Ghid

EBA/GL/2019/04

28 noiembrie 2019

Ghidul ABE privind administrarea riscurilor TIC și de securitate

Obligații de conformare și de raportare

Statutul ghidului

1. Prezentul document conține orientări emise în temeiul articolului 16 din Regulamentul (UE) nr. 1093/2010 [1] . 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 ghidul.

2. Ghidul prezintă punctul de vedere al ABE privind practicile adecvate de supraveghere în cadrul Sistemului european de supraveghere financiară sau privind modul în care trebuie aplicat dreptul Uniunii Europene 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 proceselor de supraveghere ale acestora), inclusiv în cazurile în care anumite aspecte din document 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 ghidului sau, în caz contrar, să prezinte motivele neconformării, până la ([zz.ll.aaaa]). În lipsa 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/2019/04”. Notificările trebuie transmise de persoane care au competența necesară de a raporta conformarea, 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).

Obiect, domeniu de aplicare și definiții

Obiect

5. Acest ghid se bazează pe dispozițiile articolului 74 din Directiva 2013/36/UE (CRD) cu privire la cadrul de administrare a activității și derivă din mandatul de a emite orientări, prevăzut la articolul 95 alineatul (3) din Directiva (UE) 2015/2366 (DSP2).

6. Ghidul precizează măsurile de administrare a riscului pe care instituțiile financiare (astfel cum sunt definite la punctul 9 de mai jos) trebuie să le ia, în conformitate cu articolul 74 din CRD, pentru a-și administra riscurile TIC și de securitate în cazul tuturor activităților și pe care trebuie să le ia prestatorii de servicii de plată (astfel cum sunt definiți la punctul 9 de mai jos), în conformitate cu articolul 95 alineatul (1) din DSP2, pentru a-și administra riscurile operaționale și de securitate (denumite „riscuri TIC și de securitate") asociate serviciilor de plată pe care le oferă. Ghidul cuprinde cerințe cu privire la securitatea informațiilor, inclusiv la securitatea cibernetică, în măsura în care aceste informații sunt stocate pe sisteme TIC.

Domeniul de aplicare

7. Ghidul se aplică cu privire la cadrul de administrare a riscurilor TIC și de securitate aplicabil instituțiilor financiare (astfel cum sunt definite la punctul 9). În sensul prezentului ghid, termenul „riscuri TIC și de securitate" se referă la riscurile operaționale și de securitate prevăzute la articolul 95 din DSP2 pentru prestarea de servicii de plată.

8. În cazul prestatorilor de servicii de plată (astfel cum sunt definiți la punctul 9), ghidul se aplică serviciilor de plată prestate de aceștia, în conformitate cu domeniul de aplicare și mandatul prevăzute la articolul 95 din DSP2. În cazul instituțiilor (astfel cum sunt definite la punctul 9), ghidul se aplică tuturor activităților prestate de acestea.

Destinatari

9. Ghidul se adresează instituțiilor financiare, care, în sensul prezentului ghid, se referă (1) la prestatorii de servicii de plată (PSP), astfel cum sunt definiți la articolul 4 alineatul (11) din DSP2, și (2) la instituții, adică instituții de credit și firme de investiții, astfel cum sunt definite la articolul 4 alineatul (1) punctul 3 din Regulamentul (UE) nr. 575/2013. Ghidul se aplică și autorităților competente definite la articolul 4 alineatul (1) punctul 40 din Regulamentul (UE) nr. 575/2013, inclusiv Băncii Centrale Europene, cu privire la aspectele legate de sarcinile care îi sunt conferite prin Regulamentul (UE) nr. 1024/2013, precum și autorităților competente din DSP2, definite la articolul 4 alineatul (2) punctul (i) din Regulamentul (UE) nr. 1093/2010.

Definiții

10. Dacă nu se prevede altfel, termenii folosiți și definiți în Directiva 2013/36/UE (CRD), în Regulamentul (UE) nr. 575/2013 (CRR) și în Directiva 2015/2366 (DSP2) vor avea același înțeles în cuprinsul ghidului. În plus, în sensul prezentului ghid, se aplică următoarele definiții:

Risc TIC și de securitate	Riscul înregistrării de pierderi din cauza încălcării confidențialității, pierderii integrității sistemelor și a datelor, caracterului necorespunzător sau indisponibilității sistemelor și datelor sau incapacității de a schimba tehnologia informației (TI) într-o perioadă de timp rezonabilă și la costuri rezonabile, atunci când cerințele de mediu sau de afaceri se schimbă (agilitate)[2]. Acesta include riscuri de securitate care rezultă fie din procese interne inadecvate sau care nu și-au îndeplinit funcția în mod corespunzător, fie din evenimente externe, inclusiv din atacuri cibernetice sau din securitatea fizică inadecvată.
Organ de conducere	(a) În cazul instituțiilor de credit și al firmelor de investiții, acest termen are același înțeles ca în cadrul definiției de la articolul 3 alineatul (1) punctul 7 din Directiva 2013/36/UE; (b) În cazul instituțiilor de plată sau al instituțiilor emitente de monedă electronică, acest termen se referă la directorii sau la persoanele responsabile cu conducerea și administrarea instituțiilor de plată și a instituțiilor emitente de monedă electronică și, dacă este cazul, la persoanele responsabile cu conducerea și administrarea activităților legate de serviciile de plată ale instituțiilor de plată și ale instituțiilor emitente de monedă electronică ; (c) În cazul prestatorilor de servicii de plată menționați la articolul 1 alineatul (1) punctele (c), (e) și (f) din Directiva (UE) 2015/2366, acest termen are semnificația conferită în temeiul legislației naționale sau a UE aplicabile.
Incident operațional sau de securitate	Un eveniment unic sau o serie de evenimente corelate neprevăzute de instituția financiară, care are/au sau va/vor avea probabil un impact negativ asupra integrității, disponibilității, confidențialității și/sau autenticității serviciilor.
Conducere superioară	(a) În cazul instituțiilor de credit și al firmelor de investiții, acest termen are același înțeles ca în cadrul definiției de la articolul 3 alineatul (1) punctul 9 din Directiva 2013/36/UE; (b) În cazul instituțiilor de plată și al instituțiilor emitente de monedă electronică, acest termen se referă la persoanele fizice care ocupă funcții executive în cadrul unei instituții și

[2] Definiția din Ghidul ABE privind procedurile și metodologiile comune pentru procesul de supraveghere și evaluare (EBA/GL/2014/13) din 19 decembrie 2014, modificat prin EBA/GL/2018/03.

	care sunt responsabile și răspunzătoare față de organul de conducere pentru activitatea de conducere curentă a instituției; (c) În cazul prestatorilor de servicii de plată menționați la articolul 1 alineatul (1) punctele (c), (e) și (f) din Directiva (UE) 2015/2366, acest termen are semnificația conferită în temeiul legislației naționale sau a UE aplicabile.
Apetitul la risc	Nivelul agregat de risc și tipurile de riscuri pe care prestatorii de servicii de plată și instituțiile sunt dispuse să și le asume în limita capacității lor de risc, conform modelului lor de afaceri, în vederea realizării obiectivelor lor strategice.
Funcția de audit	(a) În cazul instituțiilor de credit și al firmelor de investiții, funcția de audit este cea menționată în secțiunea 22 din Ghidul ABE privind cadrul de administrare a activității (EBA/GL/2017/11); (b) În cazul prestatorilor de servicii de plată, alții decât instituțiile de credit, funcția de audit trebuie să fie independentă de prestatorul de servicii de plată sau independentă în cadrul acestuia și poate fi o funcție de audit intern și/sau extern.
Proiecte TIC	Orice proiect sau parte a acestuia în care sunt modificate, înlocuite, respinse sau implementate sisteme și servicii TIC. Proiectele TIC pot face parte din programe de transformare mai ample în sectorul TIC sau în cel de afaceri.
Terț	O organizație care a stabilit relații comerciale sau a încheiat contracte cu o entitate pentru a furniza un produs sau un serviciu.[3]
Activ informațional	O colecție de informații, corporale sau necorporale, care se cuvine să fie protejate.
Activ TIC	Un activ de natură software sau hardware care se găsește în mediul de afaceri.
Sisteme TIC[4]	TIC configurată în cadrul unui mecanism sau al unei rețele de interconectare care susține operațiunile unei instituții financiare.
Servicii TIC[5]	Serviciile furnizate de sisteme TIC unuia sau mai multor utilizatori interni sau externi. Printre exemple se numără serviciile de introducere a datelor, de stocare a datelor, de prelucrare și de raportare a datelor, însă și serviciile de monitorizare și serviciile suport ale afacerii și deciziilor.

[3] Definiția din „Grupul celor Șapte (G7) – Elemente fundamentale pentru gestionarea riscurilor cibernetice în sectorul financiar asociate terților”.
[4] Definiția din Ghidul privind evaluarea riscurilor asociate TIC în cadrul procesului de supraveghere și evaluare (SREP) (EBA/GL/ 2017/05).
[5] EBA/GL/ 2017/05

Punerea în aplicare

Data aplicării

11. Prezentul ghid se aplică începând cu 30 iunie 2020.

Abrogare

12. Ghidul privind măsurile de securitate referitoare la riscurile operaționale și de securitate (EBA/GL/2017/17), emis în 2017, va fi abrogat de prezentul ghid la data la care acesta intră în vigoare.

Ghid privind administrarea riscurilor TIC și de securitate

1.1. Proporționalitatea

1. Toate instituțiile financiare trebuie să respecte dispozițiile stabilite în prezentul ghid într-un mod proporțional și care să țină cont de dimensiunea, organizarea lor internă și de natura, extinderea, complexitatea și gradul de risc al serviciilor și produselor pe care instituțiile financiare le prestează sau intenționează să le presteze.

1.2. Administrarea activității și strategia

1.2.1. Administrarea activității

2. Organul de conducere trebuie să se asigure că instituțiile financiare dispun de un cadru adecvat de administrare a activității și de un cadru de control intern corespunzător riscurilor lor TIC și de securitate. Organul de conducere trebuie să stabilească roluri și responsabilități clare privind funcțiile TIC, administrarea riscurilor de securitate a informațiilor și continuitatea activității, inclusiv pentru organul de conducere și comitetele sale.
3. Organul de conducere trebuie să se asigure că numărul și competențele membrilor personalului instituțiilor financiare sunt corespunzătoare pentru a sprijini permanent nevoile lor operaționale TIC și a proceselor lor de administrare a riscurilor TIC și de securitate, precum și pentru a asigura punerea în aplicare a strategiei lor TIC. Organul de conducere trebuie să se asigure că bugetul alocat este corespunzător pentru a îndeplini strategia lor TIC. În plus, instituțiile financiare trebuie să se asigure că toți membrii personalului, inclusiv persoanele care dețin funcții-cheie, beneficiază anual sau mai des, dacă este necesar, de formare profesională adecvată cu privire la riscurile TIC și de securitate, inclusiv cu privire la securitatea informațiilor (vezi și secțiunea 1.4.7).

4. Organul de conducere este pe deplin răspunzător de stabilirea, aprobarea și supravegherea punerii în aplicare a strategiei TIC a instituțiilor financiare în cadrul strategiei lor globale de afaceri, precum și de stabilirea unui cadru eficace de administrare a riscurilor TIC și de securitate.

1.2.2. Strategia

5. Strategia TIC trebuie aliniată la strategia globală de afaceri a instituțiilor financiare și trebuie să definească:

   a) modul în care trebuie să evolueze TIC a instituțiilor financiare pentru a sprijini și a participa în mod eficient la strategia lor de afaceri, inclusiv la evoluția structurii organizatorice, a modificărilor din sistemul TIC și a dependențelor cheie de terți;
   b) strategia planificată și evoluția arhitecturii TIC, inclusiv a dependențelor de terți;
   c) obiective clare de securitate a informațiilor, punând accent pe sisteme și servicii TIC, pe personal și procese.

6. Instituțiile financiare trebuie să stabilească seturi de planuri de acțiune care să conțină măsurile ce trebuie luate în vederea atingerii obiectivului strategiei TIC. Acestea trebuie comunicate tuturor membrilor relevanți ai personalului (inclusiv contractanților și furnizorilor terți, dacă este cazul și dacă este relevant). Planurile de acțiune trebuie revizuite periodic, pentru a se asigura relevanța și adecvarea acestora. De asemenea, instituțiile financiare trebuie să instituie procese de monitorizare și măsurare a eficacității punerii în aplicare a strategiei lor TIC.

1.2.3. Utilizarea de furnizori terți

7. Fără a aduce atingere dispozițiilor din Ghidul ABE privind externalizarea (EBA/GL/2019/02) și articolului 19 din DSP2, instituțiile financiare trebuie să asigure eficacitatea măsurilor de diminuare a riscurilor, astfel cum sunt definite în cadrul lor de administrare a riscurilor, inclusiv măsurile stabilite în prezentul ghid, atunci când se externalizează funcțiile operaționale aferente serviciilor de plată și/sau servicii TIC și sisteme TIC ale oricărei activități, inclusiv către entitățile din grup, sau atunci când se folosesc furnizori terți.

8. Pentru a asigura continuitatea serviciilor și sistemelor TIC, instituțiile financiare trebuie să se asigure că în contractele și acordurile privind nivelul serviciilor (atât în circumstanțe normale, cât și în caz de întrerupere a serviciului – vezi și secțiunea 1.7.2) cu furnizorii (furnizori de servicii de externalizare, entități din grup sau furnizori terți) sunt incluse următoarele:

   a) obiective și măsuri corespunzătoare și proporționale de securitate a informațiilor, inclusiv cerințe precum cerințe minime de securitate cibernetică, specificații ale ciclului de viață al datelor instituțiilor financiare, orice cerințe privind criptarea datelor, securitatea rețelei și procesele de monitorizare a securității și amplasarea centrelor de date;
   b) proceduri de gestionare a incidentelor operaționale și de securitate, inclusiv escaladarea și raportarea.

9. Instituțiile financiare trebuie să monitorizeze și să se asigure că furnizorii respectivi respectă obiectivele de securitate, măsurile și obiectivele de performanță ale instituției financiare.

1.3. Cadrul de administrare a riscurilor TIC și de securitate

1.3.1. Organizarea și obiectivele

10. Instituțiile financiare trebuie să-și identifice și să-și administreze riscurile TIC și de securitate. Funcția (funcțiile) TIC responsabilă (responsabile) de sistemele TIC, procesele și operațiunile de securitate trebuie să dispună de procese și controale corespunzătoare pentru a se asigura că toate riscurile sunt identificate, analizate, măsurate, monitorizate, administrate, raportate și menținute în limitele apetitului la risc al instituției financiare și că proiectele și sistemele pe care le livrează și activitățile pe care le prestează sunt în conformitate cu cerințele externe și interne.

11. Instituțiile financiare trebuie să atribuie responsabilitatea administrării și supravegherii riscurilor TIC și de securitate unei funcții de control, în conformitate cu cerințele din secțiunea 19 din Ghidul ABE privind cadrul de administrare a activității (EBA/GL/2017/11). Instituțiile financiare trebuie să asigure independența și obiectivitatea acestei funcții de control, separând-o în mod corespunzător de procesele operațiunilor TIC. Această funcție de control trebuie să fie direct răspunzătoare în fața organului de conducere și să fie responsabilă de monitorizarea și controlul respectării cadrului de administrare a riscurilor TIC și de securitate. Aceasta trebuie să se asigure că riscurile TIC și de securitate sunt identificate, măsurate, evaluate, administrate, monitorizate și raportate. Instituțiile financiare trebuie să se asigure că această funcție de control nu este responsabilă de niciun audit intern.

    Funcția de audit intern trebuie să aibă capacitatea, urmând o abordare bazată pe riscuri, de a revizui independent și de a oferi asigurări obiective cu privire la conformarea tuturor unităților și activităților TIC și de securitate ale unei instituții financiare cu politicile și procedurile instituției financiare și cu cerințele externe, în conformitate cu cerințele secțiunii 22 din Ghidul ABE privind cadrul de administrare a activității (EBA/GL/2017/11).

12. Instituțiile financiare trebuie să definească și să atribuie roluri și responsabilități-cheie și linii de raportare relevante, în vederea asigurării eficacității cadrului de administrare a riscurilor TIC și de securitate. Acest cadru trebuie să fie integrat complet în procesele globale ale instituțiilor financiare de administrare a riscurilor și în concordanță cu aceste procese.

13. Cadrul de administrare a riscurilor TIC și de securitate trebuie să includă stabilirea de procese pentru:

    a) determinarea apetitul la risc, în cazul riscurilor TIC și de securitate, în conformitate cu apetitul la risc al instituției financiare;
    b) identificarea și evaluarea riscurilor TIC și de securitate la care este expusă o instituție financiară;
    c) definirea măsurilor de diminuare, inclusiv controale, în vederea diminuării riscurilor TIC și de securitate;

d) monitorizarea eficacității acestor măsuri, precum și a numărului de incidente raportate, inclusiv, în cazul prestatorilor de servicii de plată, al incidentelor raportate în conformitate cu articolul 96 din DSP2 care afectează activitățile legate de TIC, precum și acționarea în sensul corectării măsurilor, dacă este necesar;
e) raportarea către organul de conducere cu privire la riscurile TIC și de securitate și cu privire la controalele aferente acestora;
f) identificarea și evaluarea posibilității de apariție a riscurilor TIC și de securitate în urma modificărilor majore ale sistemelor sau serviciilor TIC, ale proceselor sau procedurilor TIC și/sau după orice incident semnificativ operațional sau de securitate.

14. Instituțiile financiare trebuie să se asigure că acest cadru de administrare a riscurilor TIC și de securitate este documentat și îmbunătățit pe bază continuă cu „lecțiile învățate” pe durata punerii în aplicare și monitorizării sale. Cadrul de administrare a riscurilor TIC și de securitate trebuie aprobat și revizuit, cel puțin o dată pe an, de către organul de conducere.

1.3.2. Identificarea funcțiilor, a proceselor și a activelor

15. Instituțiile financiare trebuie să identifice, să stabilească și să mențină actualizată punerea în corespondență a funcțiilor aferente activității lor, a rolurilor și a proceselor suport, pentru a identifica importanța fiecăruia și interdependențele acestora, în legătură cu riscurile TIC și de securitate.

16. În plus, instituțiile financiare trebuie să identifice, să stabilească și să mențină actualizată punerea în corespondență a activelor informaționale care susțin funcțiile aferente activității lor și procesele suport, cum ar fi sistemele TIC, personalul, contractanții, terții și dependențele de alte sisteme și procese interne și externe, pentru a putea administra, cel puțin, activele informaționale care le susțin procesele și funcțiile critice aferente activității.

1.3.3. Clasificarea și evaluarea riscurilor

17. Instituțiile financiare trebuie să clasifice funcțiile aferente activității, procesele suport și activele informaționale identificate, menționate la punctele 15 și 16, în funcție de nivelul critic al acestora.

18. Pentru a defini nivelul critic al funcțiilor aferente activității, a proceselor suport și a activelor informaționale identificate, instituțiile financiare trebuie să țină seama, cel puțin, de cerințele de confidențialitate, integritate și disponibilitate. Trebuie să se atribuie răspunderi și responsabilități clare pentru activele informaționale.

19. Atunci când efectuează o evaluare a riscurilor, instituțiile financiare trebuie să revizuiască caracterul adecvat al clasificării activelor informaționale și al documentației relevante.

20. Instituțiile financiare trebuie să identifice riscurile TIC și de securitate cu impact asupra funcțiilor aferente activității, proceselor suport și activelor informaționale, identificate și clasificate în funcție de nivelul critic al acestora. Această evaluare a riscurilor trebuie efectuată și documentată anual sau la intervale mai scurte, dacă este necesar. Astfel de evaluări ale riscurilor trebuie efectuate și cu privire la orice modificări majore ale infrastructurii, proceselor

sau procedurilor care afectează funcțiile aferente activității, procesele suport sau activele informaționale și, în consecință, trebuie actualizată evaluarea curentă a riscurilor instituțiilor financiare.

21. Instituțiile financiare trebuie să se asigure că monitorizează pe bază continuă amenințările și vulnerabilitățile relevante pentru procesele aferente activității lor, funcțiile suport și activele informaționale și trebuie să revizuiască în mod regulat scenariile de risc cu impact asupra lor.

1.3.4. Diminuarea riscului

22. Pe baza evaluărilor riscurilor, instituțiile financiare trebuie să stabilească ce măsuri sunt necesare pentru diminuarea la un nivel acceptabil a riscurilor TIC și de securitate identificate și dacă este necesară modificarea proceselor aferente activității, a măsurilor de control, a sistemelor și serviciilor TIC existente. O instituție financiară trebuie să țină seama de durata necesară pentru punerea în aplicare a acestor modificări și de momentul când trebuie luate măsuri provizorii corespunzătoare în vederea diminuării riscurilor TIC și de securitate, astfel încât acestea să nu depășească apetitul la riscurile TIC și de securitate al instituției financiare.

23. Instituțiile financiare trebuie să definească și să pună în aplicare măsuri pentru diminuarea riscurilor TIC și de securitate identificate și pentru a proteja activele informaționale, în funcție de clasificarea lor.

1.3.5. Raportarea

24. Instituțiile financiare trebuie să raporteze în mod clar și la timp organului de conducere rezultatele evaluării riscurilor. Această raportare nu aduce atingere obligației prestatorilor de servicii de plată de a furniza autorităților competente o evaluare actualizată și detaliată a riscurilor, astfel cum se prevede la articolul 95 alineatul (2) din Directiva (UE) 2015/2366.

1.3.6. Auditul

25. Cadrul de administrare a activității, sistemele și procesele unei instituții financiare aferente riscurilor TIC și de securitate trebuie auditate periodic de către auditori cu suficiente cunoștințe, competențe și experiență în riscurile TIC și de securitate și în plăți (în cazul prestatorilor de servicii de plată) pentru a oferi organului de conducere asigurări independente cu privire la eficacitatea acestora. Auditorii trebuie să fie independenți în cadrul instituției financiare sau față de aceasta. Frecvența și obiectul acestor audituri trebuie să fie proporționale cu riscurile TIC și de securitate relevante.

26. Organul de conducere al unei instituții financiare trebuie să aprobe planul de audit, inclusiv orice audituri TIC și orice modificări semnificative ale acestuia. Planul de audit și execuția sa, inclusiv frecvența auditului, trebuie să reflecte și să fie proporționale cu riscurile TIC și de securitate inerente din instituția financiară și trebuie actualizate în mod regulat.

27. Trebuie instituit un proces formal de urmărire care să includă dispoziții pentru verificarea și remedierea la timp a constatărilor critice rezultate din auditul TIC.

1.4. Securitatea informațiilor

1.4.1. Politica în domeniul securității informațiilor

28. Instituțiile financiare trebuie să dezvolte și să documenteze o politică în domeniul securității informațiilor care trebuie să definească principiile generale și normele de protejare a confidențialității, integrității și disponibilității datelor și informațiilor instituțiilor financiare și ale clienților lor. În cazul prestatorilor de servicii de plată, această politică este identificată în documentul privind politica de securitate care urmează să fie adoptat în conformitate cu articolul 5 alineatul (1) litera (j) din Directiva (UE) 2015/2366. Politica în domeniul securității informațiilor trebuie să fie în concordanță cu obiectivele de securitate a informațiilor ale instituției financiare și trebuie să se bazeze pe rezultatele relevante ale procesului de evaluare a riscurilor. Politica trebuie aprobată de organul de conducere.

29. Politica trebuie să conțină o descriere a rolurilor și responsabilităților principale de gestionare a securității informațiilor și trebuie să stabilească cerințele referitoare la securitatea informațiilor pentru personal și contractanți, procese și tehnologie, recunoscând faptul că personalul și contractanții de la toate nivelurile au responsabilități în asigurarea securității informațiilor instituțiilor financiare. Politica trebuie să asigure confidențialitatea, integritatea și disponibilitatea activelor critice, fizice și logice, resurselor și datelor sensibile ale unei instituții financiare, fie că sunt în stare de repaus, în tranzit sau în folosință. Politica în domeniul securității informațiilor trebuie să fie comunicată tuturor membrilor personalului și contractanților instituției financiare.

30. Pe baza politicii în domeniul securității informațiilor, instituțiile financiare trebuie să instituie și să pună în aplicare măsuri de securitate pentru diminuarea riscurilor TIC și de securitate la care sunt expuse. Aceste măsuri trebuie să includă:

    a) organizarea și administrarea activității, în conformitate cu punctele 10 și 11;
    b) securitatea logică (secțiunea 1.4.2);
    c) securitatea fizică (secțiunea 1.4.3);
    d) securitatea operațiunilor TIC (secțiunea 1.4.4);
    e) monitorizarea securității (secțiunea 1.4.5);
    f) revizuirea, evaluarea și testarea securității informațiilor (secțiunea 1.4.6);
    g) formarea profesională și conștientizarea cu privire la securitatea informațiilor (secțiunea 1.4.7).

1.4.2. Securitatea logică

31. Instituțiile financiare trebuie să definească, să documenteze și să pună în aplicare proceduri de control al accesului logic (gestionarea identității și a accesului). Aceste proceduri trebuie puse în aplicare, impuse, monitorizate și revizuite periodic. Procedurile trebuie să includă și controale pentru monitorizarea anomaliilor. Aceste proceduri trebuie să pună în aplicare cel puțin următoarele elemente, unde termenul „utilizator” include și utilizatori tehnici:

(a) **Necesitatea de a cunoaște, privilegiile minime și separarea sarcinilor:** instituțiile financiare trebuie să gestioneze drepturile de acces la activele informaționale și la sistemele lor suport pe baza „necesității de a cunoaște”, inclusiv în ceea ce privește accesul de la distanță. Utilizatorilor trebuie să li se acorde drepturile minime de acces strict necesare pentru executarea sarcinilor lor (principiul „privilegiilor minime”), adică pentru a proteja împotriva accesului nejustificat la un set mare de date sau pentru a împiedica alocarea unor combinații de drepturi de acces care pot fi utilizate pentru a eluda controalele (principiul „separării sarcinilor”).

(b) **Răspunderea utilizatorului:** instituțiile financiare trebuie să limiteze pe cât posibil utilizarea de conturi de utilizator generice și partajate și trebuie să se asigure că utilizatorii pot fi identificați pentru acțiunile întreprinse în sistemele TIC.

(c) **Drepturile de acces privilegiat:** instituțiile financiare trebuie să pună în aplicare controale solide ale accesului privilegiat la sistem prin limitarea strictă și supravegherea îndeaproape a conturilor cu drepturi sporite de acces la sistem (de exemplu, a conturilor de administrator). Pentru a asigura comunicarea în condiții de siguranță și reducerea riscurilor, accesul administrativ de la distanță la sistemele TIC critice trebuie acordat numai pe baza principiului necesității de a cunoaște și atunci când se utilizează soluții de autentificare puternice.

(d) **Înregistrarea activităților utilizatorilor:** toate activitățile utilizatorilor privilegiați trebuie cel puțin înregistrate și monitorizate. Jurnalele de acces trebuie securizate pentru a împiedica modificarea sau ștergerea neautorizată și trebuie păstrate o perioadă de timp proporțională cu nivelul critic al funcțiilor aferente activității, al proceselor suport și al activelor informaționale identificate, în conformitate cu secțiunea 1.3.3, fără a aduce atingere cerințelor de păstrare a datelor, prevăzute în legislația națională și a UE. O instituție financiară trebuie să utilizeze aceste informații pentru facilitarea identificării și investigării activităților anormale detectate în cadrul prestării de servicii.

(e) **Gestionarea accesului:** drepturile de acces trebuie acordate, retrase sau modificate în timp util, în conformitate cu fluxurile de lucru de aprobare predefinite care îl implică pe proprietarul informațiilor accesate (proprietarul activelor informaționale). În caz de încetare a contractului de muncă, drepturile de acces trebuie retrase imediat.

(f) **Recertificarea accesului:** drepturile de acces trebuie revizuite periodic pentru a se asigura că utilizatorii nu dețin privilegii excesive și că drepturile de acces sunt retrase atunci când nu mai sunt necesare.

(g) **Metodele de autentificare:** instituțiile financiare trebuie să aplice metode de autentificare suficient de solide care să asigure respectarea adecvată și eficientă a politicilor și procedurilor de control al accesului. Metodele de autentificare trebuie să fie proporționale cu nivelul critic al sistemelor TIC, al informațiilor sau al procesului care sunt accesate. Acestea trebuie să conțină cel puțin parole complexe sau metode de autentificare mai sigure (cum ar fi autentificarea cu doi factori), în funcție de riscul relevant.

32. Accesul electronic al aplicațiilor prin depunerea de cereri de acces la date și sisteme TIC trebuie să fie limitat la minimul necesar pentru prestarea serviciului relevant.

1.4.3. Securitatea fizică

33. Instituțiile financiare trebuie să definească, să documenteze și să pună în aplicare măsuri de securitate fizică pentru a-și proteja sediile, centrele de date și zonele sensibile împotriva accesului neautorizat și al pericolelor de mediu.

34. Accesul fizic la sistemele TIC trebuie acordat numai persoanelor autorizate. Autorizarea trebuie atribuită în conformitate cu sarcinile și responsabilitățile persoanei în cauză și limitată la persoanele care sunt instruite și monitorizate în mod corespunzător. Accesul fizic trebuie revizuit periodic pentru a se asigura că drepturile de acces sunt revocate imediat ce nu mai sunt necesare.

35. Măsurile adecvate de protecție împotriva pericolelor de mediu trebuie să fie proporționale cu importanța clădirilor și nivelul critic al operațiunilor sau al sistemelor TIC din aceste clădiri.

1.4.4. Securitatea operațiunilor TIC

36. Instituțiile financiare trebuie să pună în aplicare proceduri care să împiedice apariția de probleme de securitate în sistemele și prestarea serviciilor TIC și trebuie să minimizeze impactul acestora asupra prestării de servicii TIC. Aceste proceduri trebuie să cuprindă următoarele măsuri:

    a) identificarea posibilelor vulnerabilități, care trebuie evaluate și remediate prin asigurarea actualizării programelor software și firmware, inclusiv a programelor software furnizate de instituțiile financiare utilizatorilor lor interni și externi, prin instalarea de patch-uri de securitate critice sau prin punerea în aplicare de controale compensatoare;
    b) implementarea de configurații securizate de referință pentru toate componentele rețelei;
    c) implementarea segmentării rețelei, de sisteme de prevenire a pierderii datelor și criptarea traficului din rețea (în conformitate cu clasificarea datelor);
    d) implementarea protecției punctelor finale, inclusiv a serverelor, a stațiilor de lucru și a dispozitivelor mobile; instituțiile financiare trebuie să evalueze dacă punctele finale respectă standardele de securitate definite de acestea, înainte de a li se acorda accesul la rețeaua corporației;
    e) asigurarea existenței unor mecanisme de verificare a integrității programelor software, firmware și a datelor;
    f) criptarea datelor în stare de repaus și în tranzit (în conformitate cu clasificarea datelor).

37. În plus, instituțiile financiare trebuie să stabilească pe bază continuă dacă modificările la nivelul mediului operațional existent influențează măsurile de securitate existente sau dacă impun adoptarea de măsuri suplimentare pentru diminuarea în mod corespunzător a riscurilor asociate. Aceste modificări trebuie să facă parte din procesul formal al instituțiilor financiare de gestionare a modificărilor, proces care trebuie să asigure planificarea, testarea, documentarea, autorizarea și aplicarea corespunzătoare a modificărilor.

1.4.5. Monitorizarea securității

38. Instituțiile financiare trebuie să instituie și să pună în aplicare politici și proceduri, pentru a detecta activitățile anormale care pot afecta securitatea informațiilor instituțiilor financiare și pentru a răspunde în mod corespunzător acestor evenimente. În cadrul acestei monitorizări continue, instituțiile financiare trebuie să implementeze mecanisme corespunzătoare și eficiente de detectare și raportare a intruziunilor logice sau fizice, precum și a încălcărilor confidențialității, integrității și disponibilității activelor informaționale. Procesele continue de monitorizare și de detectare trebuie să acopere:

    a) factorii interni și externi relevanți, inclusiv funcțiile administrative privind TIC și cele aferente activității;
    b) tranzacțiile pentru detectarea utilizării abuzive a accesului de către terți sau de către alte entități și a utilizării abuzive a accesului intern;
    c) eventualele amenințări interne și externe.

39. Instituțiile financiare trebuie să instituie și să pună în aplicare procese și structuri organizatorice, pentru a identifica și monitoriza constant amenințările la adresa securității care ar putea afecta semnificativ capacitatea acestora de a presta servicii. Instituțiile financiare trebuie să monitorizeze activ evoluțiile tehnologice, pentru a se asigura că sunt conștiente de riscurile de securitate. Instituțiile financiare trebuie să pună în aplicare măsuri de detecție, de exemplu pentru a identifica eventualele scurgeri de informații, coduri dăunătoare și alte amenințări la adresa securității și vulnerabilitățile cunoscute în mod public ale programelor software și hardware, și trebuie să verifice existența unor noi actualizări de securitate corespunzătoare.

40. De asemenea, procesul de monitorizare a securității trebuie să ajute o instituție financiară să înțeleagă natura incidentelor operaționale sau de securitate, să identifice tendințele și să sprijine investigațiile organizației.

1.4.6. Revizuirea, evaluarea și testarea securității informațiilor

41. Instituțiile financiare trebuie să realizeze o varietate de revizuiri, evaluări și testări ale securității informațiilor pentru a asigura identificarea eficientă a vulnerabilităților din sistemele și serviciile lor TIC. De exemplu, instituțiile financiare pot realiza analiza lacunelor pe baza standardelor de securitate a informațiilor, revizuiri ale conformității, audituri interne și externe ale sistemelor informatice sau revizuiri ale securității fizice. În plus, instituția trebuie să țină seama de bunele practici, cum ar fi: revizuiri ale codului-sursă, evaluări ale vulnerabilităților, teste de penetrare și exerciții de testare a securității de tip „red team”.

42. Instituțiile financiare trebuie să instituie și să pună în aplicare un cadru de testare a securității informațiilor, care să valideze robustețea și eficacitatea măsurilor lor de securitate a informațiilor și să se asigure că acest cadru ține seama de amenințările și vulnerabilitățile identificate prin intermediul procesului de monitorizare a amenințărilor și de evaluare a riscurilor TIC și de securitate.

43. Cadrul de testare a securității informațiilor trebuie să asigure că testele:

    a) sunt efectuate de verificatori independenți, care au suficiente cunoștințe, competențe și experiență în testarea măsurilor de securitate a informațiilor și nu sunt implicați în dezvoltarea măsurilor de securitate a informațiilor;
    b) includ scanări ale vulnerabilităților și teste de penetrare (inclusiv teste de penetrare bazate pe amenințări, atunci când este necesar și oportun) corespunzătoare nivelului de risc identificat în cadrul sistemelor și proceselor aferente activității.

44. Instituțiile financiare trebuie să efectueze pe bază continuă și în mod repetat teste ale măsurilor de securitate. În cazul tuturor sistemelor TIC critice (punctul 17), aceste teste trebuie efectuate cel puțin anual, iar în cazul prestatorilor de servicii de plată, acestea vor face parte dintr-o evaluare detaliată a riscurilor de securitate asociate serviciilor de plată pe care aceștia le prestează, în conformitate cu articolul 95 alineatul (2) din DSP2. Sistemele non-critice trebuie testate periodic printr-o abordare bazată pe riscuri, dar cel puțin o dată la trei ani.

45. Instituțiile financiare trebuie să se asigure că se efectuează teste ale măsurilor de securitate în caz de modificări la nivelul infrastructurii, al proceselor sau al procedurilor și în caz de modificări ca urmare a unor incidente operaționale sau de securitate majore sau a lansării de aplicații critice cu acces la internet, noi sau modificate substanțial.

46. Instituțiile financiare trebuie să monitorizeze și să evalueze rezultatele testelor de securitate și să-și actualizeze măsurile de securitate în mod corespunzător și fără întârzieri nejustificate, în cazul sistemelor TIC critice.

47. În cazul prestatorilor de servicii de plată, cadrul de testare trebuie să cuprindă, de asemenea, măsurile de securitate relevante cu privire la (1) terminalele de plată și dispozitivele utilizate pentru prestarea serviciilor de plată, (2) terminalele de plată și dispozitivele utilizate pentru autentificarea utilizatorilor de servicii de plată și (3) dispozitivele și programul software furnizat de prestatorul de servicii de plată utilizatorului de servicii de plată pentru a genera/primi un cod de autentificare.

48. Pe baza amenințărilor la adresa securității constatate și a modificărilor efectuate, trebuie să se realizeze testări care să includă scenariile atacurilor potențiale cunoscute și relevante.

1.4.7. Formarea profesională și conștientizarea cu privire la securitatea informațiilor

49. Instituțiile financiare trebuie să stabilească un program de formare profesională, care să includă programe periodice de conștientizare cu privire la securitate, pentru toți membrii personalului și contractanți, pentru a se asigura că aceștia sunt instruiți pentru a-și îndeplini sarcinile și responsabilitățile, în conformitate cu procedurile și politicile de securitate relevante, în vederea diminuării erorii umane, a furtului, a fraudei, a utilizării abuzive sau a pierderii, și pentru a aborda adecvat riscurile asociate securității informațiilor. Instituțiile financiare trebuie să se asigure că programul de formare profesională prevede instruirea tuturor membrilor personalului și a contractanților cel puțin anual.

1.5. Gestionarea operațiunilor TIC

50. Instituțiile financiare trebuie să-și gestioneze operațiunile TIC pe bază de procese și proceduri documentate și puse în aplicare (ceea ce, în cazul prestatorilor de servicii de plată, înseamnă documentul de politică de securitate, în conformitate cu articolul 5 alineatul (1) litera (j) din DSP2), care sunt aprobate de organul de conducere. Acest set de documente trebuie să definească modul în care instituțiile financiare operează, monitorizează și își verifică sistemele și serviciile TIC, inclusiv documentarea operațiunilor TIC critice, și trebuie să permită instituțiilor financiare să-și actualizeze inventarul activelor TIC.

51. Instituțiile financiare trebuie să se asigure că performanța operațiunilor TIC este în concordanță cu cerințele lor de afaceri. Instituțiile financiare trebuie să mențină și să-și îmbunătățească, atunci când este posibil, eficiența operațiunilor TIC, inclusiv, dar fără a se limita la necesitatea de a analiza modul în care pot fi minimizate eventualele erori ce decurg din executarea sarcinilor manuale.

52. Instituțiile financiare trebuie să pună în aplicare proceduri privind înregistrarea și monitorizarea în cazul operațiunilor TIC critice, pentru a permite detectarea, analiza și corectarea erorilor.

53. Instituțiile financiare trebuie să mențină un inventar actualizat al activelor TIC (inclusiv sistemele TIC, dispozitivele de rețea, bazele de date etc.). Inventarul activelor TIC trebuie să conțină configurația activelor TIC și legăturile și interdependențele dintre diferitele active TIC, pentru a permite un proces adecvat de gestionare a configurațiilor și modificărilor.

54. Inventarul activelor TIC trebuie să fie suficient de detaliat pentru a permite identificarea imediată a unui activ TIC, a amplasamentului acestuia, a nivelului de securitate și a proprietarului. Interdependențele dintre active trebuie documentate, pentru a ajuta instituțiile financiare să intervină în caz de incidente de securitate sau operaționale, inclusiv în caz de atacuri cibernetice.

55. Instituțiile financiare trebuie să monitorizeze și să gestioneze ciclurile de viață ale activelor TIC, pentru a asigura că acestea îndeplinesc și susțin în continuare cerințele de afaceri și de administrare a riscurilor. Instituțiile financiare trebuie să monitorizeze dacă furnizorii lor interni sau externi și dezvoltatorii oferă asistență pentru activele lor TIC și dacă sunt instalate toate patch-urile și actualizările relevante pe bază de procese documentate. Riscurile care decurg din activele TIC depășite sau pentru care nu se mai oferă suport trebuie evaluate și diminuate.

56. Instituțiile financiare trebuie să pună în aplicare procese de planificare și monitorizare a performanței și capacității, pentru a împiedica, a detecta și a răspunde prompt problemelor importante legate de performanța sistemelor TIC și de deficiențe ale capacității TIC.

57. Instituțiile financiare trebuie să definească și să implementeze proceduri pentru realizarea de copii de rezervă și de restaurare a datelor și a sistemelor TIC, pentru a se asigura că acestea pot fi recuperate, conform cerințelor. Domeniul de aplicare și frecvența operațiunilor de realizare a copiilor de rezervă trebuie stabilite în conformitate cu cerințele de redresare aferente activității și cu nivelul critic al datelor și al sistemelor TIC și trebuie analizate în funcție de

evaluarea riscurilor. Testarea procedurilor de realizare a copiilor de rezervă și de restaurare trebuie efectuată periodic.

58. Instituțiile financiare trebuie să se asigure că aceste copii de rezervă ale datelor și ale sistemelor TIC sunt stocate în siguranță și se află la o distanță suficient de mare față de amplasamentul principal, pentru a nu fi expuse acelorași riscuri.

1.5.1 Gestionarea problemelor și incidentelor TIC

59. Instituțiile financiare trebuie să instituie și să pună în aplicare un proces de gestionare a problemelor și incidentelor, pentru a monitoriza și înregistra incidentele TIC de securitate și operaționale și pentru a permite instituțiilor financiare să continue sau să reia rapid procesele și funcțiile critice aferente activității, atunci când se produc întreruperi. Instituțiile financiare trebuie să stabilească pragurile și criteriile corespunzătoare pentru clasificarea evenimentelor drept incidente operaționale sau de securitate, astfel cum este prevăzut în secțiunea „Definiții” din prezentul ghid, precum și indicatorii de avertizare timpurie care trebuie să servească drept alerte, pentru a permite detectarea timpurie a acestor incidente. Pentru prestatorii de servicii de plată, aceste criterii și praguri nu aduc atingere clasificării incidentelor majore, în conformitate cu articolul 96 din DSP2 și cu Ghidul privind raportarea incidentelor majore în temeiul DSP2 (EBA/GL/2017/10).

60. Pentru a minimiza impactul evenimentelor defavorabile și a permite redresarea la timp, instituțiile financiare trebuie să instituie procese și structuri organizatorice corespunzătoare pentru a asigura monitorizarea, manevrarea și urmărirea în mod integrat și consecvent a incidentelor operaționale și de securitate și pentru a asigura identificarea și eliminarea principalelor cauze, pentru a evita reapariția unor astfel de incidente. Procesul de gestionare a problemelor și incidentelor trebuie să stabilească:

    a) proceduri de identificare, urmărire, înregistrare, categorisire și clasificare a incidentelor, potrivit unei reguli de prioritate, în funcție de nivelul critic al activității;
    b) rolurile și responsabilitățile pentru diferite scenarii de incidente (de exemplu, erori, defecțiuni, atacuri cibernetice);
    c) proceduri de gestionare a problemelor pentru a identifica, analiza și soluționa principala cauză a unuia sau a mai multor incidente – o instituție financiară trebuie să analizeze incidentele operaționale sau de securitate care ar putea afecta instituția financiară, care au fost identificate sau care au avut loc în cadrul și/sau în afara organizației, și trebuie să ia în considerare lecțiile-cheie învățate din aceste analize și să actualizeze în consecință măsurile de securitate;
    d) planuri eficiente de comunicare internă, inclusiv proceduri de notificare și escaladare a incidentelor – care să acopere și reclamațiile clienților legate de securitate – pentru a asigura că:
        i) incidentele cu un posibil impact negativ ridicat asupra sistemelor și serviciilor TIC sunt raportate conducerii superioare relevante și conducerii superioare din domeniul TIC;

ii) organul de conducere este informat ad-hoc în caz de incidente semnificative, cel puțin cu privire la impactul, măsurile luate și controalele suplimentare care urmează să fie definite ca urmare a incidentelor.

e) proceduri de intervenție în caz de incidente, pentru reducerea impactului acestora și pentru a asigura că serviciul devine operațional și sigur rapid;

f) planuri specifice de comunicare externă pentru procese și funcții critice asociate activității pentru:

i) a colabora cu părțile interesate relevante, pentru a interveni în mod eficient în caz de incidente și a se redresa în urma acestora;

ii) a oferi părților externe (de exemplu, clienților, altor participanți pe piață, autorității de supraveghere) informații în timp util, în mod corespunzător și în conformitate cu regulamentul aplicabil.

1.6. Gestionarea proiectelor și modificărilor TIC

1.6.1. Gestionarea proiectelor TIC

61. O instituție financiară trebuie să pună în aplicare un program și/sau un proces de guvernanță a proiectelor care să definească rolurile, responsabilitățile și răspunderile, pentru a susține în mod eficient punerea în aplicare a strategiei TIC.

62. O instituție financiară trebuie să monitorizeze și să diminueze în mod corespunzător riscurile ce decurg din portofoliul ei de proiecte TIC (gestionarea programului), ținând seama și de riscurile care pot rezulta din interdependențele dintre diferite proiecte și din dependențele mai multor proiecte de aceleași resurse și/sau competențe.

63. O instituție financiară trebuie să instituie și să pună în aplicare o politică de gestionare a proiectelor TIC, care să includă cel puțin:

a) obiectivele proiectului;
b) rolurile și responsabilitățile;
c) evaluarea riscurilor asociate proiectului;
d) planul, calendarul și etapele proiectului;
e) principalele obiective intermediare;
f) cerințele de gestionare a modificărilor.

64. Politica de gestionare a proiectelor TIC trebuie să asigure că cerințele de securitate a informațiilor sunt analizate și aprobate de către o funcție independentă de funcția care le-a elaborat.

65. O instituție financiară trebuie să se asigure că toate domeniile afectate de un proiect TIC sunt reprezentate în echipa de proiect și că echipa de proiect deține cunoștințele necesare pentru a asigura implementarea sigură și cu succes a proiectului.

66. Elaborarea și evoluția proiectelor TIC și riscurile lor asociate trebuie raportate organului de conducere, individual sau agregat, în funcție de importanța și de dimensiunea proiectelor TIC, în mod regulat și ad-hoc, după caz. Instituțiile financiare trebuie să includă riscul asociat proiectului în cadrul lor de administrare a riscurilor.

1.6.2. Achiziția și dezvoltarea de sisteme TIC

67. Instituțiile financiare trebuie să elaboreze și să pună în aplicare un proces care să reglementeze achiziția, dezvoltarea și întreținerea sistemelor TIC. Acest proces trebuie conceput folosind o abordare bazată pe riscuri.

68. O instituție financiară trebuie să se asigure că, înainte de orice achiziție sau dezvoltare a sistemelor TIC, cerințele funcționale și nefuncționale (inclusiv cerințele de securitate a informațiilor) sunt clar definite și aprobate de către conducerea relevantă.

69. O instituție financiară trebuie să se asigure că sunt instituite măsuri pentru diminuarea riscurilor de modificare neintenționată sau de manipulare intenționată a sistemelor TIC pe durata dezvoltării și implementării în mediul de producție.

70. Instituțiile financiare trebuie să dețină o metodologie pentru testarea și aprobarea sistemelor TIC înainte de prima lor utilizare. Această metodologie trebuie să țină seama de nivelul critic al activelor și proceselor aferente activității. Testarea trebuie să asigure faptul că noile sisteme TIC funcționează așa cum au fost proiectate. De asemenea, acestea trebuie să utilizeze medii de testare care să reflecte în mod corespunzător mediul de producție.

71. Instituțiile financiare trebuie să testeze sistemele TIC, serviciile TIC și măsurile de securitate a informațiilor, pentru a identifica eventualele puncte slabe, încălcări și incidente de securitate.

72. O instituție financiară trebuie să implementeze medii TIC separate pentru a asigura separarea adecvată a sarcinilor și pentru a atenua impactul modificărilor neverificate asupra sistemelor de producție. În special, o instituție financiară trebuie să asigure separarea mediilor de producție de mediile de dezvoltare, de testare și de alte medii care nu au legătură cu producția. O instituție financiară trebuie să asigure integritatea și confidențialitatea datelor de producție în mediile care nu au legătură cu producția. Accesul la datele din mediul de producție este limitat la utilizatorii autorizați.

73. Instituțiile financiare trebuie să pună în aplicare măsuri pentru protejarea integrității codurilor-sursă ale sistemelor TIC dezvoltate intern. De asemenea, acestea trebuie să documenteze în mod amănunțit dezvoltarea, implementarea, operarea și/sau configurarea sistemelor TIC, pentru a reduce orice dependență inutilă de experții în domeniu. Documentația sistemului TIC trebuie să conțină, unde este cazul, cel puțin documentația de utilizare, documentația tehnică a sistemului și procedurile de operare.

74. Procesele de achiziție și dezvoltare a sistemelor TIC ale unei instituții financiare trebuie să se aplice și sistemelor TIC dezvoltate sau gestionate de utilizatorii finali ai funcției aferente activității din afara organizației TIC (de exemplu, în aplicațiile informatice ale utilizatorilor finali) folosind o abordare bazată pe riscuri. Instituția financiară trebuie să țină o evidență a aplicațiilor acestea care sprijină procesele și funcțiile critice aferente activității.

1.6.3. Gestionarea modificărilor TIC

75. Instituțiile financiare trebuie să instituie și să pună în aplicare un proces de gestionare a modificărilor TIC pentru a se asigura că toate modificările aduse sistemelor TIC sunt înregistrate, testate, evaluate, aprobate, implementate și verificate în mod controlat. Instituțiile financiare trebuie să gestioneze modificările necesare în timpul situațiilor de urgență (adică modificări ce trebuie introduse cât mai repede posibil) urmând proceduri care să asigure o protecție adecvată.

76. Instituțiile financiare trebuie să stabilească dacă modificările la nivelul mediului operațional existent influențează măsurile de securitate existente sau dacă impun adoptarea de măsuri suplimentare pentru diminuarea riscurilor implicate. Aceste modificări trebuie să fie în conformitate cu procesul formal de gestionare a modificărilor pentru instituțiile financiare.

1.7. Gestionarea continuității activității

77. Instituțiile financiare trebuie să instituie un proces solid de gestionare a continuității activității pentru a-și maximiza capacitatea de a presta servicii pe o bază continuă și pentru a limita pierderile în caz de întrerupere gravă a activității, în conformitate cu articolul 85 alineatul (2) din Directiva 2013/36/UE și cu titlul VI din Ghidul ABE privind cadrul de administrare a activității (EBA/GL/2017/11).

1.7.1. Analiza impactului asupra activității

78. Ca parte a bunei gestionări a continuității activității, instituțiile financiare trebuie să realizeze o analiză de impact asupra activității (BIA), analizând expunerea lor la întreruperi grave ale activității și evaluând, din punct de vedere cantitativ și calitativ, impactul potențial al acestora (inclusiv asupra confidențialității, integrității și disponibilității), folosind date interne și/sau externe (de exemplu, date de la furnizorii terți, relevante pentru un proces aferent activității, sau date disponibile public care pot fi relevante pentru analiza de impact asupra activității) și analize pe bază de scenarii. Analiza de impact asupra activității trebuie să țină seama și de nivelul critic al funcțiilor aferente activității, al proceselor suport, al terților și al activelor informaționale identificate și clasificate și de interdependențele acestora, în conformitate cu secțiunea 1.3.3.

79. Instituțiile financiare trebuie să se asigure că sistemele și serviciile lor TIC sunt concepute și sunt în concordanță cu analiza lor de impact asupra activității, de exemplu cu redundanța anumitor componente critice, pentru a preveni întreruperile cauzate de evenimente cu impact asupra componentelor respective.

1.7.2. Planificarea continuității activității

80. Pe baza analizelor de impact asupra activității, instituțiile financiare trebuie să elaboreze planuri pentru a asigura continuitatea activității (planuri de asigurare a continuității activității - BCP), care trebuie să fie documentate și aprobate de organele lor de conducere. Planurile trebuie să țină seama în mod special de riscurile care ar putea afecta în mod negativ sistemele și serviciile

TIC. Planurile trebuie să sprijine obiectivele de a proteja și, dacă este cazul, de a restabili confidențialitatea, integritatea și disponibilitatea funcțiilor aferente activității lor, a proceselor suport și a activelor informaționale. Instituțiile financiare trebuie să se coordoneze cu părțile interesate interne și externe relevante, după caz, pe durata elaborării acestor planuri.

81. Instituțiile financiare trebuie să pună în aplicare planuri de asigurare a continuității activității pentru a se asigura că acestea pot reacționa în mod corespunzător la eventuale scenarii de intrare în dificultate și că sunt capabile să-și redreseze operațiunile activităților lor de afaceri critice în urma unor întreruperi, conform obiectivului timp de recuperare (RTO - intervalul maxim în care un sistem sau un proces trebuie să fie restabilit după un incident) și obiectivului punct de recuperare (RPO - perioada maximă în care se acceptă pierderea datelor în cazul unui incident). În cazul unei întreruperi grave a activității care declanșează planuri specifice de asigurare a continuității activității, instituțiile financiare trebuie să stabilească o prioritate a acțiunilor de continuitate folosind o abordare bazată pe riscuri, care se poate baza pe evaluările riscurilor realizate în conformitate cu secțiunea 1.3.3. În cazul prestatorilor de servicii de plată, aceasta include, de exemplu, facilitarea procesării ulterioare a tranzacțiilor critice odată cu continuarea eforturilor de remediere.

82. O instituție financiară trebuie să ia în considerare o serie de scenarii diferite în planul său de asigurare a continuității activității, inclusiv cele extreme dar plauzibile la care ar putea fi expusă, inclusiv un scenariu de atac cibernetic, și trebuie să evalueze impactul potențial al unor astfel de scenarii. Pe baza acestor scenarii, o instituție financiară trebuie să descrie modul în care sunt asigurate continuitatea sistemelor și serviciilor TIC și securitatea informațiilor acesteia.

1.7.3. Planurile de intervenție și de redresare

83. Pe baza analizelor de impact asupra activității (punctul 78) și a scenariilor plauzibile (punctul 82), instituțiile financiare trebuie să elaboreze planuri de intervenție și de redresare. Aceste planuri trebuie să precizeze condițiile în care poate fi declanșată activarea planurilor și măsurile care trebuie luate pentru a asigura disponibilitatea, continuitatea și redresarea cel puțin a sistemelor și serviciilor TIC critice ale instituțiilor financiare. Planurile de intervenție și de redresare trebuie să vizeze atingerea obiectivelor de redresare a operațiunilor instituțiilor financiare.

84. Planurile de intervenție și de redresare trebuie să țină seama atât de opțiunile de redresare pe termen scurt, cât și de cele pe termen lung. Planurile trebuie:

    a) să pună accentul pe redresarea operațiunilor funcțiilor critice aferente activității, ale proceselor suport, ale activelor informaționale și pe interdependențele acestora, pentru a evita efectele negative asupra funcționării instituțiilor financiare și asupra sistemului financiar, inclusiv asupra sistemelor de plată și asupra utilizatorilor serviciilor de plată, și pentru a asigura executarea operațiunilor de plată în așteptare;
    b) să fie documentate și puse la dispoziția unităților operaționale și cele suport și ușor accesibile în caz de urgență;
    c) să fie actualizate în conformitate cu lecțiile învățate din incidente, teste, cu noile riscuri și amenințări identificate și cu prioritățile și obiectivele de redresare modificate.

85. Planurile trebuie să aibă în vedere și opțiuni alternative, în cazul în care este posibil ca redresarea să nu fie fezabilă pe termen scurt, din cauza costurilor, riscurilor, logisticii sau a situațiilor neprevăzute.

86. În plus, în cadrul planurilor de intervenție și de redresare, instituția financiară trebuie să aibă în vedere și punerea în aplicare a măsurilor de asigurare a continuității pentru a atenua incapacitățile furnizorilor terți, măsuri extrem de importante pentru asigurarea continuității serviciilor TIC ale instituției financiare [în concordanță cu dispozițiile Ghidului ABE privind externalizarea (EBA/GL/2019/02) referitoare la planurile de continuitate a activității].

1.7.4. Testarea planurilor

87. Instituțiile financiare trebuie să-și testeze periodic planurile de asigurare a continuității activității. În special, acestea trebuie să se asigure că planurile de asigurare a continuității funcțiilor critice aferente activității lor, ale proceselor suport, ale activelor informaționale și interdependențele lor (inclusiv cele furnizate de terți, unde este cazul) sunt testate cel puțin anual, în conformitate cu punctul 89.

88. Planurile de asigurare a continuității activității trebuie actualizate cel puțin anual, pe baza rezultatelor testelor, a informațiilor privind amenințările curente și a lecțiilor învățate din evenimentele anterioare. Orice modificări ale obiectivelor de redresare (inclusiv ale RTO și RPO) și/sau modificări ale funcțiilor aferente activității, ale proceselor suport și ale activelor informaționale trebuie să fie considerate, dacă este cazul, și ca o bază pentru actualizarea planurilor de asigurare a continuității activității.

89. Testarea de către instituțiile financiare a planurilor lor de asigurare a continuității activității trebuie să demonstreze capacitatea acestora de a susține viabilitatea activităților instituțiilor financiare până la restabilirea operațiunilor critice. În mod specific, acestea trebuie:

    a) să includă testarea unui set corespunzător de scenarii extreme dar plauzibile, inclusiv a celor avute în vedere la elaborarea planurilor de asigurare a continuității activității (precum și testarea serviciilor prestate de terți, unde este cazul); aceasta trebuie să includă transferarea funcțiilor critice aferente activității, a proceselor suport și a activelor informaționale în mediul de redresare în caz de dezastru și demonstrarea faptului că pot fi gestionate astfel o perioadă suficient de reprezentativă și că funcționarea normală poate fi restabilită ulterior;
    b) să fie concepute pentru a contesta ipotezele pe care se bazează planurile de asigurare a continuității activității, inclusiv mecanismele de guvernanță și planurile de comunicare în situații de criză; și
    c) să includă proceduri pentru a verifica capacitatea personalului și a contractanților, a sistemelor și serviciilor TIC de a răspunde în mod corespunzător în cazul scenariilor definite la punctul 89 litera (a).

90. Rezultatele testelor trebuie să fie documentate și toate deficiențele identificate în urma testelor trebuie analizate, abordate și raportate organului de conducere.

1.7.5. Comunicările în situații de criză

91. În cazul unei întreruperi sau al unei urgențe și pe parcursul punerii în aplicare a planurilor de asigurare a continuității activității, instituțiile financiare trebuie să se asigure că au introdus măsuri eficiente de comunicare în situații de criză, astfel încât toate părțile interesate interne și externe relevante, inclusiv autoritățile competente, atunci când reglementările naționale o cer, precum și prestatorii relevanți (furnizori de servicii de externalizare, entități din grup sau furnizori terți) să fie informați în timp util și în mod corespunzător.

1.8. Gestionarea serviciilor de plată în relația cu utilizatorul

92. Prestatorii de servicii de plată trebuie să instituie și să pună în aplicare procese de sporire a gradului de conștientizare al utilizatorilor de servicii de plată cu privire la riscurile de securitate asociate cu serviciile de plată, acordând asistență și îndrumare utilizatorilor de servicii de plată.

93. Asistența și îndrumarea acordate utilizatorilor de servicii de plată trebuie să fie actualizate în funcție de noile amenințări și vulnerabilități, iar utilizatorul de servicii de plată trebuie să fie informat despre modificări.

94. În cazul în care funcționalitatea produsului o permite, prestatorii de servicii de plată trebuie să le permită utilizatorilor de servicii de plată să dezactiveze funcționalitățile de plată specifice, aferente serviciilor de plată furnizate de prestatorul de servicii de plată utilizatorului de servicii de plată.

95. În cazul în care, în conformitate cu articolul 68 alineatul (1) din Directiva (UE) 2015/2366, un prestator de servicii de plată a acceptat limitele de cheltuieli ale plătitorului în ceea ce privește operațiunile de plată efectuate prin intermediul instrumentelor de plată specifice, prestatorul de servicii de plată trebuie să ofere plătitorului opțiunea de a ajusta aceste limite până la limita maximă admisă.

96. Prestatorii de servicii de plată trebuie să acorde utilizatorilor de servicii de plată opțiunea de a primi alerte referitoare la încercările inițiate și/sau eșuate de începere a operațiunilor de plată, permițându-le să detecteze utilizarea frauduloasă sau dăunătoare a conturilor lor.

97. Prestatorii de servicii de plată trebuie să-i informeze pe utilizatorii de servicii de plată despre actualizările procedurilor de securitate care afectează utilizatorii de servicii de plată în ceea ce privește prestarea serviciilor de plată.

98. Prestatorii de servicii de plată trebuie să acorde asistență utilizatorilor de servicii de plată în orice chestiuni, cereri de sprijin și notificări de anomalii sau aspecte referitoare la probleme de securitate legate de serviciile de plată. Utilizatorii de servicii de plată trebuie să fie informați în mod corespunzător despre modul de obținere a asistenței respective.