EBA/REC/2017/03

28.03.2018

Recomandări

privind externalizarea către furnizori de servicii de tip cloud

1. Obligații de conformare și de raportare

Statutul prezentelor recomandări

1. Prezentul document conține recomandări 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 recomandările.

2. Recomandările prezintă punctul de vedere al ABE privind practicile adecvate în materie de supraveghere în cadrul Sistemului european de supraveghere financiară sau privind modul în care ar trebui aplicat dreptul Uniunii într-un anumit domeniu. Autoritățile competente, astfel cum sunt definite la articolul 4 alineatul (2) din Regulamentul (UE) nr. 1093/2010 și cărora li se aplică recomandările, trebuie să se conformeze prin integrarea acestora în practicile lor, după caz (de exemplu, prin modificarea cadrului legislativ sau a procedurilor de supraveghere proprii), inclusiv în cazurile în care recomandările 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 s-au conformat sau intenționează să se conformeze prezentelor recomandări sau, în caz contrar, care sunt motivele neconformării, până la 28.05.2018. 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/REC/2017/03”. Notificările trebuie transmise de persoane care au competența necesară pentru a raporta conformitatea, în numele autorităților competente din care fac parte. Orice schimbare cu privire la statutul 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

1. Prezentele recomandări precizează mai detaliat condițiile de externalizare menționate în ghidul CEBS privind externalizarea din 14 decembrie 2006 și se aplică externalizării de către instituțiile definite la articolul 4 alineatul (1) punctul (3) din Regulamentul (UE) nr. 575/2013 către furnizori de servicii de tip cloud.

Destinatari

2. Prezentul ghid se adresează autorităților competente prevăzute la articolul 4 alineatul (2) litera (i) din Regulamentul (UE) nr. 1093/2010 și instituțiilor financiare prevăzute la articolul 4 alineatul (1) punctul (3) din Regulamentul (UE) nr. 575/2013.[2]

Definiții

3. Cu excepția cazului în care se prevede altfel, termenii utilizați și definiți în Directiva 2013/36/UE[3] privind cerințele de capital și ghidul CEBS au același înțeles în recomandări. În plus, în sensul prezentelor recomandări, se aplică următoarele definiții:

Servicii de tip cloud	Servicii furnizate cu ajutorul tehnologiilor de calcul de tip cloud, și anume un model pentru permiterea accesului universal, convenabil, la cerere în rețea la un grup comun de resurse de calcul configurabile (de exemplu rețele, servere, soluții de stocare, aplicații și servicii), care poate fi rapid pus la dispoziție și lansat cu un efort minim de gestionare sau interacțiune cu furnizorul serviciului.
Cloud public	Infrastructură de tip cloud disponibilă pentru utilizare liberă de către publicul larg.
Cloud privat	Infrastructură de tip cloud disponibilă pentru utilizare exclusivă de către o singură instituție.
Cloud comunitar	Infrastructură de tip cloud disponibilă pentru utilizare exclusivă de către o anumită comunitate de instituții, incluzând câteva instituții dintr-un singur grup.

[2] Regulamentul (UE) nr. 575/2013 al Parlamentului European și al Consiliului din 26 iunie 2013 privind cerințele prudențiale pentru instituțiile de credit și societățile de investiții și de modificare a Regulamentului (UE) nr. 648/2012.

[3] 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.

Cloud hibrid	Infrastructură de tip cloud compusă din două sau mai multe infrastructuri distincte de tip cloud.

3. Punere în aplicare

Data aplicării

5. Prezentele recomandări se aplică de la 1 iulie 2018.

4. Recomandări privind externalizarea către furnizori de servicii de tip cloud

4.1 Evaluarea importanței semnificative

1. Instituțiile care externalizează trebuie să evalueze, înainte de orice externalizare a activităților lor, care activități trebuie considerate importante. Instituțiile trebuie să efectueze această evaluare a importanței activităților pe baza orientării 1(f) din ghidul CEBS și, în ceea ce privește externalizarea către furnizori de servicii de tip cloud în mod special, ținând cont de toate cele de mai jos:

   (a) criticitatea și profilul de risc inerent al activităților ce urmează a fi externalizate, mai exact dacă sunt activități critice pentru continuitatea/viabilitatea activității instituției și a obligațiilor acesteia față de clienții săi;

   (b) impactul operațional direct al perioadelor de indisponibilitate și riscurile juridice și reputaționale asociate;

   (c) impactul pe care orice întrerupere a activității l-ar putea avea asupra planurilor de venituri ale instituției;

   (d) impactul posibil pe care nerespectarea confidențialității sau o scăpare în integritatea datelor l-ar putea avea asupra instituției și clienților acesteia.

4.2 Obligația de a informa în mod adecvat superiorii

2. Instituțiile care externalizează trebuie să informeze în mod adecvat autoritățile competente despre activitățile importante ce urmează a fi externalizate către furnizori de servicii de tip cloud. Instituțiile trebuie să realizeze acest lucru pe baza punctului 4.3 din ghidul CEBS și, în orice caz, să pună la dispoziția autorităților competente următoarele informații:

   (a) denumirea furnizorului de servicii de tip cloud și denumirea societății sale mamă (dacă este cazul);
   (b) o descriere a activităților și a datelor ce urmează a fi externalizate;
   (c) țara sau țările în care serviciul urmează să fie prestat (inclusiv locația datelor);
   (d) data începerii serviciului;
   (e) ultima dată de reînnoire a contractului (dacă este cazul);
   (f) legea aplicabilă ce guvernează contractul;
   (g) data de expirare a serviciului sau următoarea dată de reînnoire a contractului (dacă este cazul).

3. Ca urmare a informațiilor furnizate în conformitate cu punctul anterior, autoritatea competentă poate cere de la instituția care externalizează mai multe informații legate de analiza sa de risc pentru activitățile importante ce urmează a fi externalizate, cum ar fi:

   (a) dacă furnizorul de servicii de tip cloud are un plan de asigurare a continuității activității potrivit pentru serviciile furnizate instituției care externalizează;
   (b) dacă instituția care externalizează are o strategie de ieșire în caz de reziliere de către oricare dintre părți sau de întrerupere a prestării serviciilor de către furnizorul de servicii de tip cloud;
   (c) dacă instituția care externalizează deține abilitățile și resursele necesare pentru a monitoriza cum se cuvine activitățile externalizate.

4. Instituția care externalizează trebuie să țină un registru de informații actualizat cu privire la toate activitățile sale importante și neimportante externalizate furnizorilor de servicii de tip cloud la nivel de instituție și de grup. Instituția care externalizează trebuie să pună la dispoziția autorității competente, la cerere, o copie a acordului de externalizare și informațiile aferente înregistrate în acest registru, indiferent dacă activitatea externalizată unui furnizor de servicii de tip cloud a fost estimată de instituție ca importantă.

5. În registrul menționat la punctul anterior trebuie incluse cel puțin următoarele informații:

   (a) informațiile menționate la punctul 2 literele (a)-(g), dacă nu au fost deja furnizate;
   (b) tipul de externalizare (modelul de serviciu de tip cloud și modelul de desfășurare în cloud, adică cloud public/privat/hibrid/comunitar);
   (c) părțile care beneficiază de serviciile de tip cloud în baza acordului de externalizare;
   (d) dovada aprobării externalizării de către organul de conducere sau comitetele delegate, dacă este cazul:
   (e) denumirile oricăror subcontractanți, dacă este cazul;
   (f) țara în care este înregistrat furnizorul/principalul subcontractant al serviciului de tip cloud;
   (g) dacă externalizarea a fost evaluată ca importantă (da/nu);
   (h) data ultimei evaluări a importanței activităților externalizate, realizată de instituție;
   (i) dacă furnizorul/subcontractantul (subcontractanții) serviciului de tip cloud susține operațiuni economice care depind de timp (da/nu);
   (j) o evaluare a capacității de substituire a furnizorului de servicii de tip cloud (ușor, dificil sau imposibil de substituit);
   (k) identificarea unui furnizor de servicii alternativ, dacă este posibil;
   (l) data ultimei evaluări a riscurilor externalizării sau ale acordului de subcontractare.

4.3 Drepturile de acces și de audit

Pentru instituții

6. Pe baza orientării 8(2)(g) din ghidul CEBS și în vederea externalizării în cloud, instituțiile care externalizează trebuie să se asigure și că au încheiat un acord scris cu furnizorul de servicii de tip cloud, prin care acesta din urmă să-și asume obligația:

   (a) de a-i furniza instituției, oricărui terț desemnat de instituție în acest scop și auditorului statutar al instituției acces deplin în spațiile sale comerciale (sediu social și centre de operațiuni), inclusiv la gama completă de dispozitive, sisteme, rețele și date utilizate pentru a furniza serviciile externalizate (drept de acces);

   (b) de a-i conferi instituției, oricărui terț desemnat de instituție în acest scop și auditorului statutar al instituției drepturi nerestricționate de inspecție și audit cu privire la serviciile externalizate (drept de audit).

7. Exercitarea efectivă a dreptului de acces și a dreptului de audit nu trebuie stânjenit sau limitat de acorduri contractuale. Dacă realizarea auditurilor sau utilizarea anumitor tehnici de audit ar putea da naștere unui risc pentru mediul unui alt client, vor trebui convenite modalități alternative pentru a oferi un nivel de asigurare similar impus de instituție.

8. Instituția care externalizează trebuie să-și exercite dreptul de audit și dreptul de acces într-o manieră bazată pe risc. În cazul în care o instituție care externalizează nu își folosește propriile resurse de audit, trebuie să ia în considerare utilizarea unuia dintre instrumentele de mai jos:

   (a) audituri centralizate, organizate în comun cu alți clienți ai aceluiași furnizor de servicii de tip cloud și realizate de acești clienți sau de o terță parte numită de aceștia, pentru a utiliza mai eficient resursele de audit și a reduce sarcina organizatorică atât pentru clienți, cât și pentru furnizorul de servicii de tip cloud.

   (b) Certificări de la terțe părți și rapoarte de audit intern sau efectuate de terți, puse la dispoziție de furnizorul de servicii de tip cloud, cu condiția ca:

      i. instituția care externalizează să se asigure că obiectul certificării sau al raportului de audit acoperă sistemele (adică procesele, aplicațiile, infrastructura, centrele de date etc.) și controalele identificate drept cheie de instituția care externalizează.
      ii. instituția care externalizează să evalueze detaliat și în permanență conținutul certificărilor sau al rapoartelor de audit și, în special, să se asigure că versiunile viitoare ale unui raport de audit continuă să acopere controalele-cheie și să verifice dacă certificarea sau raportul de audit nu sunt depășite.
      iii. instituția care externalizează este mulțumită de aptitudinea părții care realizează certificarea sau auditul (de ex. cu privire la rotația societății de certificare sau de audit, calificările, expertiza, reefectuarea/verificarea dovezilor din fișierul de audit ce stă la baza acestuia).

iv. certificările să fie emise și auditurile să fie efectuate conform standardelor recunoscute pe scară largă și să includă un test de eficacitate operațională a controalelor-cheie implementate.

v. instituția care externalizează să aibă dreptul contractual de a solicita extinderea obiectului certificărilor sau al rapoartelor de audit la anumite sisteme și/sau controale care sunt relevante. Numărul și frecvența acestor cereri de modificare a obiectului trebuie să fie rezonabile și legitime din punctul de vedere al gestionării riscurilor.

9. Având în vedere că soluțiile de tip cloud au un nivel ridicat de complexitate tehnică, instituția care externalizează trebuie să verifice dacă personalul care efectuează auditul - care poate consta din auditorii săi interni sau din grupul de auditori care acționează în numele său, sau auditorii desemnați ai furnizorului de servicii de tip cloud - sau, după caz, personalul care revizuiește certificarea realizată de o terță parte sau rapoartele de audit ale furnizorului de servicii are aptitudinile și cunoștințele necesare pentru a efectua audituri și/sau evaluări eficiente și relevante ale soluțiilor de tip cloud.

Pentru autoritățile competente

10. Pe baza orientării 8(2)(h) din ghidul CEBS și în vederea externalizării în cloud, instituțiile care externalizează trebuie să se asigure că au încheiat un acord scris cu furnizorul de servicii de tip cloud, prin care acesta din urmă să își asume obligația:

    (a) de a-i oferi autorității competente ce supraveghează instituția care externalizează (sau orice terță parte numită în acest scop de autoritatea respectivă) acces complet în spațiile comerciale ale furnizorului de servicii de tip cloud (sediul social și centre operaționale), inclusiv la gama completă de dispozitive, sisteme, rețele și date utilizate pentru a furniza serviciile externalizate (drept de acces);

    (b) de a-i conferi autorității competente ce supraveghează instituția care externalizează (sau oricărui terț desemnat în acest scop de autoritatea respectivă) drepturi nerestricționate de inspecție și audit cu privire la serviciile externalizate (drept de audit).

11. Instituția care externalizează trebuie să se asigure că acordurile contractuale nu stânjenesc autoritatea competentă a acesteia în îndeplinirea funcției sale de supraveghere și a obiectivelor sale.

12. Informațiile pe care autoritățile competente le obțin din exercitarea drepturilor de acces și audit trebuie să fie supuse cerințelor de asigurare a secretului profesional și de confidențialitate menționate la articolul 53 și urm. din Directiva 2013/36/UE (CRD IV). Autoritățile competente trebuie să se abțină de la a încheia orice fel de acord contractual sau declarație ce le-ar putea împiedica să respecte prevederile dreptului Uniunii în materie de confidențialitate, secret profesional și schimb de informații.

13. Pe baza constatărilor sale de audit, autoritatea competentă trebuie să abordeze orice deficiențe identificate, dacă va fi necesar, prin impunerea unor măsuri direct asupra instituției care externalizează.

4.4 În special pentru dreptul de acces

14. Acordul menționat la punctele 6 și 10 trebuie să cuprindă următoarele prevederi:

(a) Partea care intenționează să-și exercite dreptul de acces (instituție, autoritate competentă, auditor sau terț care acționează pentru instituție sau autoritatea competentă) trebuie ca, înaintea unei vizite planificate la fața locului, să trimită o notificare într-un termen rezonabil până la vizita la fața locului în spațiul comercial respectiv, mai puțin în cazul în care această notificare prealabilă nu a fost posibilă din cauza unei situații de urgență sau de criză.

(b) Furnizorul de servicii de tip cloud trebuie să coopereze pe deplin cu autoritățile competente adecvate, precum și cu instituția și cu auditorul său în legătură cu vizita la fața locului.

4.5 Securitatea datelor și a sistemelor

15. Așa cum prevede orientarea 8(2)(e) din ghidul CEBS, contractul de externalizare trebuie să oblige furnizorul de servicii externalizate să asigure confidențialitatea informațiilor transmise de instituția financiară. În concordanță cu orientarea 6(6)(e) din ghidul CEBS, instituțiile trebuie să pună în aplicare acorduri pentru a asigura continuitatea serviciilor oferite de furnizorii de servicii externalizate. Pe baza orientărilor 8(2)(b) și 9 din ghidul CEBS, nevoile respective ale instituțiilor care externalizează cu privire la calitate și performanță trebuie menționate în contracte de externalizare în formă scrisă și în acorduri privind nivelul serviciilor. Aceste aspecte de securitate trebuie monitorizate în permanență (orientarea 7).

16. În sensul punctului anterior, instituția trebuie să efectueze, înainte de externalizare și în vederea luării deciziei respective în cunoștință de cauză, cel puțin următoarele:

(a) să identifice și să-și clasifice activitățile, procesele și datele și sistemele asociate în ceea ce privește sensibilitatea și protecțiile necesare;

(b) să efectueze o selecție detaliată bazată pe riscuri a activităților, a proceselor și a datelor și sistemelor asociate referitor la care se ia în calcul externalizarea către o soluție informatică de tip cloud;

(c) să stabilească și să decidă asupra nivelului adecvat de protecție a confidențialității datelor, asupra continuității activităților externalizate și asupra integrității și trasabilității datelor și sistemelor în contextul externalizării de tip cloud vizate. De asemenea, instituțiile trebuie să ia în considerare măsuri specifice atunci când este necesar pentru datele aflate în tranzit, datele din memorie și datele în repaus, cum ar fi

utilizarea tehnologiilor de criptare în combinație cu o arhitectură de management adecvat al cheilor.

17. Ulterior, instituțiile trebuie să se asigure că încheie un acord scris cu furnizorul de servicii de tip cloud în care să se prevadă, printre altele, obligațiile acestuia din urmă conform punctului 16(c).

18. Instituțiile trebuie să monitorizeze în permanență desfășurarea activităților și luarea măsurilor de securitate în acord cu orientarea 7 din ghidul CEBS, inclusiv incidentele, și să revizuiască, după caz, dacă externalizarea activităților respectă punctele anterioare; acestea trebuie să ia imediat măsuri corective necesare.

4.6 Locația datelor și procesarea datelor

19. Așa cum se precizează în orientarea 4(4) din ghidul CEBS, instituțiile trebuie să acorde o atenție specială atunci când încheie și gestionează acorduri de externalizare încheiate în afara SEE din cauza posibilelor riscuri privind protecția datelor și a riscurilor pentru supravegherea eficientă de către autoritatea de supraveghere.

20. Instituția care externalizează trebuie să adopte o abordare bazată pe riscuri în ceea ce privește datele și considerentele legate de locația de prelucrare a datelor atunci când externalizează către un mediu de tip cloud. Evaluarea trebuie să ia în considerare impactul posibil asupra riscurilor, inclusiv riscurile juridice și problemele de conformitate, precum și limitările de supraveghere legate de țările în care serviciile externalizate sunt sau ar putea fi furnizate și în care datele sunt sau ar putea fi stocate. Evaluarea trebuie să cuprindă considerente legate de o mai mare stabilitate politică și de securitate a jurisdicțiilor în discuție; legile în vigoare în aceste jurisdicții (inclusiv legile privind protecția datelor); și prevederile de punere în aplicare a legii, în vigoare în jurisdicțiile respective, inclusiv prevederile legii insolvenței ce s-ar aplica în cazul nerespectării obligațiilor de către un furnizor de servicii de tip cloud. Instituția care externalizează trebuie să se asigure că aceste riscuri sunt menținute în limite acceptabile proporționale cu importanța activității externalizate.

4.7 Externalizarea în lanț

21. Așa cum prevede orientarea 10 din ghidul CEBS, instituțiile trebuie să ia în considerare riscurile asociate externalizării „în lanț” în cazul în care furnizorul de servicii externalizate subcontractează elemente ale serviciului către alți furnizori. Instituția care externalizează trebuie să fie de acord cu externalizarea în lanț numai dacă subcontractantul va respecta la rândul său pe deplin obligațiile existente între instituția care externalizează și furnizorul de servicii externalizate. Mai mult decât atât, instituția care externalizează trebuie să ia măsurile potrivite pentru a aborda riscul oricărui punct slab sau al oricărei nerespectări a obligațiilor în furnizarea activităților subcontractante ce au un efect semnificativ asupra capacității furnizorului de servicii externalizate de a-și respecta obligațiile prevăzute în acordul de externalizare.

22. Acordul de externalizare dintre instituția care externalizează și furnizorul de servicii de tip cloud trebuie să precizeze orice tipuri de activități excluse din posibila subcontractare și să indice faptul că furnizorul de servicii de tip cloud își păstrează întreaga responsabilitate și obligație de supervizare în ceea ce privește serviciile pe care le-a subcontractat.

23. Acordul de externalizare trebuie să includă pentru furnizorul de servicii de tip cloud și obligația de a informa instituția care externalizează despre orice modificări semnificative planificate la nivel de subcontractanți sau de servicii subcontractate precizate în acordul inițial, ce ar putea afecta capacitatea furnizorului de servicii de a-și îndeplini obligațiile asumate prin acordul de externalizare. Perioada de notificare a acestor modificări trebuie convenită dinainte pe cale contractuală pentru a-i permite instituției care externalizează să efectueze o evaluare a riscurilor în ceea ce privește efectele modificărilor propuse înainte ca modificarea efectivă a subcontractanților și a serviciilor subcontractate să intre în vigoare.

24. În cazul în care un furnizor de servicii de tip cloud planifică să facă schimbări privind subcontractantul sau serviciile subcontractate, ce ar avea un efect advers asupra evaluării riscurilor aferente serviciilor agreate, instituția care externalizează trebuie să aibă dreptul de a rezilia contractul.

25. Instituția care externalizează trebuie să revizuiască și să monitorizeze în permanență performanța serviciului în general, indiferent dacă acesta este furnizat de furnizorul de servicii de tip cloud sau de subcontractanții acestuia.

4.8 Planurile de urgență și strategiile de ieșire

26. Așa cum prevăd orientările 6.1, 6(6)(e) și 8(2)(d) din ghidul CEBS, instituția care externalizează trebuie să planifice și să implementeze acorduri pentru menținerea continuității activității sale în cazul în care furnizarea serviciilor de către un furnizor de servicii externalizate eșuează sau se deteriorează într-o măsură inacceptabilă. Aceste aranjamente trebuie sa includă planuri de urgență și o strategie de ieșire clar definită. Mai mult decât atât, contractul de externalizare trebuie să cuprindă o clauză de gestionare a rezilierii și a ieșirii care să permită transferul activităților desfășurate de furnizorul de servicii externalizate către un alt furnizor de servicii externalizate sau reincorporarea lor în instituția care externalizează.

27. O instituție care externalizează trebuie să se asigure că este capabilă să iasă din acordurile de externalizare a serviciilor de tip cloud, dacă va fi necesar, fără nicio întrerupere inoportună în furnizarea serviciilor sale și fără efecte adverse asupra respectării de către aceasta a regimului de reglementare și fără ca ieșirea să se facă în detrimentul continuității sau al calității furnizării sale de servicii clienților. Pentru a realiza acest lucru, o instituție care externalizează trebuie:

    (a) să elaboreze și să implementeze planuri de ieșire complete, documentate și suficient de mult testate, dacă este cazul;

    (b) să identifice soluții alternative și să dezvolte planuri de tranziție care să îi permită să extragă și să transfere activitățile și datele existente de la furnizorul de servicii de tip

cloud la aceste soluții în mod controlat și suficient de testat, ținând cont de problemele de localizare a datelor și de menținerea continuității activității în faza de tranziție;

(c) să se asigure că acordul de externalizare cuprinde o obligație a furnizorului de servicii de tip cloud de a sprijini suficient instituția care externalizează în transferul ordonat al activității către un alt furnizor de servicii de tip cloud sau către conducerea directă a instituției care externalizează în cazul rezilierii acordului de externalizare.

28. La dezvoltarea strategiilor de ieșire, o instituție care externalizează trebuie să ia în considerare următoarele:

(a) să dezvolte indicatori-cheie de risc pentru a identifica un nivel de serviciu inacceptabil;

(b) să efectueze o analiză a impactului economic proporțională cu activitățile externalizate pentru a identifica ce resurse umane și materiale ar fi necesare pentru a implementa planul de ieșire și de cât timp ar fi nevoie;

(c) să aloce roluri și responsabilități pentru gestionarea planurilor de ieșire și a activităților de tranziție;

(d) să definească criteriile de succes ale tranziției.

29. Instituția care externalizează trebuie să includă indicatori care să poată declanșa planul de ieșire în cadrul monitorizării sale permanente a serviciilor și al supravegherii serviciilor oferite de furnizorul de servicii de tip cloud.