EBA/GL/2017/05

11/09/2017

Ghid

Ghid privind evaluarea riscurilor asociate TIC în cadrul procesului de supraveghere și evaluare (SREP)

1. Conformitate și obligații de raportare

Statutul prezentului ghid

1. Prezentul document conține orientări emise în temeiul articolului 16 din Regulamentul (UE) nr. 1093/20101. În conformitate cu articolul 16 alineatul (3) din Regulamentul (UE) nr. 1093/2010, autoritățile competente și instituțiile financiare trebuie să depună toate eforturile necesare pentru a respecta orientările.

2. Ghidul prezintă punctul de vedere al ABE privind practicile adecvate în materie de supraveghere în cadrul Sistemului european al supraveghetorilor financiari sau privind modul în care ar trebui aplicat dreptul Uniunii într-un anumit domeniu. Autoritățile competente cărora li se aplică ghidul, astfel cum sunt definite la articolul 4 alineatul (2) din Regulamentul (UE) nr. 1093/2010, trebuie să se conformeze și să îl integreze în practicile lor, după caz (de exemplu, prin modificarea cadrului legislativ sau a procedurilor de supraveghere ale acestora), inclusiv în cazurile în care anumite puncte din cuprinsul documentului sunt adresate în primul rând instituțiilor.

Cerințe de raportare

3. În conformitate cu articolul 16 alineatul (3) din Regulamentul (UE) nr. 1093/2010, autoritățile competente trebuie să notifice ABE dacă se conformează sau intenționează să se conformeze prezentului ghid sau, în caz contrar, motivele neconformării, până la 13.11.2017. În absența unei notificări până la acest termen, ABE va considera că autoritățile competente nu s-au conformat. Notificările se trimit prin intermediul formularului disponibil pe site-ul ABE la adresa compliance@eba.europa.eu , cu mențiunea „EBA/GL/2017/05”. Notificările trebuie trimise de persoane care au autoritatea de a raporta cu privire la respectarea ghidului în numele autorităților competente. Orice schimbare cu privire la starea de conformare trebuie adusă, de asemenea, la cunoștința ABE.

4. Notificările vor fi publicate pe site-ul ABE, în conformitate cu articolul 16 alineatul (3).

[1] Regulamentul (UE) nr. 1093/2010 al Parlamentului European și al Consiliului din 24 noiembrie 2010 de instituire a Autorității europene de supraveghere (Autoritatea bancară europeană), de modificare a Deciziei nr. 716/2009/CE și de abrogare a Deciziei 2009/78/CE a Comisiei (JO L 331, 15.12.2010, p.12).

2. Obiectul, domeniul de aplicare și definiții

Obiectul și domeniul de aplicare

5. Prezentul ghid întocmit în conformitate cu articolul 107 alineatul (3) din Directiva 2013/36/UE[2] vizează să asigure convergența practicilor de supraveghere în evaluarea riscului asociat tehnologiei informației și comunicațiilor (TIC) în cadrul procesului de supraveghere și evaluare (SREP) prevăzut la articolul 97 din Directiva 2013/36/UE și menționat ulterior în Ghidul ABE privind procedurile și metodologiile comune pentru procesul de supraveghere și evaluare (SREP)[3]. În mod specific, prezentul ghid enunță criteriile de evaluare pe care trebuie să le aplice autoritățile competente în cadrul evaluării de supraveghere a guvernanței și strategiei instituțiilor cu privire la TIC și al evaluării de supraveghere a expunerilor la riscul asociat TIC și a procedurilor de control al riscurilor asociate TIC ale instituțiilor. Prezentul ghid constituie parte integrantă din Ghidul SREP al ABE.

6. Autoritățile competente trebuie să aplice prezentul ghid în conformitate cu nivelul de aplicare a SREP prevăzut în Ghidul SREP al ABE și în conformitate cu modelul de angajament minim și cu cerințele de proporționalitate prevăzute în acesta.

Destinatari

7. Prezentul ghid se adresează autorităților competente, astfel cum sunt definite la articolul 4 alineatul (2) punctul (i) din Regulamentul (UE) nr. 1093/2010.

Definiții

8. Dacă nu se prevede altfel, termenii utilizați și definiți în Directiva 2013/36/UE, în Regulamentul (UE) nr. 575/2013 și în definițiile din Ghidul SREP al ABE au același înțeles în prezentul ghid. În plus, în sensul prezentului ghid, se aplică următoarele definiții:

Sisteme TIC	TIC configurată în cadrul unui mecanism sau al unei rețele de interconectare care susține operațiunile unei instituții.
Servicii asociate TIC	Serviciile furnizate de sisteme TIC unuia sau mai multor utilizatori interni sau externi. Printre exemple se numără

[2] Directiva 2013/36/UE a Parlamentului European și a Consiliului din 26 iunie 2013 cu privire la accesul la activitatea instituțiilor de credit și supravegherea prudențială a instituțiilor de credit și a firmelor de investiții, de modificare a Directivei 2002/87/CE și de abrogare a Directivelor 2006/48/CE și 2006/49/CE (1) - JO L 176, 27.6.2013.

[3] EBA/GL/2014/13

	serviciile de introducere a datelor, de stocare a datelor, de prelucrare și de raportare a datelor, însă și serviciile de monitorizare și de asistență comercială și decizională.
Risc de disponibilitate și continuitate TIC	Riscul ca performanța și disponibilitatea sistemelor și datelor TIC să fie afectate negativ, inclusiv imposibilitatea de a recupera la timp serviciile instituției din cauza unei defecțiuni la componentele hardware sau software ale TIC; vulnerabilitățile de la nivelul gestionării sistemului TIC; sau orice alt eveniment, astfel cum se prezintă mai detaliat în anexă.
Risc de securitate TIC	Riscul de acces neautorizat la sisteme și date TIC din interiorul sau din afara instituției (de exemplu, atacuri cibernetice), astfel cum se prezintă mai detaliat în anexă.
Risc de schimbare TIC	Riscul care apare ca urmare a incapacității instituției de a gestiona cu promptitudine și în mod controlat schimbările asociate sistemului TIC, în special în cazul programelor de schimbare ample și complexe, astfel cum se prezintă mai detaliat în anexă.
Riscul de integritate a datelor TIC	Riscul ca datele stocate și prelucrate prin sisteme TIC să fie incomplete, inexacte sau neconsecvente la nivelul diferitelor sisteme TIC, spre exemplu ca urmare a procedurilor de control TIC precare sau absente în diferitele faze ale ciclului de viață al datelor TIC (mai exact, proiectarea arhitecturii datelor, dezvoltarea modelului de date și/sau a dicționarelor de date, verificarea datelor introduse, controlarea și prelucrarea extracțiilor, transferurilor și prelucrării datelor, inclusiv a datelor generate), afectarea capacității unei instituții de a furniza servicii și de a prezenta informații financiare și de gestionare (a riscurilor) în mod corect și cu promptitudine, astfel cum se prezintă mai detaliat în anexă.
Risc de externalizare TIC	Riscul ca angajarea unui terț sau a unei alte entități din cadrul grupului (externalizare intragrup) pentru a furniza sisteme TIC sau servicii conexe să afecteze negativ performanța și gestionarea riscurilor în cadrul instituției, astfel cum se prezintă mai detaliat în anexă.

3. Punerea în aplicare

Data aplicării

9. Prezentul ghid se aplică începând cu 1 ianuarie 2018.

4. Cerințe pentru evaluarea riscurilor asociate TIC

Titlul 1 - Dispoziții generale

10. Autoritățile competente trebuie să evalueze riscul asociat TIC și strategia privind măsurile în materie de guvernanță și TIC în cadrul procesului SREP cu respectarea modelului de angajament minim și a criteriilor privind proporționalitatea prezentate la titlul 2 din Ghidul SREP al ABE. În mod specific, aceasta înseamnă că:

    a. frecvența evaluării riscurilor asociate TIC ar depinde de modelul de angajament minim determinat de categoria SREP în care este încadrată o instituție și de programul specific de supraveghere al acesteia; și

    b. profunzimea, detalierea și intensitatea evaluării TIC trebuie să fie proporționale cu dimensiunea, structura și mediul operațional al instituției, precum și cu natura, amploarea și complexitatea activităților sale.

11. Principiul proporționalității se aplică, pe parcursul prezentului ghid, la nivelul domeniului de aplicare, al frecvenței și al intensității angajamentului de supraveghere și al dialogului stabilit cu o instituție, precum și la nivelul așteptărilor în ceea ce privește standardele pe care trebuie să le respecte instituția.

12. Autoritățile competente s-ar putea baza pe sau ar putea lua în considerare activitatea deja desfășurată de către instituție sau de către autoritatea competentă în contextul evaluărilor altor riscuri sau elemente SREP pentru a avea o versiune actualizată a evaluării. În mod specific, atunci când efectuează evaluările prevăzute în prezentul ghid, autoritățile competente trebuie să selecteze cea mai adecvată abordare și metodologie de evaluare de supraveghere, care să fie cele mai potrivite și mai proporționale pentru instituție, iar autoritățile competente trebuie să utilizeze documentația existentă și disponibilă [de exemplu, rapoarte relevante și alte documente, reuniuni cu factori de gestionare (a riscurilor], constatări rezultate din inspecțiile la fața locului) pentru a fundamenta evaluarea autorităților competente.

13. Autoritățile competente trebuie să sintetizeze constatările evaluărilor lor asupra criteriilor prevăzute în prezentul ghid și să le utilizeze pentru a ajunge la concluzii cu privire la evaluarea elementelor SREP prevăzute în Ghidul SREP al ABE.

14. În mod specific, evaluarea strategiei privind guvernanța și TIC, care a fost efectuată în conformitate cu titlul 2 din prezentul ghid, trebuie să genereze constatări care să fundamenteze sinteza constatărilor evaluării elementului SREP privind procedurile de control intern al guvernanței și la nivelul instituției prevăzute la titlul 5 din Ghidul SREP al ABE și să se reflecte în scorul respectiv atribuit elementului SREP

respectiv. Mai mult, autoritățile competente trebuie să aibă în vedere faptul că orice impact negativ semnificativ al evaluării strategiei TIC asupra strategiei economice a instituției sau orice preocupări referitoare la faptul că s-ar putea ca instituția să nu aibă suficiente resurse și capacități TIC pentru a realiza și a susține schimbările strategice planificate importante trebuie să fundamenteze analiza modelului economic efectuată în conformitate cu titlul 4 din Ghidul SREP al ABE.

15. Rezultatul evaluării riscului TIC prevăzute în titlul 3 din prezentul ghid trebuie să fundamenteze constatările evaluării riscului operațional și trebuie să fie considerat ca un element care fundamentează scorul relevant prevăzut la titlul 6.4 din Ghidul SREP al ABE.

16. Este de precizat faptul că, deși autoritățile competente trebuie să evalueze, în general, subcategoriile de riscuri în cadrul categoriilor principale (mai exact, riscul TIC va fi evaluat în cadrul riscului operațional), în cazul în care acestea consideră că unele subcategorii sunt semnificative, acestea pot evalua individual astfel de subcategorii. În acest scop, în cazul în care riscul TIC este identificat ca fiind un risc semnificativ de către autoritatea competentă, prezentul ghid prezintă și un tabel de atribuire a scorului (tabelul 1) care trebuie utilizat pentru a atribui un scor de sine stătător subcategoriei de risc TIC cu respectarea abordării generale a atribuirii scorului pentru riscurile de capital din Ghidul SREP al ABE.

17. Pentru a-și forma o opinie cu privire la problema dacă riscul TIC trebuie considerat drept unul material și, prin urmare, dacă trebuie să se evalueze posibilitatea unui risc TIC și să se atribuie un scor în acest sens ca subcategorie individuală de risc operațional, autoritățile competente pot utiliza criteriile prevăzute la secțiunea 6.1 din Ghidul SREP al ABE.

18. Atunci când aplică prezentul ghid, autoritățile competente trebuie să aibă în vedere, dacă este cazul, lista incompletă a subcategoriilor de risc TIC și a scenariilor de risc prezentată în anexă, cu precizarea că anexa evidențiază riscurile TIC care pot genera pierderi cu un grad ridicat de severitate. Autoritățile competente ar putea exclude unele riscuri TIC incluse în taxonomie dacă nu sunt relevante pentru evaluarea lor. Se așteaptă din partea instituțiilor să întrețină propriile taxonomii ale riscurilor, în loc să utilizeze taxonomia riscului TIC prezentată în anexă.

19. În cazul în care prezentul ghid se aplică în legătură cu grupuri bancare transfrontaliere și entitățile acestora și s-a înființat un colegiu de supraveghetori, autoritățile competente implicate trebuie, în contextul colaborării lor în scopul evaluării SREP în conformitate cu secțiunea 11.1 din ghidul SREP al ABE, să coordoneze, în măsura posibilității, domeniul de aplicare exact și detaliat al fiecărei informații, în mod consecvent pentru toate entitățile din cadrul grupurilor.

Titlul 2 - Evaluarea guvernanței și strategiei instituțiilor în materie de TIC

2.1 Principii generale

20. Autoritățile competente trebuie să evalueze dacă guvernanța generală și cadrul de control intern al instituției cuprind în mod corespunzător sistemele TIC și riscurile aferente și dacă structura de conducere abordează și gestionează în mod adecvat aceste aspecte, deoarece TIC este esențială pentru funcționarea corectă a unei instituții.

21. Atunci când efectuează această evaluare, autoritățile competente trebuie să consulte cerințele și standardele privind buna guvernanță internă, măsurile de control al riscurilor prezentate în Ghidul ABE privind guvernanța internă (GL 44)[4], precum și orientările internaționale din acest domeniu în măsura în care acestea sunt aplicabile, dat fiind specificitatea sistemelor TIC și a riscurilor asociate acesteia.

22. Evaluarea din prezentul titlu nu vizează elementele specifice ale guvernanței, gestionării riscurilor și procedurilor de control aferente sistemului TIC axate pe gestionarea riscurilor TIC specifice abordate la titlul 3 din prezentul ghid, ci se orientează spre următoarele domenii:

    a. strategia TIC - dacă instituția are o strategie TIC guvernată în mod corespunzător și în conformitate cu strategia economică a instituției;

    b. guvernanța internă generală - dacă măsurile de guvernanță internă generală ale instituției sunt adecvate în raport cu sistemele TIC ale instituției; și

    c. riscul TIC în cadrul de gestionare a riscurilor al instituției - dacă un cadru de gestionare și control intern al riscurilor al instituției protejează în mod corespunzător sistemele TIC ale instituției.

23. Litera (a) menționată la punctul 22, chiar dacă oferă informații despre elementele de guvernanță a instituției, trebuie să stea la baza evaluării modelului economic abordat la titlul 4 din Ghidul SREP al ABE. Literele (b) și (c) completează evaluările tematicilor vizate la titlul 5 din Ghidul SREP al ABE, iar evaluarea descrisă în prezentul ghid trebuie să stea la baza respectivei evaluări de la titlul 5 din Ghidul SREP al ABE.

24. Rezultatul acestei evaluări trebuie, dacă este cazul, să stea la baza evaluării procesului de gestionare a riscurilor și a procedurilor de control al riscurilor din titlul 3 din prezentul ghid.

2.2 Strategia TIC

25. La această secțiune, autoritățile competente trebuie să evalueze dacă instituția a stabilit o strategie: care este supusă unei supravegheri adecvate din partea structurii de conducere a instituției; care este în

[4] Ghidul ABE privind guvernanța internă, GL 44, 27 septembrie 2011.

concordanță cu strategia economică, în special în ceea ce privește actualizarea sau planificarea TIC ori implementarea unor schimbări importante și complexe; și care susține modelul economic al instituției.

2.2.1 Dezvoltarea și adecvarea strategiei TIC

26. Autoritățile competente trebuie să evalueze dacă instituția a stabilit un cadru proporțional cu natura, amploarea și complexitatea activităților sale TIC, pentru pregătirea și dezvoltarea strategiei TIC a instituției. La efectuarea acestei evaluări, autoritățile competente trebuie să aibă în vedere dacă:

    a. organele cu funcție de conducere[5] ale liniei (liniilor) de activitate sunt implicate în mod corespunzător în stabilirea priorităților TIC strategice ale instituției și dacă, la rândul lor, organele cu funcție de conducere din cadrul funcției TIC au cunoștință despre dezvoltarea, proiectarea și lansarea de strategii și inițiative economice majore pentru a asigura alinierea permanentă a sistemelor TIC, a serviciilor TIC și a funcției TIC (mai exact, persoanele responsabile de gestionarea și valorificarea acestor sisteme și servicii), precum și a strategiei economice a instituției, și dacă sistemele TIC sunt actualizate în mod eficace;

    b. strategia TIC este documentată și susținută de planuri de implementare concrete, în special în ceea ce privește reperele și planificările de resurse importante (inclusiv resursele financiare și umane) pentru a asigura faptul că acestea sunt realiste și că permit elaborarea strategiei TIC;

    c. instituția actualizează periodic strategia sa TIC, în special atunci când schimbă strategia economică, pentru a asigura alinierea permanentă dintre TIC și obiectivele, planurile și activitățile economice pe termen mediu și lung; și

    d. structura de conducere a instituției aprobă strategia TIC și planurile de implementare și monitorizează implementarea acesteia.

2.2.2 Implementarea strategiei TIC

27. Dacă strategia TIC a instituției impune implementarea unor schimbări TIC importante și complexe, sau schimbări cu implicații semnificative pentru modelul economic al instituției, autoritățile competente trebuie să evalueze dacă instituția a stabilit un cadru de control adecvat pentru dimensiunea sa, activitățile sale TIC și pentru nivelul activităților de schimbare pentru a susține implementarea eficace a strategiei TIC a instituției. La efectuarea acestei evaluări, autoritățile competente trebuie să aibă în vedere dacă respectivul cadru de control:

    a. include procese de guvernanță (de exemplu, monitorizarea și raportarea progreselor și a bugetului) și organele relevante [de exemplu, un birou de gestionare a proiectelor (BGP), un grup coordonator TIC sau un grup echivalent] pentru a susține în mod eficace implementarea programelor strategice TIC;

    b. a definit și a alocat rolurile și responsabilitățile pentru implementarea programelor strategice TIC, acordându-se o atenție deosebită experienței părților interesate cheie în organizarea,

[5] Organele cu funcție de conducere și structura de conducere definite la articolul 3 alineatul (7) „structură de conducere” și la articolul 3 alineatul (9) „organe cu funcție de conducere” din Directiva 2013/36/UE din 26 iunie 2013.

coordonarea și monitorizarea schimbărilor TIC importante și complexe și gestionării impacturilor mai ample la nivel organizațional și uman (de exemplu, gestionarea rezistenței la schimbare, formare, comunicare).

c. angajează funcțiile de control și de audit intern independente să ofere asigurarea că au fost identificate, evaluate și atenuate în mod eficace riscurile asociate implementării strategiei TIC și că acel cadru de guvernanță instituit pentru implementarea strategiei TIC este eficace; și

d. cuprinde un proces de planificare și de revizuire a planificării care oferă flexibilitate pentru reactivitate la aspectele importante identificate (de exemplu, probleme sau întârzieri ivite la nivelul implementării) sau la evoluții externe (de exemplu, schimbări importante produse în mediul economic, probleme tehnologice sau inovații) pentru a asigura o adaptare oportună a planului strategic de implementare.

2.3 Cadrul general de guvernanță internă

28. În conformitate cu titlul 5 din Ghidul SREP al ABE, autoritățile competente trebuie să evalueze dacă instituția are o structură corporativă adecvată și transparentă care este „corespunzătoare”, precum și dacă a implementat măsuri de guvernanță potrivite. În mod specific cu privire la sistemele TIC și în conformitate cu Ghidul ABE privind guvernanța internă, această evaluare trebuie să includă o evaluare a problemei dacă instituția demonstrează:

    a. faptul că deține o structură organizațională robustă și transparentă cu responsabilități clare privind TIC, care să includă structura de conducere și comitetele sale, precum și că persoanele responsabile cheie pentru TIC [de exemplu, responsabilul pentru informații (CIO), directorul general administrativ (COO) sau un rol echivalent] au acces indirect sau direct corespunzător la structura de conducere pentru a asigura raportarea, discutarea și deciderea la nivel corespunzător asupra informațiilor sau problemelor importante legate de TIC la nivelul structurii de conducere; și

    b. că structura de conducere cunoaște și abordează riscurile asociate TIC;

29. În continuarea secțiunii 5.2 din Ghidul SREP al ABE, autoritățile competente trebuie să evalueze dacă politica și strategia instituției de externalizare a TIC au în vedere, după caz, impactul externalizării TIC asupra activității și a modelului economic al instituției.

2.4 Riscul TIC în cadrul de gestionare a riscurilor instituției

30. Atunci când evaluează procedurile de control interne și de gestionare a riscurilor la nivelul instituției ale instituției, astfel cum sunt prevăzute la titlul 5 din Ghidul SREP al ABE, autoritățile competente trebuie să aibă în vedere dacă cadrul de control intern și de gestionare a riscurilor al instituției protejează în mod corespunzător sistemele TIC ale instituției proporțional cu dimensiunea și activitățile instituției, precum și cu profilul de risc TIC prevăzut la titlul 3. În special, autoritățile competente trebuie să stabilească dacă:

a. apetitul la risc și ICAAP cuprind riscurile TIC în categoria mai amplă a riscului operațional pentru definirea strategiei generale privind riscurile și stabilirea capitalului intern; și

b. riscurile TIC sunt incluse în domeniul de aplicare al cadrelor de control intern și de gestionare a riscurilor la nivelul instituției.

31. Autoritățile competente trebuie să efectueze analiza de la litera (a) de mai sus ținând cont de scenariul preconizat și de cel opus, de exemplu, scenariile incluse în verificarea specifică instituției sau în simularea de criză de supraveghere.

32. Având în vedere în mod specific litera (b), autoritățile competente trebuie să evalueze dacă funcțiile de control și audit intern independente detaliate la punctul (104) literele (a) și (d) și la punctul (105) literele (a) și (c) din Ghidul SREP al ABE sunt adecvate pentru a asigura un nivel suficient de independență între TIC și funcțiile de control și audit, date fiind dimensiunea și profilul de risc TIC al instituției.

2.5 Sinteza constatărilor

33. Aceste rezultate trebuie reflectate în sinteza constatărilor de la titlul 5 din Ghidul SREP al ABE și trebuie să facă parte din acțiunea de atribuire a scorului conform considerațiilor din tabelul 3 din Ghidul SREP al ABE.

34. Pentru evaluarea strategiei TIC, trebuie avute în vedere următoarele puncte atunci când se încheie evaluarea de mai sus:

a. dacă autoritățile competente ajung la concluzia că cadrul de guvernanță al instituției este inadecvat pentru dezvoltarea și implementarea strategiei TIC a instituției menționate la punctul 2.2, atunci aceasta trebuie să fundamenteze evaluarea guvernanței interne a instituției de la punctul 87 litera (a) de la titlul 5 din Ghidul SREP al ABE;

b. dacă, în urma evaluărilor de la punctul 2.2 de mai sus, autoritățile competente ajung la concluzia că ar exista o neconcordanță semnificativă între strategia TIC și strategia economică, ceea ce ar putea avea un impact negativ semnificativ asupra activității și/sau a obiectivelor financiare pe termen lung ale instituției, a durabilității instituției și/sau a modelului economic, sau asupra domeniilor/liniilor de activitate ale instituției care au fost stabilite ca fiind cele mai semnificative la punctul (62) litera (a) din Ghidul SREP al ABE, atunci aceasta trebuie să fundamenteze evaluarea modelului economic de la punctul 70 literele (b) și (c) de la titlul 4 din Ghidul SREP; și

c. dacă, în urma evaluărilor de la punctul 2.2 de mai sus, autoritățile competente ajung la concluzia că este posibil ca instituția să nu aibă suficiente resurse TIC și capacități de implementare a TIC pentru realizarea și susținerea schimbărilor strategice planificate importante, aceasta trebuie să fundamenteze evaluarea modelului economic de la punctul 70 litera (b) de la titlul 4 din Ghidul SREP al ABE.

Titlul 3 - Evaluarea procedurilor de control și a expunerilor la riscurile asociate TIC ale instituțiilor

3.1 Considerații generale

35. Autoritățile competente trebuie să evalueze dacă instituția și-a identificat, evaluat și atenuat în mod corespunzător riscurile asociate TIC. Acest proces trebuie să facă parte din cadrul de gestionare a riscului operațional și să fie congruent cu abordarea care aplică riscul operațional.

36. Autoritățile competente trebuie să identifice mai întâi riscurile TIC inerente semnificative la care este sau ar putea fi expusă instituția, apoi să efectueze o analiză a eficacității cadrului de gestionare a riscurilor TIC, a procedurilor și a măsurilor de control ale instituției pentru atenuarea acestor riscuri. Rezultatul evaluării trebuie să se reflecte într-o sinteză a constatărilor care stă la baza atribuirii scorului de risc operațional din Ghidul SREP. În cazul în care se consideră că riscul TIC este semnificativ, iar autoritățile competente doresc să atribuie un scor individual, trebuie să se utilizeze tabelul 1 pentru atribuirea unui scor ca risc secundar al riscului operațional.

37. Atunci când desfășoară evaluarea prevăzută la prezentul titlu, autoritățile competente trebuie să utilizeze toate sursele de informații disponibile menționate la punctul 127 de la titlul 6 din Ghidul SREP al ABE, de exemplu, activitățile de gestionare a riscurilor, raportarea și rezultatele, ca bază pentru identificarea priorităților de evaluare de supraveghere a acestora. Autoritățile competente trebuie să utilizeze și alte surse de informații pentru efectuarea acestei analize, inclusiv următoarele, după caz:

    a. autoevaluări ale riscurilor TIC și ale procedurilor de control al riscurilor (dacă sunt prevăzute în informațiile ICAAP);
    b. informații administrative (IA) privind riscul TIC transmise structurii de conducere a instituției, de exemplu, raportarea riscului TIC periodică și determinată de incidente (inclusiv în baza de date a pierderilor operaționale), datele privind expunerea la riscul TIC de la funcția de gestionare a riscurilor a instituției;
    c. constatările desprinse din auditul intern și extern în legătură cu TIC, care au fost raportate comitetului de audit al instituției.

3.2 Identificarea riscurilor TIC semnificative

38. Autoritățile competente trebuie să identifice riscurile TIC semnificative la care este expusă sau este susceptibilă de a fi expusă instituția prin etapele de mai jos.

3.2.1 Analiza profilului de risc TIC al instituției

39. Atunci când analizează profilul de risc TIC al instituției, autoritățile competente trebuie să aibă în vedere toate informațiile relevante despre expunerile la riscul TIC ale instituției, inclusiv informațiile de la punctul 37 și deficiențele sau punctele slabe semnificative identificate la nivelul organizării TIC și al procedurilor de control de la nivelul instituției de la titlul 2 din prezentul ghid și, după caz, să analizeze aceste informații în mod proporțional. În cadrul acestei analize, autoritățile competente trebuie să aibă în vedere:

    a. eventualul impact al unei întreruperi semnificative asupra sistemelor TIC și a sistemului financiar al instituției la nivel intern sau internațional;
    b. dacă instituția este susceptibilă de a fi expusă riscului de securitate TIC sau riscurilor de disponibilitate și continuitate TIC din cauza dependențelor de Internet, adoptării la nivel înalt a soluțiilor TIC inovatoare sau a altor canale de distribuție economică ce ar putea să crească susceptibilitatea ca instituția să fie ținta atacurilor cibernetice;
    c. dacă instituția este susceptibilă de a fi mai expusă riscurilor de securitate TIC, riscurilor de disponibilitate și continuitate TIC, riscurilor de integritate a datelor sau riscurilor de schimbare TIC din cauza complexității (de exemplu, ca urmare a fuziunilor sau a achizițiilor) sau a învechirii sistemelor sale TIC;
    d. dacă instituția implementează schimbări semnificative aduse sistemelor TIC și/sau funcției TIC (de exemplu, ca urmare a fuziunilor, a achizițiilor, a cesionării sau a înlocuirii sistemelor sale TIC de bază), care ar putea avea un impact negativ asupra stabilității sau funcționării ordonate a sistemelor TIC și care pot genera riscuri semnificative la nivelul disponibilității și continuității TIC, riscuri de securitate TIC, riscuri de schimbare TIC sau riscuri de integritate a datelor TIC;
    e. dacă instituția a externalizat servicii sau sisteme TIC în cadrul sau în afara grupului, ceea ce este susceptibil de a o expune unor riscuri semnificative de externalizare TIC;
    f. dacă instituția implementează măsuri agresive de reducere a costurilor TIC, care ar putea determina reducerea investițiilor și resurselor TIC, precum și a expertizei IT necesare, și care pot crește expunerea la toate tipurile de risc TIC din cadrul taxonomiei;
    g. dacă localizarea operațiunilor/centrelor de date TIC importante (de exemplu, regiuni, țări) este susceptibilă de a expune instituția unor calamități naturale (de exemplu, inundații, cutremure), instabilității politice sau conflictelor de muncă și perturbărilor civile, ceea ce poate duce la creșterea semnificativă a riscurilor de disponibilitate și continuitate TIC și a riscurilor de securitate TIC.

3.2.2 Analiza sistemelor și serviciilor TIC esențiale

40. În cadrul procesului de identificare a riscurilor TIC care ar putea avea un impact prudențial semnificativ asupra instituției, autoritățile competente trebuie să analizeze documentația primită din partea instituției și să își formeze o opinie asupra sistemelor și serviciilor TIC care sunt vitale pentru o funcționare, disponibilitate, continuitate și securitate adecvată a activităților esențiale ale instituției.

41. În acest scop, autoritățile competente trebuie să analizeze metodologia și procesele aplicate de către instituție pentru identificarea sistemelor și serviciilor TIC care sunt vitale, ținând cont de faptul că unele

sisteme și servicii TIC ar putea fi considerate vitale de către instituție din perspectiva continuității și disponibilității economice, precum și din perspectiva securității (de exemplu, prevenirea datelor) și/sau a confidențialității (de exemplu, date confidențiale). Atunci când efectuează analiza, autoritățile competente trebuie să țină cont de faptul că sistemele și serviciile vitale TIC trebuie să îndeplinească cel puțin una dintre următoarele condiții:

a. susțin operațiunile economice și canalele de distribuție (de exemplu, bancomate, Internet și servicii bancare mobile) ale instituției;

b. susțin procesele de guvernanță și funcțiile corporative esențiale, inclusiv gestionarea riscurilor (de exemplu, sisteme de gestionare a riscurilor și a trezoreriei);

c. intră sub incidența cerințelor legale și de reglementare speciale (dacă există) care impun cerințe mai înalte privind disponibilitatea, reziliența, confidențialitatea sau securitatea [de exemplu, legislația privind protecția datelor sau posibile „obiective privind timpul de recuperare” (OTR, timpul maxim în care un sistem sau un proces trebuie să fie restabilit după un incident) și „obiectivul privind punctul de recuperare” (OPR, perioada maximă de timp în care datele se pot pierde în cazul unui incident) pentru unele servicii importante din punct de vedere sistemic (dacă există și dacă este cazul)];

d. prelucrează sau stochează date confidențiale sau sensibile a căror accesare neautorizată ar putea produce un impact semnificativ asupra reputației instituției, a rezultatelor financiare sau a solidității și continuității activității sale (de exemplu, baze de date cu date sensibile despre clienți); și/sau

e. asigură funcționalități de bază care sunt esențiale pentru funcționarea adecvată a instituției (de exemplu, servicii de telecomunicații și de conectivitate, servicii de securitate TIC și cibernetică).

3.2.3 Identificarea riscurilor TIC semnificative asociate sistemelor și serviciilor TIC esențiale

42. Ținând cont de analizele efectuate asupra profilului de risc TIC al instituției și a sistemelor și serviciilor esențiale TIC de mai sus, autoritățile competente trebuie să își formeze o opinie cu privire la riscurile TIC semnificative care, conform aprecierii lor în materie de supraveghere, pot avea un impact prudențial semnificativ asupra sistemelor și serviciilor TIC esențiale ale instituției.

43. Atunci când evaluează un eventual impact al riscurilor TIC asupra sistemelor și serviciilor TIC esențiale ale unei instituții, autoritățile competente trebuie să aibă în vedere:

a. impactul financiar, inclusiv, dar nu numai, pierderea de fonduri sau active, o eventuală compensare a clienților, cheltuieli de judecată și de remediere, daune contractuale, venituri pierdute;

b. eventualitatea întreruperii activității, având în vedere, dar nu numai, importanța serviciilor financiare afectate; numărul de clienți și/sau sucursale și angajați care ar putea fi afectați;

c. un eventual impact asupra instituției sub aspectul reputației în funcție de importanța serviciului bancar sau a activității operaționale afectate (de exemplu, furtul de date despre clienți); profilul/vizibilitatea sistemelor și serviciilor TIC afectate (de exemplu, sisteme bancare mobile sau online, puncte de vânzare, bancomate sau sisteme de plată);

d. impactul de reglementare, inclusiv eventualitatea cenzurării publice de către factorul de reglementare, a aplicării de amenzi sau chiar a variației permisiunilor;

e. impactul strategic asupra instituției, spre exemplu dacă produsul strategic sau planurile economice sunt compromise sau furate.

44. Autoritățile competente trebuie să cartografieze apoi riscurile TIC identificate, care sunt identificate ca fiind semnificative, și să le clasifice în următoarele categorii de riscuri TIC, pentru care se prezintă descrieri suplimentare ale riscurilor și exemple în anexă. Autoritățile competente trebuie să analizeze riscurile TIC din anexă în cadrul evaluării de la titlul 3:

a. Risc de disponibilitate și continuitate TIC
b. Risc de securitate TIC
c. Risc de schimbare TIC
d. Riscul de integritate a datelor TIC
e. Risc de externalizare TIC

Cartografierea este prevăzută a ajuta autoritățile competente să stabilească riscurile semnificative (dacă există) și, prin urmare, trebuie supusă unei analize mai stricte și/sau mai aprofundate în următoarele etape de evaluare.

3.3 Evaluarea procedurilor de control pentru reducerea riscurilor semnificative TIC

45. Pentru a evalua expunerea instituției la riscul rezidual TIC, autoritățile competente trebuie să analizeze modul în care instituția identifică, monitorizează, evaluează și atenuează riscurile semnificative identificate de către autoritățile competente în evaluarea de mai sus.

46. În acest scop, în cazul riscurilor TIC semnificative identificate, autoritățile competente trebuie să analizeze următoarele elemente aplicabile:

a. politica și procesele de gestionare a riscurilor TIC, precum și pragurile de toleranță la risc;

b. cadrul de gestionare și supraveghere organizațională;

c. acoperirea acțiunii de audit intern și constatările desprinse ca urmare a acesteia; și

d. procedurile de control al riscurilor TIC specifice riscului TIC semnificativ identificat.

47. Evaluarea trebuie să țină cont de rezultatul analizei cadrului general de gestionare și control intern al riscurilor prevăzut la titlul 5 din Ghidul SREP al ABE, precum și al analizei guvernanței și strategiei instituției, care sunt abordate la titlul 2 din prezentul ghid, deoarece deficiențele semnificative identificate în aceste domenii ar putea influența capacitatea instituției de a gestiona și a atenua expunerile la riscul TIC ale acesteia. Dacă este cazul, autoritățile competente trebuie să utilizeze și sursele de informații de la punctul 37 din prezentul ghid.

48. Autoritățile competente trebuie să parcurgă următoarele etape de evaluare proporțional cu natura, amploarea și complexitatea activităților instituției și cu aplicarea unei analize de supraveghere adecvate pentru profilul de risc TIC al instituției.

3.3.1 Politica și procesele de gestionare a riscurilor TIC, precum și pragurile de toleranță la risc

49. Autoritățile competente trebuie să analizeze dacă instituția a instituit politici și procese adecvate de gestionare a riscurilor, precum și praguri de toleranță pentru riscurile TIC semnificative identificate. Acestea pot fi incluse în cadrul de gestionare a riscurilor operaționale sau într-un document separat. În scopul acestei evaluări, autoritățile competente trebuie să țină cont de următoarele:

    a. dacă politica de gestionare a riscurilor este formalizată și aprobată de către structura de conducere și dacă aceasta cuprinde orientări suficiente cu privire la apetitul la riscul TIC al instituției și la principalele obiective de gestionare a riscurilor TIC urmărite și/sau la pragurile de toleranță la riscul TIC aplicate; dacă politica relevantă de gestionare a riscurilor TIC trebuie comunicată, de asemenea, tuturor părților interesate relevante;

    b. dacă politica aplicabilă cuprinde toate elementele semnificative pentru gestionarea riscurilor TIC semnificative identificate;

    c. instituția a implementat un proces și proceduri aferente pentru identificarea (de exemplu, „autoevaluări privind controlarea riscurilor” (ACR), analiza scenariilor de risc) și monitorizarea riscurilor TIC semnificative implicate; și

    d. dacă instituția a instituit un sistem de raportare pentru gestionarea riscurilor TIC, care oferă informații prompte organelor cu funcție de conducere și structurii de conducere și care permite acestor organe și/sau acestei structuri să evalueze și să monitorizeze dacă planurile și măsurile de atenuare a riscurilor TIC ale instituției sunt în concordanță cu apetitul la risc și/sau pragurile de toleranță aprobate (după caz), precum și să monitorizeze schimbările produse la nivelul riscurilor TIC semnificative.

3.3.2 Cadrul de gestionare și supraveghere organizațională

50. Autoritățile competente trebuie să evalueze modul în care rolurile și responsabilitățile de gestionare a riscurilor aplicabile sunt încorporate și integrate în organizarea internă pentru gestionarea și supravegherea riscurilor TIC semnificative identificate. În acest sens, autoritățile competente trebuie să evalueze dacă instituția demonstrează următoarele:

    a. existența unor roluri și responsabilități clare pentru identificarea, evaluarea, monitorizarea, atenuarea, raportarea și supravegherea riscului TIC semnificativ implicat;

    b. dacă responsabilitățile și rolurile privind riscurile sunt comunicate în mod clar, alocate și integrate în toate părțile (de exemplu, linii de activitate, IT) și procesele relevante ale organizației, inclusiv rolurile și responsabilitățile privind colectarea și agregarea informațiilor despre riscuri și raportarea acestora către organele cu funcție de conducere și/sau structura de conducere;

    c. dacă activitățile de gestionare a riscurilor TIC sunt desfășurate cu resurse umane și tehnice suficiente și corespunzătoare calitativ. Pentru a evalua credibilitatea planurilor de atenuare

a riscurilor aplicabile, autoritățile competente trebuie să analizeze și dacă instituția a alocat suficiente fonduri bugetare și/sau alte resurse necesare pentru punerea în aplicare a acestora;

d. faptul că structura de conducere a întreprins acțiuni de continuare și de răspuns adecvate cu privire la constatări importante ale funcțiilor de control independente referitoare la riscul (riscurile) TIC, ținând cont de o posibilă delegare a unor aspecte către un comitet, dacă acesta există; și
e. dacă excepțiile de la normele și politicile TIC aplicabile sunt înregistrate și supuse unei analize documentare și raportări din partea unei funcții de control independente, cu axarea pe riscurile conexe.

3.3.3 Acoperirea acțiunii de audit intern și constatările desprinse ca urmare a acesteia

51. Autoritățile competente trebuie să verifice dacă funcția de audit intern este eficace în ceea ce privește auditarea cadrului de control al riscurilor TIC, analizând dacă:

a. cadrul de control al riscurilor TIC este auditat la calitatea, profunzimea și frecvența impusă și proporțional cu dimensiunea, activitățile și profilul de risc TIC al instituției;

b. planul de audit include acțiuni de audit privind riscurile TIC esențiale identificate de către instituție;

c. constatările importante ale auditului cu privire la TIC, inclusiv acțiunile convenite, sunt raportate structurii de conducere;

d. constatările auditului cu privire la TIC, inclusiv acțiunile convenite, sunt urmărite și se analizează periodic rapoartele privind progresele înregistrate de către organele cu funcție de conducere și/sau comitetul de audit.

3.3.4 Procedurile de control al riscurilor TIC specifice riscurilor TIC semnificative identificate

52. În cazul riscurilor TIC semnificative identificate, autoritățile competente trebuie să evalueze dacă instituția a stabilit proceduri de control specifice pentru abordarea acestor riscuri. În secțiunile următoare se prezintă o listă incompletă a procedurilor de control specifice care să fie luate în considerare atunci când se evaluează riscurile semnificative identificate la punctul 3.2.3, care au fost cartografiate și clasificate în următoarele categorii de riscuri TIC:

a. riscuri de disponibilitate și continuitate TIC;
b. riscuri de securitate TIC;
c. riscuri de schimbare TIC;
d. riscuri de integritate a datelor TIC;
e. riscuri de externalizare TIC.

(a) Proceduri de control pentru gestionarea riscurilor de disponibilitate și continuitate TIC semnificative

53. În plus față de cerințele din Ghidul SREP al ABE (punctele 279-281), autoritățile competente trebuie să evalueze dacă instituția a stabilit un cadru adecvat pentru identificarea, înțelegerea, măsurarea și atenuarea riscurilor de disponibilitate și continuitate TIC.

54. În scopul acestei evaluări, autoritățile competente trebuie să aibă în vedere, în mod specific, dacă în respectivul cadru:

a. se identifică procesele TIC esențiale și sistemele TIC de susținere relevante care trebuie să facă parte din planurile de reziliență și continuitate economică, alături de:

   i. o analiză cuprinzătoare a dependențelor dintre procesele economice și sistemele de susținere esențiale;

   ii. stabilirea obiectivelor de recuperare pentru susținerea sistemelor TIC (de exemplu, stabilite, de regulă, prin intermediul activității și/sau regulamente la nivelul OTR și OPR);

   iii. o planificare de urgență adecvată pentru a asigura disponibilitatea, continuitatea și recuperarea sistemelor și serviciilor TIC esențiale în vederea reducerii la minim a întreruperii operațiunilor instituției în limitele acceptabile.

b. există politici și standarde privind reziliența economică și mediul de control al continuității, precum și proceduri de control operațional care includ:

   i. măsuri pentru a evita ca un singur scenariu, incident sau dezastru să aibă un impact asupra sistemelor de dezvoltare și recuperare TIC;

   ii. proceduri de rezervă și de recuperare a sistemului TIC pentru software și date esențiale, care să asigure stocarea acestor rezerve într-o locație sigură și suficient de îndepărtată încât un incident sau un dezastru să nu poată distruge sau corupe aceste date esențiale;

   iii. soluții de monitorizare pentru detectarea promptă a incidentelor legate de disponibilitatea și continuitatea TIC;

   iv. un proces documentat de gestionare și escaladare a incidentelor, care să ofere și îndrumări cu privire la diferitele roluri și responsabilități de gestionare și escaladare a incidentelor, membrii comitetului (comitetelor) de criză și lanțul de comandă în caz de urgență;

   v. măsuri fizice pentru a proteja infrastructura TIC esențială a instituției (de exemplu, centre de date) de riscurile de mediu (de exemplu, inundații și alte calamități naturale) și a asigura un mediu de funcționare adecvat pentru sistemele TIC (de exemplu, aer condiționat);

   vi. procese, roluri și responsabilități pentru a asigura faptul că soluțiile și planurile de reziliență și continuitate a activității adecvate acoperă, de asemenea, sistemele și serviciile TIC externalizate;

   vii. soluții de planificare și monitorizare a performanței și capacității TIC pentru sisteme și servicii TIC esențiale cu cerințe stabilite privind disponibilitatea, pentru a depista cu promptitudine constrângerile importante la nivel de performanță și capacitate;

   viii. soluții pentru a proteja activități sau servicii de Internet esențiale (de exemplu, servicii bancare electronice), dacă este necesar și adecvat, de blocarea accesului și alte atacuri cibernetice de pe Internet, care vizează împiedicarea sau perturbarea accesului la aceste activități și servicii.

c. se testează soluții de disponibilitate și continuitate TIC în contextul unei serii de scenarii realiste, inclusiv atacuri cibernetice, teste de siguranță și teste pentru salvare de rezervă în cazul software-ului și al datelor esențiale care:

   i. sunt planificate, formalizate și documentate, iar rezultatele testelor sunt utilizate pentru a crește eficacitatea soluțiilor de disponibilitate și continuitate TIC;

   ii. includ părți interesate și funcții din cadrul organizației, cum ar fi sistemul de administrare a liniilor de activitate care include echipe de continuitate a activității și de intervenție în caz de incidente sau criză, precum și părți interesate externe relevante din ecosistem;

   iii. structura de conducere și organele cu funcție de conducere sunt implicate în mod corespunzător (de exemplu, în cadrul echipelor de gestionare a crizelor) și sunt informate cu privire la rezultatele testelor.

(b) Proceduri de control pentru gestionarea riscurilor de securitate TIC semnificative

55. Autoritățile competente trebuie să evalueze dacă instituția a stabilit un cadru eficace pentru identificarea, înțelegerea, măsurarea și atenuarea riscului de securitate TIC. În scopul acestei evaluări, autoritățile competente trebuie să aibă în vedere, în mod specific, dacă în respectivul cadru sunt prevăzute următoarele:

a. roluri și responsabilități definite clar cu privire la:
   i. persoana (persoanele) și/sau comitetele responsabile și/sau răspunzătoare pentru gestionarea curentă a securității TIC și elaborarea de politici generale de securitate TIC, acordându-se atenție independenței lor necesare;
   ii. proiectarea, implementarea, gestionarea și monitorizarea procedurilor de control privind securitatea TIC;
   iii. protecția sistemelor și serviciilor TIC esențiale, spre exemplu prin adoptarea unui proces de evaluare a vulnerabilității, gestionarea patch-ului software, protecția punctului final (de exemplu, un virus malware), instrumente de detectare și prevenire a intrușilor;
   iv. monitorizarea, clasificarea și abordarea incidentelor de securitate TIC externe sau interne; inclusiv intervenția în caz de incidente și relansarea și recuperarea sistemelor și serviciilor TIC;
   v. evaluări regulate și proactive ale amenințărilor pentru menținerea de proceduri de control al securității adecvate.

b. o politică de securitate TIC care ia în considerare și, după caz, respectă standarde și principii de securitate TIC recunoscute la nivel internațional (de exemplu, „principiul celui mai mic privilegiu”, adică limitarea accesului la nivelul minim care va permite funcționarea normală pentru gestionarea dreptului de acces, și principiul „apărării în profunzime”, adică mecanismele de securitate stratificate cresc nivelul de securitate al sistemului în ansamblu pentru proiectarea arhitecturii de securitate);

c. un proces pentru identificarea sistemelor și serviciilor TIC și cerințe proporționale privind securitatea care să reflecte un eventual risc de fraudă și/sau posibile utilizări greșite și/sau abuzuri de date confidențiale, precum și așteptări documentate în materie de securitate care să fie

respectate pentru aceste sisteme, servicii și date TIC identificate, în concordanță cu toleranța la risc a instituției și cu monitorizarea implementării corecte a acestora;

d. un proces documentat de gestionare și escaladare a incidentelor legate de securitate, care să ofere îndrumări cu privire la diferitele roluri și responsabilități de gestionare și escaladare a incidentelor, membrii comitetului (comitetelor) de criză și lanțul de comandă în cazuri de urgență de securitate;

e. funcția de înregistrare a utilizatorilor și a activității administrative pentru a permite monitorizarea eficace și detectarea și intervenția promptă în cazul unei activități neautorizate; asistarea la sau desfășurarea de anchete criminalistice cu privire la incidente de securitate. Instituția trebuie să instituie politici de înregistrare prin care să se stabilească tipuri corespunzătoare de registre de evidență care să fie păstrate, precum și perioada de păstrare a acestora;

f. campanii sau inițiative de sensibilizare și informare pentru a informa toate nivelurile din cadrul instituției cu privire la utilizarea sigură și protecția sistemelor TIC ale instituției, precum și la principalele riscuri de securitate TIC (și alte riscuri) pe care trebuie să le cunoască acestea, în special cu privire la amenințările cibernetice existente și cele evolutive (de exemplu, viruși informatici, posibile abuzuri sau atacuri interne sau externe, atacuri cibernetice) și rolul acestora în reducerea breșelor de securitate;

g. măsuri de securitate fizice adecvate (de exemplu, sisteme CCTV, alarme antifurt, uși de securitate) pentru prevenirea accesului fizic neautorizat la sisteme TIC esențiale și sensibile (de exemplu, centre de date);

h. măsuri pentru protejarea sistemelor TIC de atacurile de pe Internet (de exemplu, atacuri cibernetice) sau alte rețele externe (de exemplu, legături de telecomunicații tradiționale sau legături cu parteneri de încredere). Autoritățile competente trebuie să analizeze dacă în cadrul instituției sunt avute în vedere următoarele:

    i. un proces și soluții pentru întreținerea unui inventar de date complet și actualizat și evidența tuturor punctelor de conectare la rețea cu orientare spre exterior (de exemplu, site-uri, aplicații pe Internet, WIFI, acces la distanță) prin care terții ar putea să spargă sistemele TIC interne.

    ii. măsuri de securitate gestionate și monitorizate îndeaproape (de exemplu, sisteme de tip firewall, servere proxy, sisteme de retransmitere a mesajelor, sisteme de scanare antivirus și de conținut) pentru a securiza traficul care intră și care iese din rețea (de exemplu, mesajele electronice) și conexiunile la rețea cu orientare spre exterior prin care terții ar putea să spargă sistemele TIC interne;

    iii. procese și soluții pentru securizarea site-urilor și aplicațiilor care pot fi atacate în mod direct de pe Internet și/sau din exterior și care pot constitui drept puncte de intrare în sistemele TIC interne. În general, acestea includ o combinație de practici de dezvoltare sigure recunoscute, practici de scanare a vulnerabilității și consolidare a sistemelor TIC și/sau implementarea de soluții de securitate suplimentare precum, de exemplu, sistemele de tip firewall și/sau detectarea intrușilor (IDS) și/sau de prevenire a intrușilor;

    iv. teste periodice de pătrundere în sistemul de securitate pentru a evalua eficacitatea măsurilor și proceselor de securitate TIC interne și cibernetice implementate. Aceste teste trebuie efectuate de către personal și/sau experți externi având expertiza necesară, iar

rezultatele testelor documentată și concluziile raportate organelor cu funcție de conducere și/sau structurii de conducere. Dacă este necesar sau dacă este cazul, instituția trebuie să identifice în urma acestor teste punctele care necesită îmbunătățiri suplimentare la nivelul procedurilor de control și al proceselor de securitate și/sau să obțină asigurarea cu privire la eficacitatea acestora.

(c) Proceduri de control pentru gestionarea riscurilor de schimbare TIC semnificative

56. Autoritățile competente trebuie să evalueze dacă instituția a stabilit un cadru eficace pentru identificarea, înțelegerea, măsurarea și atenuarea riscului de schimbare TIC proporțional cu natura, amploarea și complexitatea activităților instituției, precum și cu profilul de risc TIC al instituției. Cadrul instituției trebuie să cuprindă riscurile asociate dezvoltării, testării și aprobării schimbărilor produse la nivelul sistemelor TIC, inclusiv cele asociate dezvoltării sau schimbării software-ului, înainte ca acestea să fie transmise către mediul de producție și să asigure o gestionare adecvată a ciclului de viață TIC. În scopul acestei evaluări, autoritățile competente trebuie să aibă în vedere, în mod specific, dacă în respectivul cadru sunt prevăzute următoarele:

a. procese documentate pentru gestionarea și controlarea schimbărilor aduse sistemelor (de exemplu, configurare și gestionarea patch-ului) și datelor TIC (de exemplu, rezolvarea erorilor de tip bug sau corecțiile de date), asigurarea implicării adecvate a gestionării riscurilor TIC în cazul schimbărilor TIC importante care ar putea avea un impact semnificativ asupra profilului de risc și a expunerii instituției;

b. specificații privind separarea impusă a sarcinilor în diferitele etape ale proceselor de schimbare TIC implementate (de exemplu, proiectarea și dezvoltarea de soluții, testarea și aprobarea de software nou și/sau schimbări, migrarea și implementarea în mediul de producție și rezolvarea erorilor de tip bug), cu axare pe soluțiile implementate și separarea sarcinilor pentru gestionarea și controlarea schimbărilor aduse sistemelor și datelor TIC de producție de către personalul TIC (de exemplu, dezvoltatori, administratori de sistem TIC, administratori de baze de date) sau orice altă parte (de exemplu, utilizatori economici, furnizori de date);

c. medii de testare care reflectă în mod corespunzător medii de producție;

d. un inventar al activelor care să cuprindă aplicațiile și sistemele TIC existente în mediul de producție, precum și în mediul de testare și dezvoltare, pentru ca schimbările necesare (de exemplu, actualizări sau îmbunătățiri ale versiunilor, aplicarea de coduri patch în sisteme, schimbări de configurații) să fie gestionate, implementate și monitorizate în mod corespunzător în cazul sistemelor TIC în cauză;

e. un proces pentru monitorizarea și gestionarea ciclului de viață al sistemelor TIC utilizate pentru a asigura faptul că acestea respectă și susțin în continuare cerințele efective de gestionare a activității și a riscurilor și pentru a obține certitudinea că soluțiile și sistemele TIC utilizate sunt susținute în continuare de către furnizorii acestora; și că acesta este însoțit de proceduri adecvate pentru ciclul de viață al procesului de dezvoltare a software-ului (SDLC);

f. un sistem de verificare a codului sursă al software-ului și proceduri adecvate de prevenire a schimbărilor neautorizate asupra codului sursă al software-ului elaborat la nivel intern;

g. un proces pentru realizarea unei verificări de securitate și vulnerabilitate asupra sistemelor TIC și programelor software noi sau modificate semnificativ înainte de a le lansa în producție și a le expune unor posibile atacuri cibernetice;

h. un proces și soluții pentru prevenirea divulgării neautorizate sau neintenționate a datelor confidențiale la înlocuirea, arhivarea, eliminarea sau distrugerea sistemelor TIC;

i. un proces independent de analiză și validare pentru reducerea riscurilor de eroare umană atunci când se aduc schimbări la nivelul sistemelor TIC, care ar putea avea un efect negativ important asupra disponibilității, continuității sau securității instituției (de exemplu, schimbări importante aduse configurației firewall), sau la nivelul securității instituției (de exemplu, schimbări aduse aplicațiilor de tip firewall).

(d) Proceduri de control pentru gestionarea riscurilor de integritate a datelor TIC semnificative

57. Autoritățile competente trebuie să evalueze dacă instituția a stabilit un cadru eficace pentru identificarea, înțelegerea, măsurarea și atenuarea riscului de integritate a datelor TIC proporțional cu natura, amploarea și complexitatea activităților instituției, precum și cu profilul de risc TIC al instituției. Cadrul instituției trebuie să aibă în vedere riscurile asociate păstrării integrității datelor stocate în și prelucrate prin sistemele TIC. În scopul acestei evaluări, autoritățile competente trebuie să aibă în vedere, în mod specific, dacă în respectivul cadru sunt prevăzute următoarele:

a. o politică ce definește rolurile și responsabilitățile de gestionare a integrității datelor din sistemele TIC (de exemplu, arhitectul de date, responsabili de date [6], custozi de date [7], posesori/supraveghetori de date[8]) și care oferă îndrumări cu privire la datele care sunt esențiale din perspectiva integrității datelor și care trebuie supuse unor proceduri de control TIC specifice (de exemplu, proceduri automatizate de control pentru validarea datelor introduse, proceduri de control al transferului de date, reconcilieri etc.) sau analize (de exemplu, o verificare a compatibilității cu arhitectura datelor) în diferitele faze ale ciclului de viață al datelor TIC;

b. o arhitectură documentată a datelor, un model și/sau dicționar de date, care se validează de către societate și părțile interesate informatice relevante pentru a susține consecvența necesară a datelor între sistemele TIC și pentru a asigura faptul că arhitectura datelor, modelul și/sau dicționarul de date rămân în concordanță cu cerințele economice și de gestionare a riscurilor;

c. o politică privind utilizarea admisă și recurgerea la sisteme informatice pentru utilizatori finali, în special în ceea ce privește identificarea, înregistrarea și documentarea de soluții informatice importante pentru utilizatori finali (de exemplu, atunci când se prelucrează date importante) și nivelurile de securitate preconizate pentru a preveni modificări neautorizate, atât la nivelul instrumentului în sine, cât și la nivelul datelor stocate în acesta;

[6] Un responsabil de date răspunde de prelucrarea și utilizarea datelor.
[7] Un custode de date răspunde de custodia, transportul și stocarea datelor în condiții de siguranță.
[8] Un supraveghetor de date răspunde de gestionarea și caracterul adecvat al elementelor datelor - conținut și metadate.

d. procese de abordare a excepțiilor documentate pentru rezolvarea problemelor de integritate a datelor TIC identificate în funcție de importanța și sensibilitatea acestora.

58. În cazul instituțiilor supravegheate, care sunt vizate de principiile BCBS 239 pentru agregarea eficace a datelor privind riscurile și raportarea riscurilor[9], autoritățile competente trebuie să verifice analiza riscurilor efectuată de către instituție asupra capacităților sale de raportare a riscurilor și de agregare a datelor în raport cu principiile și documentația elaborată cu privire la acestea, ținând cont de durata de implementare și de dispozițiile tranzitorii din cadrul acestor principii.

(e) Proceduri de control pentru gestionarea riscurilor de externalizare TIC semnificative

59. Autoritățile competente trebuie să evalueze dacă strategia de externalizare a instituției, care este în conformitate cu cerințele Ghidului CEBS privind externalizarea (2006), în urma cerinței de la punctul 85 litera (d) din Ghidul SREP al ABE, se aplică în mod corespunzător în cazul externalizării TIC, inclusiv în cazul externalizării intragrup care furnizează servicii TIC în cadrul grupului. Atunci când evaluează riscurile de externalizare TIC, autoritățile competente trebuie să ia în considerare faptul că riscurile de externalizate TIC pot fi acoperite și în cadrul evaluării riscurilor operaționale inerente de la punctul 240 litera (j) din Ghidul SREP al ABE pentru a evita orice duplicare a activității sau numărarea dublă.

60. În mod specific, autoritățile competente trebuie să evalueze dacă instituția a stabilit un cadru eficace pentru identificarea, înțelegerea și măsurarea riscului de externalizare TIC și, în mod specific, proceduri de control și un mediu de control pentru atenuarea riscurilor asociate serviciilor TIC semnificative externalizate, care sunt proporționale cu dimensiunea, activitățile și profilul de risc TIC al instituției și care includ:

a. o evaluare a impactului externalizării TIC asupra gestionării riscurilor de către instituție în legătură cu utilizarea furnizorilor de servicii (de exemplu, furnizori de servicii cloud) și a serviciilor acestora în cadrul procesului de achiziții care este documentat și luat în considerare de către organele cu funcție de conducere sau structura de conducere pentru decizia de a externaliza serviciile sau nu. Instituția trebuie să analizeze politicile de gestionare a riscurilor TIC, precum și procedurile de control și mediul de control TIC ale furnizorului de servicii, pentru a verifica dacă acesta îndeplinește obiectivele de gestionare internă a riscurilor și apetitul la risc la nivelul instituției. Această analiză trebuie actualizată periodic în perioada de externalizare contractuală, ținând cont de caracteristicile serviciilor externalizate;

b. o monitorizare a riscurilor TIC asociate serviciilor externalizate în perioada de externalizare contractuală în cadrul acțiunii de gestionare a riscurilor instituției, care stă la baza raportării privind gestionarea riscului TIC a instituției (de exemplu, raportarea privind continuitatea activității, raportarea privind securitatea);

[9] Comitetul de la Basel pentru supraveghere bancară, Principles for effective risk data aggregation and risk reporting (Principii pentru agregarea eficace a datelor privind riscurile și raportarea riscurilor), ianuarie 2013, disponibile online: http://www.bis.org/publ/bcbs239.pdf.

c. o monitorizare și o comparație a nivelurilor serviciilor primite cu nivelurile serviciilor convenite prin contract, care trebuie să constituie parte integrantă din contractul de externalizare sau acordul privind nivelul serviciilor (SLA); și

d. personal, resurse și competențe adecvate pentru monitorizarea și gestionarea riscurilor TIC generate de serviciile externalizate.

3.4 Sinteza constatărilor și atribuirea scorului

61. În urma evaluării de mai sus, autoritățile competente trebuie să își formeze o opinie cu privire la riscul TIC al instituției. Această opinie trebuie să se reflecte într-o sinteză a constatărilor pe care autoritățile competente trebuie să le aibă în vedere atunci când atribuie scorul riscului operațional în tabelul 6 din Ghidul SREP al ABE. Autoritățile competente trebuie să își întemeieze opinia pe riscurile TIC semnificative ținând cont de următoarele considerații care să fundamenteze evaluarea riscului operațional:

a. Considerații privind riscul

i. profilul de risc și expunerile la riscul TIC ale instituției;
ii. sistemele și serviciile TIC esențiale identificate; și
iii. semnificația riscului TIC în ceea ce privește sistemele TIC esențiale.

b. Considerații privind gestionarea și procedurile de control

i. dacă există o concordanță între politica și strategia de gestionare a riscului TIC ale instituției și strategia generală și apetitul la risc al acesteia;
ii. dacă cadrul organizațional pentru gestionarea riscului TIC este solid și conține responsabilități clare și o separare clară a sarcinilor între persoanele care își asumă riscuri și funcțiile de conducere și control;
iii. dacă sunt adecvate sistemele de cuantificare, monitorizare și raportare a riscului TIC; și
iv. dacă cadrele de control pentru riscurile TIC semnificative sunt solide.

62. Dacă autoritățile competente consideră că riscul TIC este semnificativ, iar autoritatea competentă decide să evalueze și să atribuie un scor acestui risc ca o subcategorie a riscului operațional, tabelul de mai jos (tabelul 1) prezintă considerațiile privind scorul aferent riscului TIC.

Tabelul 1: Considerații de supraveghere privind atribuirea unui scor pentru riscul TIC

Scor de risc	Opinia de supraveghere	Considerații privind riscul inerent	Considerații privind procedurile adecvate de administrare și control
1	Există un risc imperceptibil de	• Sursele de informații avute în vedere la punctul 37 nu au	

	impact prudențial semnificativ asupra instituției având în vedere nivelul de risc inerent și procedurile de gestionare și control.	evidențiat expuneri semnificative la riscul TIC. • Natura profilului de risc TIC al instituției, în legătură cu analiza sistemelor TIC esențiale și riscurile TIC semnificative pentru sistemele și serviciile TIC, nu au evidențiat riscuri TIC semnificative.	• Politica și strategia instituției privind riscul TIC sunt proporționale cu strategia generală și apetitul la risc al acesteia. • Cadrul organizațional pentru riscul TIC este solid și conține responsabilități clare și o separare clară a sarcinilor între persoanele care își asumă riscuri și funcțiile de conducere și control. • Sunt adecvate sistemele de cuantificare, monitorizare și raportare a riscului TIC. • Cadrul de control pentru riscul TIC este riguros.
2	Există un risc scăzut de impact prudențial semnificativ asupra instituției, având în vedere nivelul de risc inerent și procedurile de gestionare și control.	• Sursele de informații avute în vedere la punctul 37 nu au evidențiat expuneri semnificative la riscul TIC. • Natura profilului de risc TIC al instituției, în legătură cu analiza sistemelor TIC esențiale și riscurile TIC semnificative pentru sistemele și serviciile TIC, au evidențiat o expunere limitată la riscul TIC (de exemplu, nu mai mult de 2 din 5 dintre categoriile de risc TIC prestabilite).	
3	Există un risc mediu de impact prudențial semnificativ asupra instituției, având în vedere nivelul de risc inerent și procedurile de gestionare și control.	• Sursele de informații avute în vedere la punctul 37 au evidențiat indicații ale unor posibile expuneri semnificative la riscul TIC. • Natura profilului de risc TIC al instituției, în legătură cu analiza sistemelor TIC esențiale și riscurile TIC semnificative pentru sistemele și serviciile TIC, au evidențiat o expunere ridicată la riscul TIC (de exemplu, 3 sau mai multe din 5 dintre categoriile de risc TIC prestabilite).	
4	Există un risc ridicat de impact prudențial semnificativ asupra instituției, având în vedere nivelul de risc inerent și procedurile de gestionare și control.	• Sursele de informații avute în vedere la punctul 37 au oferit indicații multiple ale unor expuneri semnificative la riscul TIC. • Natura profilului de risc TIC al instituției, în legătură cu analiza sistemelor TIC esențiale și riscurile TIC semnificative pentru sistemele și serviciile TIC, au evidențiat o expunere ridicată la riscul TIC (de	

		exemplu, 4 sau 5 din 5 dintre categoriile de risc TIC prestabilite).	

Anexă – Taxonomia riscului TIC

5 categorii de riscuri TIC cu o listă incompletă a riscurilor TIC cu o posibilă gravitate și/sau impact operațional, reputațional sau financiar ridicate

Categorii de riscuri TIC	Riscuri TIC (listă incompletă)[10]	Descrierea riscului	Exemple
Riscuri de disponibilitate și continuitate TIC	Gestionarea unor capacități insuficiente	O lipsă de resurse (de exemplu, hardware, software, personal, furnizori de servicii) poate duce la imposibilitatea de a dimensiona serviciul pentru îndeplinirea nevoilor economice, la întreruperi în sistem, la degradarea serviciului și/sau la erori operaționale.	• Un deficit de capacitate poate afecta ratele de transmitere și disponibilitatea rețelei (de Internet) în cazul serviciilor precum cele bancare pe Internet. • Lipsa de personal (intern sau terți) poate duce la întreruperi în sistem și/sau la erori operaționale.
	Defecțiuni la sistemul TIC	Pierderea disponibilității din cauza defecțiunilor la sistemul hardware.	• Eroare de stocare/stocarea defectuoasă (pe hard disk), server sau alte echipamente TIC, de exemplu din cauza lipsei întreținerii.
		Pierderea disponibilității din cauza erorilor la sistemul software și a erorilor de tip bug.	• O buclă infinită în software-ul de aplicare împiedică executarea tranzacției. • Întreruperile datorate utilizării continue a sistemelor și soluțiilor TIC învechite care nu mai îndeplinesc cerințele actuale privind disponibilitatea și reziliența și/sau nu mai sunt susținute de furnizorii acestora.
	O planificare inadecvată a continuității și a recuperării TIC ca urmare a dezastrelor	Defectarea soluțiilor TIC de disponibilitate și/sau continuitate planificate și/sau nerecuperarea acestora ca urmare a dezastrelor (de exemplu, centru de date de recuperare de rezervă) atunci când sunt activate ca răspuns la producerea unui incident.	• Diferențele de configurare dintre centrul de date primar și cel secundar pot atrage după sine incapacitatea centrului de date de rezervă de a asigura continuitatea prevăzută a serviciului.
	Atacuri	Atacurile prevăzute pentru diferite scopuri (de	• Atacurile distribuite cu blocarea accesului au loc

[10] Riscurile TIC sunt enumerate la categoria de riscuri cu cel mai mare impact, însă acestea pot avea impact și asupra altor categorii de riscuri

Categorii de riscuri TIC	Riscuri TIC (listă incompletă)[10]	Descrierea riscului	Exemple
	cibernetice perturbatoare și distructive	exemplu, activism, șantaj), care determină supraîncărcarea sistemelor și a rețelei, împiedicând accesarea serviciilor informaționale online de către utilizatorii legitimi ai acestora.	prin intermediul mai multor sisteme informatice de pe Internet controlate de un hacker care trimite o cantitate mare de solicitări de servicii aparent legitime către serviciile de Internet (de exemplu, servicii bancare electronice).
Riscuri de securitate TIC	Atacuri cibernetice și alte atacuri externe bazate pe TIC	Atacurile lansate de pe Internet sau din rețele din exterior în diferite scopuri (de exemplu, fraudă, spionaj, activism/sabotaj, terorism cibernetic) printr-o varietate de tehnici (de exemplu, inginerie socială, încercări de pătrundere forțată prin exploatarea vulnerabilităților, transmiterea de software dăunător) care duc la preluarea controlului asupra sistemelor TIC interne.	Diferite tipuri de atacuri: • APA (Amenințare persistentă avansată) pentru preluarea controlului asupra sistemelor interne sau furtul de informații (de exemplu, informații legate de furtul de identitate, informații despre cărți de credit). • Software dăunător (de exemplu, ransomware) care criptează date în scop de șantajare. • Infectarea sistemelor TIC interne cu cai troieni pentru comiterea de acțiuni dăunătoare ascunse în sistem. • Exploatarea sistemului TIC și/sau a vulnerabilităților aplicațiilor (web) (de exemplu injectarea SQL ...) pentru dobândirea accesului la sistemul TIC intern.
		Executarea de tranzacții de plăți frauduloase de către hackeri prin spargerea sau ocolirea sistemului de securitate al serviciilor bancare electronice și de plată și/sau prin atacarea și exploatarea vulnerabilităților de securitate din cadrul sistemelor de plată interne ale instituției.	• Atacuri împotriva serviciilor bancare electronice sau de plată cu obiectivul de a efectua tranzacții neautorizate. • Crearea și transmiterea de tranzacții de plată frauduloase din interiorul sistemelor de plată interne ale instituției (de exemplu, mesaje SWIFT frauduloase).
		Executarea de către hackeri a tranzacțiilor frauduloase cu valori mobiliare prin spargerea sau ocolirea sistemului de securitate al serviciilor bancare electronice care asigură și accesul la conturile de valori mobiliare ale clienților.	• Atacuri de tipul „pump and dump”, în urma cărora hackerii dobândesc acces la conturi de valori mobiliare ale clienților prin servicii bancare electronice și plasează ordine de cumpărare sau vânzare frauduloase pentru a influența prețul pieței și/sau a obține câștiguri pe baza pozițiilor valorilor

Categorii de riscuri TIC	Riscuri TIC (listă incompletă)[10]	Descrierea riscului	Exemple
			mobiliare stabilite anterior.
		Atacuri asupra conexiunilor de comunicare și a conversațiilor de orice fel sau a sistemelor TIC cu obiectivul de a colecta informații și/sau a comite fraude.	• Interceptări/interceptarea transmisiunilor neprotejate de date de autentificare în text simplu.
	Securitate TIC internă inadecvată	Obținerea accesului neautorizat la sisteme TIC esențiale din interiorul instituției în diferite scopuri (de exemplu, fraudă, desfășurarea și ascunderea de tranzacții frauduloase, furtul de date, activism/sabotaj) printr-o varietate de tehnici (de exemplu, abuzul de și/sau sporirea privilegiilor, furtul de identitate, ingineria socială, exploatarea vulnerabilităților din sistemele TIC, transmiterea de software dăunător).	• Instalarea de înregistratori pe taste (înregistratori de taste) pentru a fura identificatori și parole ale utilizatorilor în vederea dobândirii accesului neautorizat la date confidențiale și/sau a comiterii de fraude. • Spargerea/aflarea parolelor simple pentru a dobândi drepturi de acces nelegitime sau la un nivel ridicat. • Administratorul de sistem utilizează sistemele de operare sau utilitățile bazei de date (pentru modificări directe la nivelul bazei de date) pentru comiterea de fraude.
		Cazuri de manipulare TIC neautorizată din cauza procedurilor și practicilor de gestionare a accesului TIC necorespunzătoare.	• Imposibilitatea de a dezactiva sau a șterge conturile inutile, cum ar fi cele ale angajaților care și-au schimbat funcțiile și/sau au plecat din instituție, inclusiv ale oaspeților sau furnizorilor care nu mai au nevoie de acces, asigurând accesul neautorizat la sisteme TIC. • Acordarea de drepturi și privilegii de acces excesive, permițând accesul neautorizat și/sau facilitând ascunderea activităților frauduloase.
		Amenințări la adresa securității din cauza lipsei de cunoștințe despre securitate, situații în care angajații nu înțeleg, neglijează sau nu respectă politicile și procedurile de securitate TIC.	• Angajații care sunt înșelați și determinați să ofere asistență pentru un atac (mai exact, inginerie socială). • Practici proaste privind acreditările: transmiterea parolelor, folosirea de parole „ușor” de ghicit, folosirea aceleiași parole în diferite scopuri etc.

Categorii de riscuri TIC	Riscuri TIC (listă incompletă)[10]	Descrierea riscului	Exemple
			• Stocarea de date confidențiale necriptate pe laptop-uri și soluții portabile de stocare a datelor (de exemplu, unități USB) care pot fi pierdute sau furate.
		Stocarea sau transferul neautorizat de informații confidențiale în afara instituției.	• Persoane care fură sau scapă în mod intenționat ori fac contrabandă cu informații confidențiale cu persoane neautorizate sau cu publicul.
	Securitate TIC fizică inadecvată	Deturnarea sau furtul de active TIC prin accesul fizic, provocând daune, pierderea de active sau date ori materializând altor amenințări.	• Pătrunderea prin efracție în clădiri de birouri și/sau centre de date pentru a fura echipamente TIC (de exemplu, calculatoare, laptop-uri, soluții de stocare) și/sau pentru a copia date prin accesul fizic la sisteme TIC.
		Deteriorarea intenționată sau accidentală a activelor TIC fizice din cauza terorismului, a accidentelor sau a manipulării regretabile/eronate din partea angajaților instituției și/sau a terților (furnizori, reparatori).	• Terorism fizic (mai exact, bombe teroriste) sau sabotarea activelor TIC. • Distrugerea centrului de date prin incendiu, infiltrații de apă sau alți factori.
		Protejarea fizică insuficientă împotriva calamităților naturale, care duc la distrugerea parțială sau completă a sistemelor TIC/centrelor de date.	• Cutremure, caniculă, vânturi puternice, furtuni puternice de zăpadă, inundații, incendii, fulgere.
Riscuri de schimbare TIC	Proceduri de control inadecvate pentru schimbări aduse sistemului TIC sau dezvoltarea acestuia.	Incidente provocate de erori sau vulnerabilități nedepistate ca urmare a schimbărilor (de exemplu, efecte neprevăzute ale unei schimbări sau o schimbare gestionată necorespunzător din cauza lipsei testării sau a practicilor necorespunzătoare de gestionare a schimbărilor) aduse, spre exemplu, software-ului, sistemelor și datelor TIC.	• Lansarea în producție a schimbărilor produse la nivelul software-ului sau a celor de configurații fără o testare suficientă, acestea producând efecte adverse neașteptate asupra datelor (de exemplu, corupere, ștergere) și/sau a performanței sistemului TIC (de exemplu, defectare, degradarea performanței). • Schimbări necontrolate la nivelul sistemelor sau datelor TIC din mediul de producție. • Lansarea în producție a sistemelor TIC și aplicațiilor de Internet cu un sistem precar de securitate, acordându-se ocazia hackerilor să atace serviciile de Internet furnizate și/sau să spargă sistemele TIC

Categorii de riscuri TIC	Riscuri TIC (listă incompletă)[10]	Descrierea riscului	Exemple
			interne. • Schimbări necontrolate la nivelul codului sursă al software-ului dezvoltat intern. • Testarea insuficientă din cauza absenței mediilor de testare adecvate.
	Arhitectura TIC inadecvată	O gestionare defectuoasă a arhitecturii TIC la proiectarea, dezvoltarea și întreținerea sistemelor TIC (de exemplu, software, hardware, date) poate duce, în timp, la o gestionare complexă, dificilă, costisitoare și la sisteme TIC rigide care nu mai sunt suficient armonizate cu nevoile economice și nu mai respectă cerințele efective de gestionare a riscurilor.	• Schimbările aduse sistemelor TIC, aplicațiilor software și/sau datelor, care sunt gestionate necorespunzător pe o perioadă mai lungă de timp, rezultând sisteme și arhitecturi TIC complexe, eterogene și dificil de gestionat, provocând multe efecte adverse la nivel economic și al gestionării riscurilor (de exemplu, o securitate și reziliență TIC precare, scăderea calității datelor și a capacităților de raportare). • Personalizarea și extinderea excesivă a pachetelor comerciale de software cu software-ul dezvoltat la nivel intern, ceea ce duce la imposibilitatea de a implementa ediții și versiuni superioare viitoare ale software-ului comercial, precum și la riscul de a nu mai fi susținut de către furnizor.
	Gestionarea inadecvată a ciclului de viață și a patch-ului	Absența întreținerii unui inventar adecvat al tuturor activelor TIC cu susținerea și în combinație cu practici solide privind gestionarea ciclului de viață și a patch-ului. Aceasta duce la o codificare insuficientă (și, astfel, mai vulnerabilă) a sistemelor TIC și la învechirea acestora, fiind posibil ca acestea să nu mai fie compatibile cu nevoile economice și de gestionare a riscurilor.	• Sistemele TIC necodificate și învechite care pot provoca efecte adverse la nivel economic și al gestionării riscurilor (de exemplu, lipsa de flexibilitate și agilitate, întreruperi TIC, slăbirea sistemelor de securitate și a rezilienței TIC).
Riscuri de integritate a datelor TIC	Prelucrarea sau abordarea datelor TIC disfuncționale	Din cauza erorilor sau defecțiunilor la nivel de sistem, comunicare și/sau aplicație, ori din cauza faptului că procesul de extragere, transfer și încărcare a datelor (ETI) a fost executat eronat, datele ar putea fi corupte	• Eroare la sistemul informatic la prelucrarea în lot, ducând la apariția de solduri incorecte în conturile bancare ale clienților. • Interogări executate greșit.

Categorii de riscuri TIC	Riscuri TIC (listă incompletă)[10]	Descrierea riscului	Exemple
		sau pierdute.	• Pierdere de date din cauza erorii de replicare (copiere de rezervă) a datelor.
	Proiectarea eronată a procedurilor de control pentru validarea datelor la sisteme TIC	Erori legate de absența sau ineficiența introducerii automate a datelor sau a procedurilor de control de acceptare (de exemplu, în cazul utilizării datelor terților), a transferului de date, a prelucrării și introducerii procedurilor de control în sisteme TIC (de exemplu, proceduri de control pentru validarea datelor introduse, reconcilieri de date).	• Formatarea/validarea insuficientă sau nulă a datelor introduse în aplicații și/sau interfețe ale utilizatorului. • Absența unor proceduri de control pentru reconcilierea datelor la generarea datelor de ieșire • Absența unor proceduri de control pentru procesele de extragere a datelor executate (de exemplu, interogări în baza de date), ducând la generarea de date eronate. • Utilizarea de date externe defectuoase.
	Controlarea deficientă a schimbărilor de date la nivelul producției de sisteme TIC.	Introducerea de erori de date din cauza absenței unor proceduri de control pentru corectitudinea și justificarea acțiunilor de manipulare a datelor efectuate la producția de sisteme TIC.	• Dezvoltatorii sau administratorii de baze de date care accesează și schimbă direct datele în producția de sisteme TIC în mod necontrolat, de exemplu în cazul unui incident TIC.
	Proiectarea și/sau gestionarea deficientă a arhitecturii datelor, a fluxurilor de date, a modelelor de date sau a dicționarelor de date	Gestionarea deficientă a arhitecturilor datelor, a modelelor de date, a fluxurilor de date sau a dicționarelor de date poate duce la generarea mai multor versiuni ale acelorași date în sistemele TIC, care nu mai sunt consecvente din cauza modelelor de date sau a definițiilor de date aplicate diferit, și/sau a diferențelor la nivelul procesului de generare și schimbare a datelor aferente.	• Existența unor baze de date diferite ale clienților pe produs sau unitate economică, cu definiții și câmpuri de date diferite, ducând la imposibilitatea de reconciliere și la dificultatea de comparare a datelor integrate ale clienților la nivelul întregii instituții sau al întregului grup financiar.
Riscuri de externalizare TIC	Reziliența inadecvată a serviciilor unui terț sau ale unei	Indisponibilitatea serviciilor TIC, serviciilor de telecomunicații și utilități esențiale externalizate. Pierderea sau coruperea datelor esențiale/sensibile încredințate furnizorului de servicii	• Indisponibilitatea serviciilor de bază ca urmare a defecțiunilor de la nivelul sistemelor sau aplicațiilor TIC (externalizate) ale furnizorilor. • Întreruperea legăturilor de telecomunicații.

Categorii de riscuri TIC	Riscuri TIC (listă incompletă)[10]	Descrierea riscului	Exemple
	alte entități din cadrul grupului		• Întreruperea alimentării cu energie.
	Guvernanța necorespunzătoare a acțiunii de externalizare	Degradarea avansată a funcționării sau defectarea din cauza unor procese ineficace de pregătire sau control din partea furnizorului de servicii către care s-a realizat externalizarea. Guvernanța ineficace a acțiunii de externalizare poate duce la absența competențelor și capacităților adecvate pentru identificarea, evaluarea, atenuarea și monitorizarea integrală a riscurilor TIC și poate limita capacitățile operaționale ale instituțiilor.	• Proceduri de abordare a incidentelor, mecanisme de control contractual și garanții dezvoltate defectuos și integrate în acordul cu furnizorul de servicii, crescând dependența umană esențială de terți și furnizori. • Procedurile de control inadecvate pentru gestionarea schimbărilor, care vizează mediul TIC al furnizorului de servicii, pot duce la degradarea avansată a funcționării sau la defectare.
	Securitatea inadecvată a unui terț sau a unei alte entități din cadrul grupului	Spargerea sistemelor TIC ale furnizorilor de servicii terți, cu un impact direct asupra serviciilor externalizate sau a datelor esențiale/confidențiale stocate la furnizorul de servicii. Dobândirea accesului neautorizat de către angajații furnizorului de servicii la date esențiale/sensibile stocate la furnizorul de servicii	• Pătrunderea ilegală a infractorilor sau a teroriștilor la furnizorii de servicii, ca punct de intrare în sistemele TIC ale instituțiilor sau pentru a accesa/distruge date esențiale sau sensibile stocate la furnizorul de servicii. • Existența unor persoane răufăcătoare la furnizorul de servicii, care încearcă să sustragă și să vândă date sensibile.