi pe baza măsurilor proprii identificate pentru gestionarea riscurilor care sunt determinate pe baza registrului de riscuri centralizat, întocmeşte şi propune *Planul pentru implementarea măsurilor de control al riscurilor* pentru anul în curs, până la finele lunii februarie, urmărind, de asemenea, deciziile conducerii executive şi ale Consiliului de Administraţie cu privire la activitatea societăţii, recomandările privind măsurile de control cuprinse în rapoartele de audit, constatările şi recomandările Compartimentului de Conformitate.

(2) *Planul pentru implementarea măsurilor de control al riscurilor* conţine informaţii cu privire la, dar nelimitându-se la: tipul/categoria de risc identificat şi impactul acestuia, termene de implementare, interdependenţe între departamentele operaţionale, dacă este cazul, observaţii.

(3) *Planul pentru implementarea măsurilor de control al riscurilor* propus este revizuit/aprobat de către conducerea executivă şi Comitetul de Risc înainte de a fi transmis spre aprobare către Consiliul de Administraţie.

(4) *Planul pentru implementarea măsurilor de control al riscurilor* aprobat de C.A. este transmis directorilor fiecărui departament în vederea aplicării măsurilor aprobate.-

Art.37.(1) Trimestrial şi ori de câte ori este cazul, departamentele operaţionale informează administratorul de risc cu privire la stadiul implementării măsurilor de control al riscului, a eficacităţii acestora, precum şi cu privire la rezultatul reevaluarării riscurilor din sfera lor de responsabilitate pentru care au fost stabilite măsurile, pentru analiză şi monitorizare.

(2) Administratorul de risc analizează cauzele, efectele şi măsurile propuse de către departamentele operaţionale care au notificat evenimentul care a determinat un risc operaţional prin formularul „Alertă la risc", solicită informaţii suplimentare şi propune completarea măsurilor, dacă este cazul.

(3) Administratorul de risc monitorizează îndeplinirea măsurilor stabilite în *Planul pentru implementarea măsurilor de control al riscurilor* şi informează trimestrial şi ori de câte ori este necesar atât conducerea executivă, cât şi Comitetul de Risc, Comitetul de Audit şi Consiliul de Administraţie.-

Art.38.(1) Cel puţin anual şi ori de câte ori este cazul conducătorii structurilor organizatorice asigură analizarea stadiului implementării măsurilor de control, a eficacităţii acestora, precum şi reevaluarea riscurilor din sfera lor de responsabilitate.

(2) Anual, conducătorii structurilor organizatorice elaborează un raport cu privire la desfăşurarea procesului de gestionare/revizuire a riscurilor la nivelul structurii organizatorice. Raportul poate fi integrat în raportul administratorului de risc în czul în care procesul de gestionare/revizuire a riscurilor se efectuează în colaborare cu administratorul de risc. Raportul cuprinde o sinteză a activităţilor desfăşurate, în perioada de raportare, în cadrul procesului de gestionare a riscurilor, conţinând cel puţin următoarele aspecte:

1. activităţile derulate în perioada pentru care se întocmeşte raportul, în scopul tratării riscurilor identificate;
2. riscuri noi, tipul de răspuns şi măsurile de control instituite/propuse;
3. rezultatele reevaluării riscurilor, în cazul în care riscurile au fost reevaluate în perioada raportată;
4. menţiuni cu privire la întocmirea/actualizarea Registrului riscurilor;
5. alte aspecte/probleme considerate relevante, în legătură cu modul în care au fost gestionate riscurile la nivelul structurii organizatorice.

(3) *Raportul privind gestionarea și revizuirea riscurilor* cuprinde, distinct, două secţiuni referitoare la:

- riscurile cu un nivel al expunerii ridicat şi foarte ridicat, care ar putea afecta îndeplinirea obiectivelor specifice ale structurilor organizatorice;
- stadiul implementării Planului menţionat la art.36, la data raportării.

(4) Conducătorul structurii organizatorice transmite conducerii societăţii și persoanei/comitetului desemnate/desemnat de aceasta cu r*esponsabilități în gestionarea riscurilor, dacă există*, un exemplar al raportului, în vederea:

1. întocmirii şi actualizării Registrului riscurilor centralizat, prin agregarea datelor/informaţiilor cuprinse în Registrul riscurilor de la nivelul fiecărei structuri organizatorice;

2. întocmirii şi actualizării profilului de risc al societăţii, prin regruparea riscurilor identificate, evaluate şi ierarhizate în raport cu mărimea deviaţiei expunerii fiecărui risc de la toleranţa la risc;

3. întocmirii raportului privind evaluarea internă a riscurilor operaționale generate de sistemele informatice ce va fi raportat Autorităţii de Supraveghere Financiară, în conformitate cu prevederile art.49 alin.(1) lit. a) din Norma A.S.F. nr. 4/2018. În cadrul raportului se cuprinde, distinct, o secţiune referitoare la riscurile cu un nivel al expunerii ridicat şi foarte ridicat, care ar putea afecta îndeplinirea activităţii societății.

(5) În situaţia în care intervin modificări în conţinutul rapoartelor şi a registrelor de riscuri, conducătorii structurilor organizatorice asigură transmiterea rapoartelor şi/sau registrelor revizuite în cel mai scurt timp posibil, dar nu mai târziu de 15 zile de la data modificării acestora, către conducerea S.S.I.F. Vienna Investment Trust S.A.-

Art.39. S.S.I.F. Vienna Investment Trust S.A. aplică proceduri operaționale în domeniul combaterii spălării banilor și finanțării terorismului, precum și regimului de sancțiuni internaționale ca parte integrată a reglementărilor emise de A.S.F. –

❖ ***Rapoarte şi informaţii***

↳ **Rapoarte lunare**

Art.40.(1) Administratorul de risc raportează lunar Directorului general şi Comitetului de Risc:

- evenimentele cu scor de risc (calculat în conformitate cu Planul operaţional al managementului riscului de piaţă – P-17) mai mare decât 4 identificate în activitatea curentă a departamentelor operaţionale şi transmise administratorului de risc fie prin intermediul formularului „Alertă la risc”, fie urmare a revizuirii periodice a Registrului riscurilor. Informaţiile vor fi preluate din Registrul centralizat al riscurilor operaţionale.
- evenimentele cu impact potenţial asupra societăţii identificate în procesul de monitorizare curentă a operaţiunilor desfăşurate de către departamentele operaţionale, pe baza rapoartelor primite de la aceste departamente.

(2) Rapoartele se întocmesc separat pentru lunile: ianuarie, februarie, aprilie, mai, iulie, august, octombrie şi noiembrie, informaţiile corespunzătoare lunilor: martie, iunie şi decembrie vor fi incluse în rapoartele trimestriale/semestriale aferente.-

↳ **Rapoarte trimestriale**

Art.41. Trimestrial şi ori de câte ori este cazul, departamentele operaţionale informează administratorul de risc cu privire la stadiul implementării măsurilor de control al riscului, în cazul în care s-au trasat măsuri de control al riscului în trimestrul respectiv, a eficacităţii acestora, precum şi cu privire la rezultatul reevaluarea riscurilor din sfera lor de responsabilitate pentru care au fost stabilite măsurile, pentru analiză şi monitorizare.-

Art.42. Administratorul de risc raportează trimestrial şi ori de câte ori este necesar Consiliului de Administraţie şi conducerii executive şi informează Comitetul de Risc şi Comitetul de Audit cu privire la:

- aplicarea regulilor şi procedurilor privind identificarea, evaluarea, monitorizarea, gestionarea și raportarea riscurilor, din proprie initiaţivă sau la solicitarea Consiliului de Administraţie / conducerii executive;
- monitorizarea îndeplinirii şi stadiul implementării măsurilor stabilite în *Planul pentru implementarea măsurilor de control al riscurilor* şi adoptate de către Consiliul de Administraţie, la data raportării, după caz;
- rezultatele măsurilor implementate în activitatea departamentelor operaţionale, după caz;
- riscurile operaţionale identificate şi la care se expune societatea, respectiv riscurile cu un nivel al expunerii ridicat şi foarte ridicat, care ar putea afecta îndeplinirea proceselor asociate activităţilor departamentelor operaţionale cu respectarea obiectivelor specifice ale structurilor organizatorice;
- rezultatele controalelor şi verificărilor realizate la nivelul departamentelor operaţionale;
- propuneri de măsuri care pot diminua riscurile identificate şi posibilele pierderi.-

Art.43. Rapoartele se întocmesc separat pentru trimestrul I şi trimestrul III. Informaţiile corespunzătoare rapoartelor trimestrului II şi trimestrului IV vor fi incluse în rapoartele semestriale aferente.-

Rapoarte semestriale

Art.44.(1) Informaţiile cuprinse în registrele de riscuri ale departamentelor operaţionale sunt actualizate cel puţin semestrial la nivelul fiecărui departament şi apoi agreate la nivelul Departamentului de Administrare Riscuri. Informaţiile actualizate sunt transmise administratorului de risc, acesta din urmă centralizând şi analizând informaţiile şi registrele actualizate, întocmind matricea riscurilor pentru fiecare departament, precum şi matricea riscurilor agregată şi, pe baza acestora, formulează propuneri de măsuri în vederea diminuării riscurilor potenţiale identificate. –

(2) Administratorul de risc întocmeşte şi prezintă semestrial Consiliului de Administraţie, Comitetului de Risc şi conducerii executive Raportul privind administrarea riscurilor în vederea analizării şi evaluării eficienţei sistemului de management al riscurilor în funcţie de politicile, procedurile și controalele efectuate.

(3) *Raportul privind administrarea riscurilor* cuprinde informaţiile corespunzătoare rapoartelor trimestrului II şi trimestrului IV menţionate la art. 41 şi art. 42, precum şi:

a) rezultatele monitorizării cu privire la apetitul şi limitele toleranţei la risc, inclusiv cele privind cerinţele de adecvare a capitalului;
b) analiza eficacităţii indicatorilor şi parametrilor utilizaţi pentru monitorizarea performanţelor privind managementul riscurilor societăţii, în concordanţă cu cele mai bune practici aplicabile, inclusiv cu privire la sistemele şi instrumentele de management al riscurilor utilizate în cadrul societăţii şi propuneri de modificare/îmbunătăţire/actualizare a respectivilor indicatori sau parametri, după caz;
c) propuneri privind scenariile de stres şi planuri de testare a acestora privind operaţiunile desfăşurate în cadrul departamentelor operaţionale, pe baza situaţiilor identificate în activitatea de monitorizare în colaborare cu respectivele departamente;
d) analiza riscurilor asociate proiectelor strategice sau cu impact semnificativ asupra activităţii societăţii şi propuneri pentru administrarea acestora.

(4) *Raportul privind administrarea riscurilor* va prezenta informaţiile sub următoarea structură:

1. numărul de evenimente apărute, clasificate pe arii/zone de riscuri şi categorii;
2. descrierea riscurilor, tipul de risc (potenţial/materializat), circumstanţe/factori care favorizează apariţia riscurilor, posibile consecinţe;
3. scorul de risc aferent respectivului eveniment operaţional;
4. pentru fiecare risc identificat şi evaluat vor fi făcute propuneri cu privire la măsurile de gestionare şi monitorizare (inclusiv propuneri de strategie spre a fi adoptate sau alt plan de acţiuni) considerate a fi adecvate situaţiei particulare, respectiv una din următoarele:
    i. **acceptarea (tolerarea) riscului**, în cazul riscurilor cu expunere scăzută sau atunci când aplicarea unei strategii de răspuns la risc nu este posibilă;
    ii. **monitorizarea permanentă a riscului**, în cazul riscurilor cu impact semnificativ, dar cu probabilitate mică de apariţie;
    iii. **evitarea riscului**, cu precizarea că aplicarea acestei strategii este limitată în cazul activităţilor care ţin de obiectul de activitate al organizației și de deciziile conducerii acesteia;
    iv. **transferarea (externalizarea) riscului**, îndeosebi în cazul riscurilor pentru care se înregistrează doar cheltuieli financiare care pot fi acoperite prin produse de asigurare;
    v. **tratarea (atenuarea) riscului**, caz în care se identifică măsurile posibile care pot fi luate astfel încât riscurile să fie controlate satisfăcător, se grupează în variante alternative, se alege varianta cea mai avantajoasă din perspectiva raportului cost/beneficiu.
5. propunerea unui termen posibil de punere în aplicare a măsurilor de control al riscurilor;
6. alte informaţii precum: nivelul riscului rezidual şi eventuale observaţii.

(5) Testele de stres vor avea conţinutul prezentat în Anexa nr.8, fiind realizate semestrial şi ori de câte ori personalul implicat sesizează erori de funcţionare a programelor/sistemelor informatice importante sau actualizarea programului/sistemului informatic presupune o modificare majoră a acestuia, respectiv afectează situaţiile supuse testelor de stres anterioare şi pentru care testele nu mai sunt, astfel, valide.-

Rapoarte anuale

Art.45. Administratorul de risc prezintă anual recomandări privind limitele de toleranţă Comitetului de Risc şi, împreună cu acesta, raportează revizuirea limitelor de toleranţă Consiliului de Administraţie al societăţii. Propunerile privind introducerea unor noi limite de toleranţă sau revizuirea celor existente se realizează de către administratorul de risc împreună cu şi pe baza informaţiilor primite de la departamentele operaţionale, cel puţin anual.-

Art.46. Evaluarea riscului se efectuează regulat, dar cel puţin anual. Funcția de administrare a riscului integrează toate riscurile semnificative pentru entitate pe o hartă ce reprezintă profilul de risc al S.S.I.F. Vienna Investment Trust S.A. Profilul de risc este analizat şi discutat oricând au loc schimbări importante în societate.-

Art.47. Metodologia de determinare a indicatorilor cheie de risc este supusă revizuirii anuale, fiind modificată/completată corespunzător cu natura şi evoluţia activităţilor S.S.I.F. Vienna Investment Trust.-

Art.48. Administratorul de risc, împreună cu şi pe baza măsurilor de gestionare şi monitorizare primite de la fiecare departament operaţional, precum şi pe baza măsurilor proprii identificate pentru gestionarea riscurilor care sunt determinate pe baza registrului de riscuri centralizat, întocmeşte şi propune *Planul pentru implementarea măsurilor de control al riscurilor* pentru anul în curs, până la finele lunii februarie, urmărind, de asemenea, deciziile conducerii executive şi ale Consiliului de Administraţie cu privire la activitatea societăţii, recomandările privind măsurile de control cuprinse în rapoartele de audit, constatările şi recomandările Compartimentului de Conformitate.-

Art.49. Anual, conducătorii structurilor organizatorice elaborează un raport cu privire la desfăşurarea procesului de gestionare/revizuire a riscurilor la nivelul structurii organizatorice, precum şi cu privire la analizarea stadiului implementării măsurilor de control şi a eficacităţii acestora, în conformitate cu art.38.-

Rapoarte curente

Art.50.(1) Administratorul de risc raportează imediat Directorului general identificarea unor nereguli în activitatea curentă a departamentelor operaţionale şi/sau a unor posibile prejudicii, precum şi situaţiile cu impact potenţial semnificativ asupra societăţii. Situaţiile cu impact potenţial semnificativ vor fi aduse de îndată la cunoştinţa Consiliului de Administraţie, cu informarea Comitetului de Risc.

(2) Administratorul de risc raportează cu privire la zonele de risc specifice atât din proprie initiaţivă, cât şi la cererea Consiliului de Administraţie, a Comitetului de Risc sau a conducerii executive.-

Rapoarte către Autoritatea de Supraveghere Financiară

Art.51.(1) S.S.I.F. Vienna Investment Trust S.A. evaluează anual și monitorizează continuu riscurile operaționale generate de utilizarea sistemelor informatice, prioritizează resursele, implementează măsuri de securitate informatică și monitorizează eficacitatea acestora prin aplicarea managementului de risc.

(2) Rezultatul evaluării interne a riscurilor operaționale este transmis A.S.F. anual, până la 31 martie a anului curent, pentru anul anterior.-

Art.52.(1) S.S.I.F. Vienna Investment Trust S.A., încadrată la categoria de risc important, auditează extern sau cu resurse interne certificate, sistemul informatic utilizat, o dată la 2 ani.

(2) Raportul de audit IT este transmis A.S.F. până la 30 iunie a anului curent, pentru perioada supusă auditării, corespunzătoare categoriei de risc, însoţit de copia certificatului de auditor IT semnată pentru conformitate cu originalul valabil la momentul întocmirii raportului de audit.

(3) În cazul în care au fost identificate deficienţe/vulnerabilităţi, Raportul de audit IT se transmite împreună cu planul de acțiune din care să rezulte modalitatea de remediere a vulnerabilităților identificate pe parcursul derulării activității de audit IT.-

Art.53. Rapoartele privind evaluarea internă a riscurilor operaționale prevăzute la art.51, alin.(2) și rapoartele de audit IT prevăzute la art.52, alin.(2) se depun la A.S.F. pe suport hârtie sau în format electronic cu semnătură electronică extinsă.-

Art.54. Societatea transmite, până la data de 31 martie a anului curent pentru anul anterior, o raportare electronică anuală cu indicatorii menționați în Anexa nr. 7, în cazul în care aceşti indicatori sunt aplicabili şi sunt aferenţi sistemelor informatice importante.-

❖ ***Managementul Securităţii Sistemelor Informatice şi de Comunicaţii***

Art.55. S.S.I.F. Vienna Investment Trust S.A. evaluează intern anual, sau de câte ori este nevoie, rezultatele sistemului de securitate, revizia rezultatelor și acțiunile corective pentru determinarea nivelului de maturitate internă a controalelor de securitate ale societății, conform tabelului din Anexa nr.6, care este parte integrantă din evaluarea internă a riscurilor. -

Secţiunea 4 - Riscul de legislaţie

Art.56. Departamentul Juridic şi persoana care îndeplineşte funcţia de conformitate vor urmări în permanenţă noile apariţii legislative, informând în cel mai scurt timp posibil Societatea şi personalul acesteia, inclusiv administratorul de risc, cu privire la noile dispoziţii legale incidente activităţii societăţii.-

Art.57. În scopul asigurării stabilității S.S.I.F. și a bunei funcționări, vor fi respectate cu strictețe cerințele prudențiale și de adecvare a capitalului pentru prevenirea, evaluarea corectă, monitorizarea și administrarea riscurilor. În situația în care persoana care îndeplineşte funcţia de conformitate cu atribuții în monitorizarea și administrarea riscurilor ia cunostință de eventuale încălcări ale regimului juridic aplicabil, inclusiv ale regulilor şi procedurilor interne ale S.S.I.F., are obligația să informeze imediat, în scris, Consiliul de Administrație.-

Secţiunea 5 - Dispoziţii finale

Art.58.(1) Consiliul de administrație analizează și actualizează la nevoie, adecvarea și eficienţa sistemului de administrare a riscului în vederea gestionării eficiente a activelor deţinute de către societate, precum și modul de administrare a riscurilor aferente la care aceasta este expusă.
(2) Sistemul de administrare a riscului prevăzut la alin.(1) asigură concordanța activităților de control cu riscurile generate de activitățile și procesele care fac obiectul controlului.-
Art.59. Sistemul de Conformitate al societății verifică adecvarea proceselor de identificare, evaluare, monitorizare, gestionare şi raportare a riscurilor, a fiabilităţii informaţiilor financiare şi nefinanciare raportate intern şi extern și a conformității acestora cu legislația specifică aplicabilă, precum și cu deciziile interne ale S.S.I.F. Vienna Investment Trust S.A.-

Art.60. Consiliul de administrație se asigură că toate angajamentele referitoare la remunerare sunt structurate corect și responsabil și că politicile de remunerare permit și promovează o administrare eficientă a riscurilor fără a conduce la o asumare de riscuri care să depășească nivelul toleranței la risc a societății.-

Art.61. Consiliul de administrație se asigură de respectarea cerințelor privind externalizarea/delegarea unor activități operaționale sau funcții, atât înainte de efectuarea acesteia, cât și pe toată durata externalizării/delegării, astfel încât externalizarea/delegarea unor activităţi operaţionale sau funcții să nu genereze o creștere nejustificată a riscurilor operaționale.-

Art.62. S.S.I.F. Vienna Investment Trust S.A. menține şi revizuieste periodic reguli şi proceduri pentru identificarea, evaluarea, monitorizarea, gestionarea şi raportarea riscurilor.-

Anexa nr.1

Activitate		*Categoria de risc a entității*			
		Majoră	*Importantă*	*Medie*	*Scăzută*
A) Evaluare internă a riscului operațional și registrul riscurilor		*x*	*x*	*x*	*x*
B) Organizare pe procese					
1	*Management disponibilitate*	*x*	*x*	*x*	
2	*Management utilizatori*	*x*	*x*	*x*	*x*
3	*Management incidente*	*x*	*x*	*x*	
4	*Management schimbare*				
a)	*Management ciclu viață programe informatice*	*x*	*x*	*x*	*x*
b)	*Management versiuni*	*x*	*x*	*x*	*x*
c)	*Managementl testare*	*x*	*x*	*x*	*x*
5	*Management capacitate*	*x*	*x*	*x*	
6	*Management configuraţii*	*x*	*x*		
7	*Management niveluri servicii (SLA)*	*x*	*x*	*x*	
8	*Management securitate*				
a)	*Cerințe generale*	*x*	*x*	*x*	*x*
b)	*Scanare de vulnerabilităţi*	*x*	*x*	*x*	*x*
c)	*Teste de penetrare* [1]	x	x	x	
9	*Management continuitate*	*x*	*x*	*x*	
C) Puncte de control și măsură					
a)	*Controale generale*	*x*	*x*	*x*	
b)	*Controale program informatic*	*x*	*x*		
c)	*Controale flux financiar*	*x*	*x*	*x*	*x*
D) Implementare indicatori cheie de performanță (KPI)		*x*			
E) Implementare indicatori cheie de risc (KRI)		*x*	*x*		
F) Managementul securității stemului informatic					
a)	*Măsuri organizatorice*	*x*	*x*		
b)	*Proceduri de securitate*	*x*	*x*	*x*	*x*
c)	*Evaluarea internă de securitate*	*x*			
d)	*Plan de cooperare*	*x*	*x*	*x*	*x*

Anexa nr.2

Formular alertă la risc

<table>
<tr><td colspan="4">S.S.I.F. Vienna Investment Trust S.A.</td></tr>
<tr><td colspan="4">Structura organizatorică: ----------</td></tr>
<tr><td colspan="4">DETALII PRIVIND RISCUL</td></tr>
<tr><td rowspan="3">Descrierea riscului</td><td colspan="3">Categorie resursă IT: ----------</td></tr>
<tr><td colspan="3">Denumire resursă IT: ----------</td></tr>
<tr><td colspan="3">Amenințări (factori de risc):
1.----------
2. ----------
3. ----------
4. ----------
5. ----------</td></tr>
<tr><td></td><td colspan="3">Vulnerabilitate (descrierea riscului): ----------
----------</td></tr>
<tr><td>Evaluare valorii resursei</td><td colspan="3"><table><tr><td></td><td></td><td></td></tr><tr><td>1</td><td>2</td><td>3</td></tr></table>1. neimportantă; 2. necesară; 3. vitală.</td></tr>
<tr><td rowspan="2">Evaluarea riscului</td><td colspan="3">Evaluarea probabilității de apariție<table><tr><td></td><td></td><td></td></tr><tr><td>1</td><td>2</td><td>3</td></tr></table>1. neglijabilă; 2. medie; 3. mare.</td></tr>
<tr><td colspan="3">Evaluarea vulnerabilității (impactului)<table><tr><td></td><td></td><td></td></tr><tr><td>1</td><td>2</td><td>3</td></tr></table>1. neglijabilă; 2. medie; 3. mare.</td></tr>
<tr><td rowspan="2">Opinie cu privire la tipul de răspuns la risc</td><td colspan="3">Tipul de răspuns la risc (strategia adoptată):
----------</td></tr>
<tr><td colspan="3">Măsuri de control al riscului recomandate:----------
----------</td></tr>
<tr><td colspan="4">Documentația utilizată pentru fundamentarea riscului identificat (dacă este cazul):----------
----------</td></tr>
<tr><td>Nume:

--</td><td>Semnătura:
----------</td><td colspan="2">Data întocmirii:
zz/ll/aaaa</td></tr>
</table>

Anexa nr.3

PLANUL DE ACŢIUNE ÎMPOTRIVA RISCURILOR

Nr. crt.	Acţiuni preventive stabilite	Responsabili (persoana, compartiment)	Termen limită

Anexa nr.4

FIŞĂ DE URMĂRIRE A RISCURILOR

Riscul monitorizat: .....

Nivelul riscului: ☐ scăzut
☐ mediu
☐ ridicat

Acţiuni preventive - .....
- .....

Acţiuni corective - .....
- .....

Stadiul implementării acţiunilor corective / preventive: .....

Dificultăţi întâmpinate: .....

Noi acţiuni propuse	Responsabil	Termen
.....	.....	.....
.....	.....	.....
.....	.....	.....

Nume: _____

Semnătura: _____

Data urmăririi riscului: _____/_____/_____

Data primei evaluări _____/_____/_____

Anexa nr.5

Registrul riscurilor

Project Name:			Project Manager Name:																
Identificarea riscurilor												Activitati de diminuare a riscurilor							
Risk ID	Titul riscului (amenintare)	Vulnerabilitate (amenintare asociata)	Categoria riscului	Responsabil gestionarea riscului	Rata-Probabilitate	Probabilitate	Impact	Nivel impact	Risk Exposure (Actual)	Rating	Tipul riscului (Oportunitate / Amenintare)	Masuri implementate	Eficienta masurilor % (90,60,30)	Nivel Risc rezidual	Raspunsul la risc / Instrumente de control	Data implementare instrumente de control	Strategie adoptata	Data ultimei revizuiri	Observatii
			Sisteme																
			Procese																
			Oameni																
			Mediu extern																

Evaluare internă a maturităţii controalelor de securitate

Domenii ale Securității Informației	Ratingul maturității controalelor de securitate					
	0 - Ne existent	**1 - Inițial / Ad-Hoc**	**2 - Repetabil dar intuitiv**	**3 - Proces definit**	**4 - Controlat și măsurabil**	**5 - Optimizat**
I. Politici de securitate	Nu au fost stabilite politici prin care să se definească securitatea informațională	Politicile și procedurile nu au fost formalizate	Au fost definite obiective, dar acestea nu sunt clare si concise sau, dupa caz, nu sunt aplicabile in raport activitatea propriu-zisa desfasurate de entitate	Personalul responsabil a fost informat si instruit cu privire la politicile si obiectivele stabilite	Se aplică proceduri de verificare a realizării obiectivelor stabilite prin politici	Politicile corespund exigentelor sporite, sunt revizuite periodic, inclusiv in cazul aparitiei riscurilor semnificative
II. Securitatea organizațională	Nu au fost definite principiile care stau la baza managementului securității	Există principii la nivel informal	Au fost definite principii, dar acestea nu sunt clare și concise sau, dupa caz, nu sunt aplicabile in raport activitatea propriu-zisa desfasurata de entitate	Intreg personalul responsabil a fost informat si instruit in legatura cu principiile aprobate de conducere	Se aplică proceduri de verificare a respectării principiilor stabilite și aprobate	Procedurile sunt revizuite si imbunatatite periodic, inclusiv in cazul aparitiei riscurilor semnificative
III. Controlul și clasificarea activelor	Nu au fost definite proceduri de securitate și siguranță a activelor	Procedurile de securitate și siguranță a activelor sunt aplicate informal	A fost stabilita modalitatea de control, dar acestea nu se efectueaza in mod concret	Persoanele responsabile au fost informate in raport cu procedurile de securitate și siguranță a activelor	Persoanele responsabile aplică adecvat procedurile de securitate și siguranță a activelor	Procedurile de securitate și siguranță a activelor sunt revizuite și modificate periodic, inclusiv in cazul aparitiei riscurilor semnificative
IV. Securitatea personalului	Nu au fost definite principiile care stau la baza managementului securității si incidentelor	Există principii la doar la nivel informal	Au fost definite principii, dar acestea nu sunt clare și concise sau, dupa caz, nu sunt aplicabile in raport activitatea propriu-zisa desfasurata de entitate	Asupra principiilor aprobate de conducere a fost informat si instruit întreg personalul responsabil	Se aplică proceduri de verificare a respectării principiilor stabilite și aprobate	Procedurile sunt revizuite si imbunatatite periodic, inclusiv in cazul aparitiei riscurilor semnificative
V. Securitatea fizica și de mediului de lucru	Nu au fost definite planuri/ proceduri de securiate	Există politici si proceduri doar la nivel informal	Au fost definite proceduri, dar acestea nu sunt clare și concise sau, dupa caz, nu sunt aplicabile in raport activitatea propriu-zisa desfasurata de entitate	Asupra procedurilor aprobate de conducere a fost informat si instruit întreg personalul responsabil	Se aplică proceduri de verificare a respectării principiilor stabilite și aprobate	Procedurile sunt revizuite periodic, si sunt avute in vedere concluziile controalelor generale implementate in cadrul entitatilor
VI. Securitatea echipamentelor	Nu au fost definite planuri/ proceduri de securiate	Există politici si proceduri doar la nivel informal	Au fost definite proceduri, dar acestea nu sunt clare și concise sau, dupa caz, nu sunt aplicabile in raport activitatea propriu-zisa desfasurata de entitate	Asupra procedurilor aprobate de conducere a fost informat si instruit întreg personalul responsabil	Se aplică proceduri de verificare a respectării principiilor stabilite și aprobate	Procedurile sunt revizuite si imbunatatite periodic, inclusiv in cazul aparitiei riscurilor semnificative
VII. Controale generale	Nu au fost definite controalele generale pentru gestionarea activității	Există politici si proceduri doar la nivel informal	Au fost definite proceduri, dar acestea nu sunt clare și concise sau, dupa caz, nu sunt aplicabile in raport activitatea propriu-zisa desfasurata de entitate	Asupra procedurilor aprobate de conducere a fost informat si instruit întreg personalul responsabil	Se aplică proceduri de verificare stabilite si aprobate de conducere, se respecta indicatiile privind controalele generale	Procedurile sunt revizuite si imbunatatite periodic, inclusiv in cazul aparitiei riscurilor semnificative
VIII. Managementul operațiunilor și a comunicațiilor	Nu au fost definite obiectivele specifice	Există politici si proceduri doar la nivel informal	Au fost definite proceduri, dar acestea nu sunt clare și concise sau, dupa caz, nu sunt aplicabile in raport activitatea propriu-zisa desfasurata de entitate	Asupra procedurilor aprobate de conducere a fost informat si instruit întreg personalul responsabil	Se aplică proceduri de verificare a respectării principiilor stabilite și aprobate de conducere	Procedurile sunt revizuite si imbunatatite periodic, inclusiv in cazul aparitiei riscurilor semnificative

Domenii ale Securității Informației	Ratingul maturității controalelor de securitate					
	0 - Ne existent	**1 - Inițial / Ad-Hoc**	**2 - Repetabil dar intuitiv**	**3 - Proces definit**	**4 - Controlat și măsurabil**	**5 - Optimizat**
IX. Controlul accesului	Nu au fost definite controalele pentru verificarea accesului	Există politici si proceduri doar la nivel informal	Au fost definite proceduri, dar acestea nu sunt clare și concise sau, dupa caz, nu sunt aplicabile in raport activitatea propriu-zisa desfasurata de entitate	Principiile care guvernează accesul securizat la informaţii au fost aduse la cunostinta personalului responsabil, care a fost instruit in consecinta	Se aplică proceduri de verificare a respectării principiilor stabilite și aprobate de conducere	Procedurile sunt revizuite si imbunatatite periodic, inclusiv in cazul aparitiei riscurilor semnificative
X. Întreținerea și dezvoltarea sistemelor	Nu au fost definite instrumente și proceduri	Există politici si proceduri doar la nivel informal	Au fost definite proceduri, dar acestea nu sunt clare și concise sau, dupa caz, nu sunt aplicabile in raport activitatea propriu-zisa desfasurata de entitate	Asupra procedurilor aprobate de conducere a fost informat si instruit întreg personalul responsabil	Au fost respectate cerintele legate de securitate ce trebuie avute in vedere in fiecare etapa a ciclului de viata a sistemelor	Procedurile sunt revizuite si imbunatatite periodic, inclusiv in cazul aparitiei riscurilor semnificative
XI. Continuitatea afacerii	Nu au fost definite controalele de management al continuitatii	Există politici si proceduri doar la nivel informal	Au fost definite proceduri, dar acestea nu sunt clare și concise sau, dupa caz, nu sunt aplicabile in raport activitatea propriu-zisa desfasurata de entitate	Asupra procedurilor aprobate de conducere a fost informat si instruit întreg personalul responsabil	Se aplică proceduri de verificare a respectării principiilor stabilite și aprobate	Procedurile sunt revizuite si imbunatatite periodic, inclusiv in cazul aparitiei riscurilor semnificative
XII. Conformitate	Nu au fost definite controalele privind asigurarea conformității	Există politici si proceduri doar la nivel informal	Au fost definite proceduri, dar acestea nu sunt clare și concise sau, dupa caz, nu sunt aplicabile in raport activitatea propriu-zisa desfasurata de entitate	Asupra procedurilor aprobate de conducere a fost informat si instruit întreg personalul responsabil	Se aplică proceduri de verificare a respectării principiilor stabilite și aprobate	Procedurile sunt revizuite si imbunatatite periodic, inclusiv in cazul aparitiei riscurilor semnificative

Anexa nr.7

Indicatori de raportare electronică anuală

Obiectiv în perioada de raportare	Indicator
1	2
Indicatori referitori la accesarea online a serviciilor oferite de entitate	
	Număr de clienți (total utilizatori) care accesează serviciile online oferite de entitate
Indicatori referitori la persoanele care pot să efectueze modificări ale sistemelor/programelor informatice importante	
	Număr de persoane (total utilizatori) care au acces direct la bazele de date ale entității (referitor la portofolii, tranzacții si active) cu drepturi de modificare asupra acestora, rol de administrator sau privilegii echivalente
	Număr de persoane (total utilizatori) care au drepturi de modificare asupra programelor informatice importante ale entității (programe informatice interne/externe/on-line accesate via Internet)
Indicatori referitori la principiul dublei validări prin operațiuni in sistemele informatice importante	
	Număr de operațiuni INIȚIATE care presupun dubla validare
	Număr de operațiuni CONFIRMATE care presupun dubla validare
	Număr de operațiuni ANULATE care presupun dubla validare
Indicatori referitori la accesul la sistemele informatice importante	
	Număr de persoane (total utilizatori) care au acces la sistemele informatice importante care conțin informații referitoare la portofolii, tranzacții și active
	Număr administratori de sistem (total utilizatori) care au acces la credențialele conturilor de acces ale clienților
Indicatori referitori la incidente interne de securitate informatică, declarate	
	Număr total incidente interne de securitate informatică
	Număr total incidente informatice externe
	Număr încălcări politică și proceduri securitate
	Număr pierderi date generate de acțiuni neaprobate
	Număr incidente declarate aferente pierderii de date (date electronice)
	Număr de incidente declarate care au dus la distrugere accidentală sau intenționată de documente / înregistrări / fișiere
	Număr de incidente declarate de încălcare gravă a regulilor / fraude / înșelătorii
	Număr incidente declarate de distrugere in centrul de date
	Număr mediu de zile de la identificarea unui incident de securitate pană la rezolvarea acestuia
Niveluri servicii agreate interne și pentru clienți	
	Număr ore de indisponibilitate neprogramată a sistemelor informatice importante la care au acces clienții (precum, dar nelimitat la aplicații de tranzacționare online, aplicații online pentru subscrierea de polite de asigurare)
	Număr de ore de indisponibilitate neprogramată a serviciilor IT externalizate care afectează serviciile oferite către clienții entităților
Management schimbări	
	Numărul programelor informatice importante
	Numărul de modificări aduse programelor informatice importante
	Număr erori în exploatare generate de deficiențe în proiectarea sistemelor informatice importante
	Număr erori în exploatare neidentificate în testarea sistemelor informatice importante
Indicatori managementul continuității	
	Număr de teste efectuate conform planului de continuitate a afacerii
	Număr de teste efectuate conform planului de recuperare în caz de dezastru
Audituri și testări	
	Număr de audituri interne anuale

Anexa nr.8

RAPORT TESTARE

Scenariu:

……

Acţiune	Funcţie	Nume
……	……..	……..

Data: ……

Functiile sistemului informatic

……
……
……

Arhitectura sistemului informatic

……
……
……

Testare. Demonstrarea functionalității

(se va indica locul desfăşurării testării, perioada testării, subiectul testării)
Programul demonstratiei:
(se vor indica etapele testării, în ce constă testarea şi rezulatul aşteptat)

Rezultate colectate în urma testării:

- Timpul de răspuns: ……
- Timpul de răspuns minim și maxim: ……
- Timpul de răspuns mediu: ……
- Throughput (câte acţiuni concurente poate să susţină sistemul): ……
- Erori: ……

DEFICIENȚE

……
……
……

FINALIZAREA TESTĂRII

……
……
……

CONCLUZIILE ECHIPEI DE TESTARE

DEPARTAMENT	PERSOANA CARE A TESTAT	FUNCTIONARE CORECTĂ		SEMNATURĂ
		DA	NU	