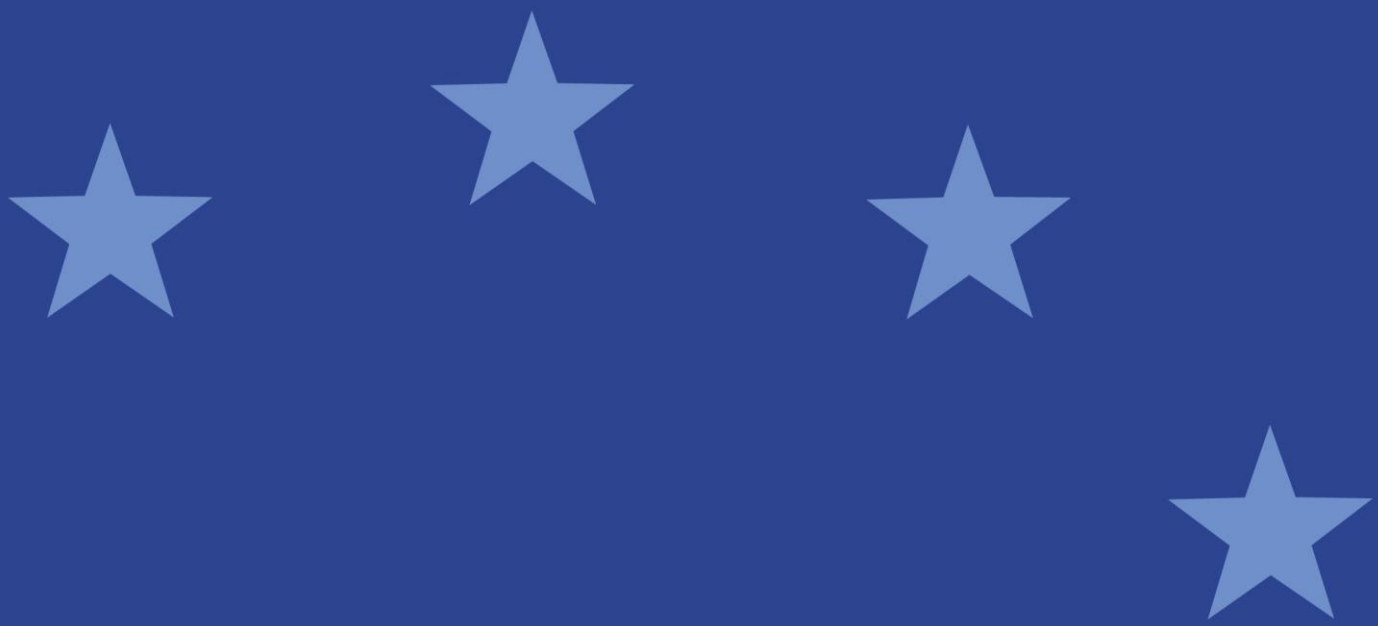
esma European Securities and Markets Authority

Ghid

privind externalizarea către furnizorii de servicii cloud



10/05/2021 | ESMA50-164-4285 RO

Cuprins

I. Domeniu de aplicare 2
II. Referințe legislative, abrevieri și definiții 3
III. Scop 10
IV. Conformitate și obligații de raportare 10
V. Ghid privind externalizarea către furnizorii de servicii cloud 11
Orientarea 1. Guvernanță, supraveghere și documentare 11
Orientarea 2. Analiza de preexternalizare și procesul de diligență 13
Orientarea 3. Elemente contractuale esențiale 15
Orientarea 4. Securitatea informațiilor 16
Orientarea 5. Strategiile de ieșire 17
Orientarea 6. Drepturi de acces și de audit 18
Orientarea 7. Subcontractarea externalizării 20
Orientarea 8. Notificarea scrisă adresată autorităților competente 21
Orientarea 9. Supravegherea angajamentelor de externalizare în cloud 21

I. Domeniu de aplicare

Cui i se adresează?

1. Prezentul ghid se aplică autorităților competente și (i) administratorilor de fonduri de investiții alternative (AFIA) și depozitarilor de fonduri de investiții alternative, (ii) organismelor de plasament colectiv în valori mobiliare (OPCVM), societăților de administrare și depozitarilor OPCVM și societăților de investiții care nu au desemnat o societate de administrare autorizată în conformitate cu Directiva OPCVM (iii) contrapărților centrale (CPC), inclusiv CPC-urilor de nivel 2 din țări terțe care respectă cerințele EMIR relevante, (iv) registrelor centrale de tranzacții (RCT), (v) firmelor de investiții și instituțiilor de credit atunci când desfășoară servicii și activități de investiții, furnizorilor de servicii de raportare a datelor și operatorilor de piață ai locurilor de tranzacționare, (vi) depozitarilor centrali de titluri de valoare (CSD), (vii) agențiilor de rating de credit (ARC), (viii) registrelor centrale de securitizări (RCS) și (ix) administratorilor de indici de referință critici.

2. ESMA va lua în considerare, de asemenea, acest ghid atunci când va evalua măsura în care conformitatea cu cerințele EMIR relevante de către o contraparte centrală de nivel 2 dintr-o țară terță este asigurată de conformitatea sa cu cerințele comparabile din țara terță, în conformitate cu articolul 25 alineatul (2b) litera (a) din EMIR.

Ce se aplică?

3. Prezentul ghid se aplică în legătură cu următoarele dispoziții:

   a) articolele 15, 18, 20 și articolul 21 alineatul (8) din DAFIA; articolele 13, 22, 38, 39, 40, 44, 45, articolul 57 alineatul (1) litera (d), articolul 57 alineatul (2), articolul 57 alineatul (3), articolele 58, 75, 76, 77, 79, 81, 82 și 98 din Regulamentul delegat (UE) 2013/231 al Comisiei;
   b) articolul 12 alineatul (1) litera (a), articolul 13, articolul 14 alineatul (1) litera (c), articolele 22, 22a, articolul 23 alineatul (2), articolele 30 și 31 din Directiva OPCVM; articolul 4 alineatele (1)-(3), articolul 4 alineatul (5), articolul 5 alineatul (2), articolele 7, 9, articolul 23 alineatul (4), articolele 32, 38, 39 și 40 din Directiva 2010/43/UE a Comisiei; articolul 2 alineatul (2) litera (j), articolul 3 alineatul (1), articolul 13 alineatul (2), articolele 15, 16 și 22 din Regulamentul delegat (UE) 2016/438 al Comisiei;
   c) articolul 25, articolul 26 alineatul (1), articolul 26 alineatul (3), articolul 26 alineatul (6), articolele 34, 35 și 78-81 din EMIR; articolele 5 și 12 din SFTR; articolul 3 alineatul (1) litera (f), articolul 3 alineatul (2), articolul 4, articolul 7 alineatul (2) literele (d) și (f), articolele 9 și 17 din Regulamentul delegat (UE) nr. 153/2013 al Comisiei; articolele 16 și 21 din Regulamentul delegat (UE) nr. 150/2013 al Comisiei; articolele 16 și 21 din Regulamentul delegat (UE) 2019/359 al Comisiei;
   d) articolul 16 alineatul (2), articolul 16 alineatul (4), articolul 16 alineatul (5), articolul 18 alineatul (1), articolul 19 alineatul (3) litera (a), articolul 47 alineatul (1)

literele (b) și (c), articolul 48 alineatul (1), articolul 64 alineatul (4), articolul 65 alineatul (5) și articolul 66 alineatul (3)1 din MiFID II; articolul 21 alineatele (1)-(3), articolul 23, articolul 29 alineatul (5), articolele 30, 31 și 32 din Regulamentul delegat (UE) 2017/565 al Comisiei; articolele 6, 15 și articolul 16 alineatul (6) din Regulamentul delegat (UE) 2017/584 al Comisiei; articolele 6, 7, 8 și 9 din Regulamentul delegat (UE) 2017/571 al Comisiei;

e) articolele 22, 26, 30, 42, 44 și 45 of CSDR și articolele 33, 47, articolul 50 alineatul (1), articolul 57 alineatul (2) litera (i), articolele 66, 68, 75, 76, 78 și 80 din Regulamentul delegat (UE) 2017/392 al Comisiei;
f) articolul 9 și anexa I, secțiunea A punctele 4 și 8 și anexa II punctul 17 din Regulamentul ARC și articolele 11 și 25 din Regulamentul delegat (UE) 2012/449 al Comisiei;
g) articolul 10 alineatul (2) din SECR;
h) articolul 6 alineatul (3) și articolul 10 din Regulamentul privind indicii de referință și punctul 7 din anexa I la Regulamentul delegat (UE) 2018/1646 al Comisiei.

Când se aplică?

4. Prezentul ghid se aplică de la 31 iulie 2021 tuturor angajamentelor de externalizare în cloud încheiate, reînnoite sau modificate la această dată sau ulterior. Societățile trebuie să revizuiască și să modifice în consecință angajamentele existente de externalizare în cloud, pentru a se asigura că iau în considerare prezentul ghid până la 31 decembrie 2022. În cazul în care revizuirea angajamentelor de externalizare în cloud a funcțiilor critice sau importante nu este finalizată până la data de 31 decembrie 2022, societățile trebuie să informeze autoritatea competentă corespunzătoare cu privire la acest aspect, precizând inclusiv măsurile avute în vedere pentru a finaliza revizuirea sau pentru posibila strategie de ieșire.

II. Referințe legislative, abrevieri și definiții

Referințe legislative

Regulamentul ESMA	Regulamentul (UE) nr. 1095/2010 al Parlamentului European și al Consiliului din 24 noiembrie 2010 de instituire a Autorității europene de supraveghere (Autoritatea europeană pentru valori mobiliare și piețe), de modificare a Deciziei nr. 716/2009/CE și de abrogare a Deciziei 2009/77/CE a Comisiei[2]
DAFIA	Directiva 2011/61/UE a Parlamentului European și a Consiliului din 8 iunie 2011 privind administratorii fondurilor de investiții alternative și de modificare a Directivelor

[1] Începând cu 1 ianuarie 2022, trimiterea la articolul 64 alineatul (4), la articolul 65 alineatul (5) și la articolul 66 alineatul (3) din MiFID II trebuie interpretată ca referindu-se la articolul 27g alineatul (4), la articolul 27h alineatul (5) și la articolul 27i alineatul (3) din MiFIR.
[2] JO L 331, 15.12.2010, p. 84

	2003/41/CE și 2009/65/CE și a Regulamentelor (CE) nr. 1060/2009 și (UE) nr. 1095/2010[3]
Regulamentul delegat (UE) nr. 231/2013 al Comisiei	Regulamentul delegat (UE) nr. 231/2013 al Comisiei din 19 decembrie 2012 de completare a Directivei 2011/61/UE a Parlamentului European și a Consiliului în ceea ce privește derogările, condițiile generale de operare, depozitarii, efectul de levier, transparența și supravegherea[4]
Directiva OPCVM	Directiva 2009/65/CE a Parlamentului European și a Consiliului din 13 iulie 2009 de coordonare a actelor cu putere de lege și a actelor administrative privind organismele de plasament colectiv în valori mobiliare (OPCVM)[5]
Directiva 2010/43/UE a Comisiei	Directiva 2010/43/UE a Comisiei din 1 iulie 2010 de punere în aplicare a Directivei 2009/65/CE a Parlamentului European și a Consiliului în ceea ce privește cerințele organizatorice, conflictele de interese, regulile de conduită, administrarea riscului și conținutul acordului dintre depozitar și societatea de administrare[6]
Regulamentul delegat (UE 2016/438 al Comisiei	Regulamentul delegat (UE) 2016/438 al Comisiei din 17 decembrie 2015 de completare a Directivei 2009/65/CE a Parlamentului European și a Consiliului în ceea ce privește obligațiile depozitarilor[7]
EMIR	Regulamentul (UE) nr. 648/2012 al Parlamentului European și al Consiliului din 4 iulie 2012 privind instrumentele financiare derivate extrabursiere, contrapărțile centrale și registrele centrale de tranzacții[8]
SFTR	Regulamentul (UE) 2015/2365 al Parlamentului European și al Consiliului din 25 noiembrie 2015 privind transparența operațiunilor de finanțare prin instrumente financiare și transparența reutilizării și de modificare a Regulamentului (UE) nr. 648/2012[9]
Regulamentul delegat (UE) nr. 153/2013 al Comisiei	Regulamentul delegat (UE) nr. 153/2013 al Comisiei din 19 decembrie 2012 privind completarea Regulamentului (UE) nr. 648/2012 al Parlamentului European și al Consiliului, în ceea ce privește standarde tehnice de reglementare privind cerințele pentru contrapărțile centrale[10]

[3] JO L 174, 1.7.2011, p. 1
[4] JO L 83, 22.3.2013, p. 1
[5] JO L 302, 17.11.2009, p. 32
[6] JO L 176, 10.7.2010, p. 42
[7] JO L 78, 24.3.2016, p. 11
[8] JO L 201, 27.7.2012, p. 1
[9] JO L 337, 23.12.2015, p. 1
[10] JO L 52, 23.2.2013, p. 41

Regulamentul delegat (UE) nr. 150/2013 al Comisiei	Regulamentul delegat (UE) nr. 150/2013 al Comisiei din 19 decembrie 2012 de completare a Regulamentului (UE) nr. 648/2012 al Parlamentului European și al Consiliului privind instrumentele financiare derivate extrabursiere, contrapărțile centrale și registrele centrale de tranzacții în ceea ce privește standarde tehnice de reglementare în care se precizează detaliile cererii de înregistrare ca registru central de tranzacții[11]
Regulamentul delegat (UE) 2019/359 al Comisiei	Regulamentul delegat (UE) 2019/359 al Comisiei din 13 decembrie 2018 de completare a Regulamentului (UE) 2015/2365 al Parlamentului European și al Consiliului în ceea ce privește standardele tehnice de reglementare care precizează detaliile cererii de înregistrare ca registru central de tranzacții și de extindere a acestei înregistrări[12]
MiFID II	Directiva 2014/65/UE a Parlamentului European și a Consiliului din 15 mai 2014 privind piețele instrumentelor financiare și de modificare a Directivei 2002/92/CE și a Directivei 2011/61/UE[13]
MiFIR	Regulamentul (UE) nr. 600/2014 al Parlamentului European și al Consiliului din 15 mai 2014 privind piețele instrumentelor financiare și de modificare a Regulamentului (UE) nr. 648/2012[14]
Regulamentul delegat (UE 2017/565 al Comisiei	Regulamentul delegat (UE) 2017/565 al Comisiei din 25 aprilie 2016 de completare a Directivei 2014/65/UE a Parlamentului European și a Consiliului în ceea ce privește cerințele organizatorice și condițiile de funcționare aplicabile firmelor de investiții și termenii definiți în sensul directivei menționate[15]
Regulamentul delegat (UE) 2017/584 al Comisiei	Regulamentul delegat (UE) 2017/584 al Comisiei din 14 iulie 2016 de completare a Directivei 2014/65/UE a Parlamentului European și a Consiliului în ceea ce privește standardele tehnice de reglementare în care sunt precizate cerințele organizatorice pentru locurile de tranzacționare[16]
Regulamentul delegat (UE) 2017/571 al Comisiei	Regulamentul delegat (UE) 2017/571 al Comisiei din 2 iunie 2016 de completare a Directivei 2014/65/UE a Parlamentului European și a Consiliului în ceea ce privește standardele tehnice de reglementare referitoare la autorizarea, cerințele organizatorice și publicarea

[11] JO L 52, 23.2.2013, p. 25
[12] JO L 81, 22.3.2019, p. 45
[13] JO L 173, 12.6.2014, p. 349
[14] JO L 173, 12.6.2014, p. 84
[15] JO L 87, 31.3.2017, p. 1
[16] JO L 87, 31.3.2017, p. 350

	tranzacțiilor pentru furnizorii de servicii de raportare a datelor[17]
CSDR	Regulamentul (UE) nr. 909/2014 din 23 iulie 2014 privind îmbunătățirea decontării titlurilor de valoare în Uniunea Europeană și privind depozitarii centrali de titluri de valoare și de modificare a Directivelor 98/26/CE și 2014/65/UE și a Regulamentului (UE) nr. 236/2012[18]
Regulamentul delegat (UE) 2017/392 al Comisiei	Regulamentul delegat (UE) 2017/392 al Comisiei din 11 noiembrie 2016 de completare a Regulamentului (UE) nr. 909/2014 al Parlamentului European și al Consiliului cu privire la standarde tehnice de reglementare în materie de autorizare, supraveghere și cerințe operaționale pentru depozitarii centrali de titluri de valoare[19]
Regulamentul ARC	Regulamentul (CE) nr. 1060/2009 al Parlamentului European și al Consiliului din 16 septembrie 2009 privind agențiile de rating de credit[20]
Regulamentul delegat (UE) nr. 449/2012 al Comisiei	Regulamentul delegat (UE) nr. 449/2012 al Comisiei din 21 martie 2012 de completare a Regulamentului (CE) nr. 1060/2009 al Parlamentului European și al Consiliului în ceea ce privește standardele tehnice de reglementare privind informațiile care trebuie furnizate pentru înregistrarea și certificarea agențiilor de rating de credit[21]
SECR	Regulamentul (UE) 2017/2402 al Parlamentului European și al Consiliului din 12 decembrie 2017 de stabilire a unui cadru general privind securitizarea și de creare a unui cadru specific pentru o securitizare simplă, transparentă și standardizată, și de modificare a Directivelor 2009/65/CE, 2009/138/CE și 2011/61/UE, precum și a Regulamentelor (CE) nr. 1060/2009 și (UE) nr. 648/2012[22]
Regulamentul privind indicii de referință	Regulamentul (UE) 2016/1011 al Parlamentului European și al Consiliului din 8 iunie 2016 privind indicii utilizați ca indici de referință în cadrul instrumentelor financiare și al contractelor financiare sau pentru a măsura performanțele fondurilor de investiții și de modificare a Directivelor 2008/48/CE și 2014/17/UE și a Regulamentului (UE) nr. 596/2014[23]

[17] JO L 87, 31.3.2017, p. 126
[18] JO L 257, 28.8.2014, p. 1
[19] JO L 65, 10.3.2017, p. 48
[20] JO L 302, 17.11.2009, p. 1.
[21] JO L 140, 30.5.2012, p. 32
[22] JO L 347, 28.12.2017, p. 35.
[23] JO L 171, 29.6.2016, p. 1

Regulamentul delegat (UE) 2018/1646 al Comisiei	Regulamentul delegat (UE) 2018/1646 al Comisiei din 13 iulie 2018 de completare a Regulamentului (UE) 2016/1011 al Parlamentului European și al Consiliului în ceea ce privește standardele tehnice de reglementare pentru informațiile care trebuie furnizate într-o cerere de autorizare și într-o cerere de înregistrare[24]
RGPD	Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE[25]

Abrevieri

FSC	Furnizor de servicii cloud
ESMA	Autoritatea Europeană pentru Valori Mobiliare și Piețe
UE	Uniunea Europeană

Definiții

funcție	orice procese, servicii sau activități;
funcție critică sau importantă	orice funcție a cărei anomalie sau deficiență în îndeplinirea sa ar compromite considerabil: a) respectarea de către societate a obligațiilor sale în temeiul legislației aplicabile; b) performanța financiară a unei societăți sau c) viabilitatea sau continuitatea principalelor servicii și activități ale unei societăți;
servicii cloud	servicii furnizate utilizând cloud computing;
cloud computing sau cloud[26]	o paradigmă care permite accesul în rețea la un bazin scalabil și elastic de resurse fizice sau virtuale care pot fi partajate (de exemplu servere, sisteme de operare, rețele, software, aplicații și echipamente de stocare) cu funcție de auto-service și de administrare la cerere;
furnizor de servicii cloud	un terț care furnizează servicii cloud în cadrul unui angajament de externalizare în cloud;

[24] JO L 274, 5.11.2018, p. 43
[25] JO L 119, 4.5.2016, p. 1-88
[26] Cloud computing este adesea abreviat în „cloud”. Termenul „cloud” este utilizat în restul documentului pentru a facilita lectura.

angajament de externalizare în cloud	un angajament sub orice formă, inclusiv acorduri de delegare, între: (i) o societate și un FSC prin care respectivul FSC îndeplinește o funcție care altfel ar fi asumată de societatea însești sau (ii) o societate și un terț care nu este un FSC, dar care se bazează în mod semnificativ pe un FSC pentru a îndeplini o funcție care altfel ar fi asumată de societatea însești. În acest caz, o trimitere la un „FSC" în acest ghid trebuie interpretată ca referindu-se la un astfel de terț.
subcontractare a serviciilor externalizate	o situație în care FSC transferă mai departe funcția externalizată (sau o parte a acestei funcții) către un alt furnizor de servicii în cadrul unui angajament de externalizare;
model de implementare în cloud	modul în care cloudul poate fi organizat pe baza controlului și partajării resurselor fizice sau virtuale. Modelele de implementare în cloud includ cloudul comunitar[27], hibrid[28], privat[29] și public[30];
societăți	a) administratori de fonduri de investiții alternative sau „AFIA", astfel cum sunt definiți la articolul 4 alineatul (1) litera (b) din DAFIA și depozitari, astfel cum se menționează la articolul 21 alineatul (3) din DAFIA („depozitari de fonduri de investiții alternative"); b) societăți de administrare, astfel cum sunt definite la articolul 2 alineatul (1) litera (b) din Directiva OPCVM („societăți de administrare OPCVM") și depozitari, astfel cum sunt definiți la articolul 2 alineatul (1) litera (a) din Directiva OPCVM („depozitari ai OPCVM"); c) contrapărți centrale (CPC), astfel cum sunt definite la articolul 2 alineatul (1) din EMIR

[27] Un model de implementare în cloud în care serviciile cloud acceptă și sunt partajate exclusiv printr-un grup specific de clienți ai serviciilor cloud care au cerințe comune și o relație de reciprocitate și unde resursele sunt controlate de cel puțin un membru al acestui grup.
[28] Un model de implementare în cloud care utilizează cel puțin două modele diferite de implementare în cloud.
[29] Un model de implementare în cloud în care serviciile cloud sunt utilizate exclusiv de un singur client de servicii cloud, iar resursele sunt controlate de respectivul client de servicii cloud.
[30] Un model de implementare în cloud în care serviciile cloud sunt potențial disponibile pentru orice client de servicii cloud, iar resursele sunt controlate de furnizorul de servicii cloud.

și contrapărți centrale de nivel 2 din țări terțe, în sensul articolului 25 alineatul (2a) din EMIR, care respectă cerințele EMIR relevante în conformitate cu articolul 25 alineatul (2b) litera (a) din EMIR;

d) registre centrale de tranzacții, astfel cum sunt definite la articolul 2 alineatul (2) din EMIR și la articolul 3 alineatul (1) din SFTR;

e) firme de investiții, astfel cum sunt definite la articolul 4 alineatul (1) punctul 1 din MiFID II și instituții de credit, astfel cum sunt definite la articolul 4 alineatul (1) punctul 27 din MiFID II, atunci când prestează servicii și activități de investiții în sensul articolului 4 alineatul (1) punctul 2 din MiFID II;

f) furnizori de servicii de raportare a datelor, astfel cum sunt definiți la articolul 4 alineatul (1) punctul 63 din MiFID II[31];

g) operatori de piață ai locurilor de tranzacționare în sensul articolului 4 alineatul (1) punctul 24 din MiFID II;

h) depozitari centrali de titluri de valoare (CSD), astfel cum sunt definiți la articolul 2 alineatul (1) punctul 1 din CSDR;

i) agenții de rating de credit, astfel cum sunt definite la articolul 3 alineatul (1) litera (b) din Regulamentul ARC;

j) registre centrale de securitizări, astfel cum sunt definite la articolul 2 punctul 23 din SECR;

k) administratori de indici de referință critici, astfel cum sunt definiți la articolul 3 alineatul (1) punctul 25 din Regulamentul privind indicii de referință.

[31] Începând cu 1 ianuarie 2022, trimiterea la această dispoziție trebuie interpretată ca o trimitere la articolul 2 alineatul (1) punctul 36 litera (a) din MiFIR.

III. Scop

5. Ghidul este elaborat în temeiul articolului 16 alineatul (1) din Regulamentul ESMA. Obiectivele prezentului ghid sunt de a stabili practici de supraveghere coerente, eficiente și eficace în cadrul Sistemului european de supraveghere financiară (SESF) și de a asigura aplicarea comună, uniformă și consecventă a cerințelor menționate în secțiunea 1.1 de la rubrica „Ce se aplică?” atunci când societățile externalizează către FSC-uri. În special, aceste ghiduri au scopul de a ajuta societățile și autoritățile competente să identifice, să abordeze și să monitorizeze riscurile și provocările care decurg din angajamentele de externalizare în cloud, de la luarea deciziei de externalizare, selectarea unui furnizor de servicii cloud, monitorizarea activităților externalizate până la furnizarea de strategii de ieșire.

IV. Conformitate și obligații de raportare

Statutul ghidului

6. Conform articolului 16 alineatul (3) din Regulamentul ESMA, autoritățile competente și societățile trebuie să depună toate eforturile necesare pentru a respecta ghidul.

7. Autoritățile competente cărora li se aplică prezentul ghid trebuie să se conformeze prin includerea lui în cadrele lor juridice și/sau de supraveghere naționale, după caz, inclusiv în cazul în care ghiduri specifice vizează, în principal, societățile. În acest caz, autoritățile competente trebuie să asigure, prin activități de supraveghere, respectarea ghidului de către societăți.

8. Prin supravegherea sa continuă directă, ESMA va evalua aplicarea acestui ghid de agențiile de rating, de registrele centrale de tranzacții, de registrele centrale de securitizări, de contrapărțile centrale de nivel 2 din țările terțe și, de la 1 ianuarie 2022, de furnizorii de servicii de raportare a datelor și de administratorii de indici UE de referință critici.

Cerințe de raportare

9. În termen de două luni de la data publicării ghidului pe site-ul ESMA în toate limbile oficiale ale UE, autoritățile competente cărora li se aplică prezentul ghid trebuie să informeze ESMA (i) dacă respectă ghidul, (ii) dacă nu respectă, dar intenționează să respecte ghidul sau (iii) dacă nu respectă și nu intenționează să respecte ghidul.

10. În caz de neconformitate, autoritățile competente trebuie, de asemenea, să informeze ESMA în termen de două luni de la data publicării ghidului pe site-ul ESMA în toate limbile oficiale ale UE cu privire la motivele de neconformare cu ghidul. Pe site-ul ESMA este disponibil un model de notificare. Odată ce a fost completat, modelul va fi transmis la ESMA.

11. Societățile nu sunt obligate să raporteze dacă respectă sau nu prezentul ghid.

V. Ghid privind externalizarea către furnizorii de servicii cloud

Orientarea 1. Guvernanță, supraveghere și documentare

12. O societate trebuie să aibă o strategie de externalizare în cloud definită și actualizată, care să fie compatibilă cu strategiile relevante și cu politicile și procesele interne ale societății, inclusiv în ceea ce privește tehnologia informației și comunicațiilor, securitatea informațiilor și gestionarea riscurilor operaționale.

13. O societate trebuie:

a) să atribuie clar responsabilitățile în cadrul organizației pentru documentarea, gestionarea și controlul angajamentelor de externalizare în cloud;
b) să aloce resurse suficiente pentru a asigura respectarea acestui ghid și a tuturor cerințelor legale aplicabile angajamentelor sale de externalizare în cloud;
c) să instituie o funcție de supraveghere a externalizării în cloud sau să desemneze membri ai personalului de nivel superior care să se afle în directa subordine a organului de conducere și să răspundă de gestionarea și supravegherea riscurilor aranjamentelor de externalizare în cloud. Atunci când respectă acest ghid, societățile trebuie să țină seama de natura, amploarea și complexitatea activității lor, inclusiv în ceea ce privește riscul pentru sistemul financiar și riscurile inerente funcțiilor externalizate, și să se asigure că organul lor de conducere deține competențele tehnice relevante pentru a înțelege riscurile pe care presupun angajamentele de externalizare în cloud[32]. Societățile mici și mai puțin complexe trebuie să asigure cel puțin o repartizare clară a sarcinilor și responsabilităților pentru gestionarea și supravegherea angajamentelor de externalizare în cloud.

14. O societate trebuie să monitorizeze performanța activităților, măsurile de securitate și respectarea de către FSC-urile sale a nivelurilor de servicii convenite. Această monitorizare trebuie să se bazeze pe riscuri, acordând o atenție deosebită funcțiilor critice sau importante care au fost externalizate.

[32] Pentru firmele de investiții și instituțiile de credit, vezi „Ghid comun ESMA și ABE privind evaluarea adecvării membrilor organului de conducere și a persoanelor care dețin funcții cheie în conformitate cu Directiva 2013/36/UE și Directiva 2014/65/UE” (EBA/GL/2017/12).

15. O societate trebuie să reevalueze dacă aranjamentele sale de externalizare în cloud vizează o funcție critică sau importantă, periodic și ori de câte ori riscul, natura sau amploarea unei funcții externalizate s-a modificat substanțial.

16. O societate trebuie să mențină un registru actualizat de informații cu privire la toate angajamentele sale de externalizare în cloud, făcând distincție între externalizarea funcțiilor critice sau importante și alte angajamente de externalizare. Atunci când face distincția între externalizarea funcțiilor critice sau importante și alte angajamente de externalizare, aceasta trebuie să furnizeze un scurt rezumat al motivelor pentru care funcția externalizată este sau nu este considerată critică sau importantă. Ținând seama de legislația națională, o societate trebuie să țină, de asemenea, o evidență a angajamentelor de externalizare în cloud reziliate, pentru o perioadă de timp adecvată.

17. În cazul angajamentelor de externalizare în cloud care vizează funcții critice sau importante, registrul trebuie să conțină cel puțin următoarele informații pentru fiecare angajament de externalizare:

    a) un număr de referință;
    b) data de începere și, după caz, următoarea dată de reînnoire a contractului, data de încetare și/sau perioadele de preaviz pentru FSC și pentru societate;
    c) o scurtă descriere a funcției externalizate, inclusiv datele externalizate și dacă aceste date conțin date cu caracter personal (de exemplu, prin furnizarea unui răspuns de tip „Da” sau „Nu” într-un câmp de date separat);
    d) o categorie atribuită de societate care reflectă natura funcției externalizate (de exemplu, funcția de tehnologia informației, funcția de control), care trebuie să faciliteze identificarea diferitelor tipuri de angajamente de externalizare în cloud;
    e) dacă funcția externalizată sprijină operațiuni de afaceri care sunt critice din punct de vedere al timpului;
    f) numele și numele de marcă (dacă este cazul) al FSC, țara sa de înregistrare, numărul de înregistrare, identificatorul entității juridice (dacă este disponibil), adresa sa înregistrată, datele sale de contact relevante, precum și denumirea societății-mamă (dacă este cazul);
    g) legea de reglementare a angajamentului de externalizare în cloud și, dacă există, alegerea jurisdicției;
    h) tipul de servicii cloud și modele de implementare și natura specifică a datelor care trebuie păstrate și locațiile (și anume, regiunile sau țările) în care pot fi stocate aceste date;
    i) data celei mai recente evaluări a caracterului critic sau a importanței funcției externalizate și data următoarei evaluări planificate;
    j) data celei mai recente evaluări a riscului/celui mai recent audit al FSC, împreună cu un scurt rezumat al principalelor rezultate, și data următoarei evaluări planificate/următorului audit planificat;
    k) persoana fizică sau organul de decizie din cadrul societății care a aprobat angajamentul de externalizare în cloud;
    l) dacă este cazul, numele oricărui subcontractant căruia îi este externalizată în lanț o funcție critică sau importantă (sau părți substanțiale ale acesteia), inclusiv țările

în care sunt înregistrați subcontractanții, unde va fi prestat serviciul subcontractat și locațiile (și anume, regiunile sau țările) în care vor fi stocate datele;

m) costul bugetar anual estimat al angajamentului de externalizare în cloud.

18. În cazul angajamentelor de externalizare în cloud referitoare la funcții necritice sau neimportante, o societate trebuie să definească informațiile care trebuie incluse în registru pe baza naturii, amplorii și complexității riscurilor inerente funcției externalizate.

Orientarea 2. Analiza de preexternalizare și procesul de diligență

19. Înainte de a încheia orice angajament de externalizare în cloud, o societate trebuie:

a) să evalueze dacă angajamentul de externalizare în cloud privește o funcție critică sau importantă;
b) să identifice și să evalueze toate riscurile relevante ale angajamentului de externalizare în cloud;
c) să efectueze procesul de diligență corespunzător asupra FSC-ului potențial;
d) să identifice și să evalueze orice conflict de interese pe care îl poate genera externalizarea.

20. Analiza de preexternalizare și procesul de diligență asupra potențialului FSC trebuie să fie proporționale cu natura, amploarea și complexitatea funcției pe care societatea intenționează să o externalizeze și cu riscurile inerente acestei funcții. Aceasta trebuie să conțină cel puțin o evaluare a impactului potențial al angajamentului de externalizare în cloud asupra riscurilor operaționale, juridice, de conformitate și reputaționale ale societății.

21. În cazul în care angajamentul de externalizare în cloud privește funcții critice sau importante, o societate trebuie, de asemenea:

a) să evalueze toate riscurile relevante care pot apărea ca urmare a angajamentului de externalizare în cloud, inclusiv riscurile legate de tehnologia informației și comunicațiilor, de securitatea informațiilor, continuitatea activității, legalitate și conformitate, riscurile reputaționale, riscurile operaționale și posibile limitări în materie de supraveghere pentru societate, care rezultă din:
   i. serviciul cloud selectat și modelele de implementare propuse;
   ii. migrația și/sau procesul de implementare;
   iii. sensibilitatea funcției și a datelor conexe care sunt avute în vedere pentru a fi externalizate și măsurile de securitate care trebuie luate;
   iv. interoperabilitatea sistemelor și aplicațiilor societății și ale FSC, și anume capacitatea lor de a face schimb de informații și de a utiliza reciproc informațiile care au făcut obiectul unui schimb;
   v. portabilitatea datelor societății, și anume capacitatea de a transfera cu ușurință datele societății de la un FSC la altul sau înapoi către societate;
   vi. stabilitatea politică, situația de securitate și sistemul juridic (inclusiv dispozițiile în vigoare în materie de aplicare a legii, dispozițiile legale privind insolvența care s-ar aplica în caz de faliment al FSC, legislația în vigoare privind protecția datelor și îndeplinirea condițiilor pentru transferul datelor

cu caracter personal într-o țară terță conform RGPD) în țările (din interiorul sau din afara UE) în care ar fi furnizate funcțiile externalizate și în care ar fi stocate datele externalizate; în cazul subcontractării, riscurile suplimentare care pot apărea dacă subcontractantul se află într-o țară terță sau într-o țară diferită de cea a FSC și, în cazul unui lanț de subcontractare, orice risc suplimentar care poate apărea, inclusiv în legătură cu absența unui contract direct între societate și subcontractantul care realizează funcția externalizată;

vii. concentrarea posibilă în cadrul societății (inclusiv, după caz, la nivelul grupului său), cauzată de angajamente multiple de externalizare în cloud cu același FSC, precum și concentrarea posibilă în cadrul sectorului financiar al UE, cauzată de situația în care mai multe societăți folosesc același FSC sau un grup mic de FSC-uri. La evaluarea riscului de concentrare, societatea trebuie să aibă în vedere toate angajamentele sale de externalizare în cloud (și, dacă este cazul, angajamentele de externalizare în cloud la nivelul grupului său) cu respectivul FSC.

b) să țină seama de beneficiile și costurile preconizate ale angajamentului de externalizare în cloud, inclusiv cântărirea oricăror riscuri semnificative care pot fi reduse sau mai bine gestionate împotriva oricăror riscuri semnificative care pot apărea ca urmare a angajamentului de externalizare în cloud.

22. În cazul externalizării de funcții critice sau importante, procesul de diligență trebuie să includă o evaluare a adecvării FSC. La evaluarea adecvării FSC, o societate trebuie să se asigure că FSC are o bună reputație în afaceri, deține abilitățile, resursele (de exemplu, resurse umane, informatice și financiare), structura organizatorică și, dacă este cazul, autorizația (autorizațiile) sau înregistrarea (înregistrările) relevantă (relevante) necesare pentru a îndeplini în mod fiabil și profesional funcția critică sau importantă și a-și respecta obligațiile pe durata angajamentului de externalizare în cloud. Factorii suplimentari care trebuie avuți în vedere în cadrul procesului de diligență cu privire la FSC conțin, dar nu se limitează la:

a) gestionarea securității informațiilor și, în special, protecția datelor cu caracter personal, confidențiale sau sensibile în alt mod;
b) asistența pentru servicii, inclusiv planurile și contactele de asistență și procesele de gestionare a incidentelor;
c) planurile de asigurare a continuității activității și planurile de recuperare în caz de dezastru;

23. Acolo unde este cazul și pentru a sprijini procesul de diligență efectuat, o societate poate utiliza, de asemenea, certificări bazate pe standarde internaționale și rapoarte de audit externe sau interne.

24. Dacă o societate ia cunoștință de deficiențe semnificative și/sau de modificări semnificative ale serviciilor furnizate sau ale situației FSC, analiza de preexternalizare și procesul de diligență privind FSC trebuie revizuite imediat sau, dacă este necesar, reluate.

25. În cazul în care încheie un nou angajament de externalizare sau reînnoiește un angajament existent cu un FSC care a fost deja evaluat, societatea trebuie să stabilească, pe baza unei abordări bazate pe riscuri, dacă este necesar un nou proces de diligență.

Orientarea 3. Elemente contractuale esențiale

26. Drepturile și obligațiile care le revin unei societăți și furnizorului de servicii cloud trebuie să fie clar definite printr-un acord scris.

27. Acordul scris trebuie să acorde în mod expres societății posibilitatea de a-l rezilia, atunci când este necesar.

28. În cazul externalizării unor funcții critice sau importante, acordul scris trebuie să conțină cel puțin:

    a) o descriere clară a funcției externalizate;

    b) data de începere și data de încetare a acordului, după caz, și perioadele de preaviz pentru FSC și pentru întreprindere;

    c) legea de reglementare a acordului și, dacă există, alegerea jurisdicției;

    d) obligațiile financiare ale societății și ale FSC;

    e) dacă este permisă subcontractarea și, dacă da, în ce condiții, având în vedere Orientarea 7;

    f) locația (locațiile) (și anume, regiunile sau țările) în care va fi asigurată funcția externalizată și în care vor fi păstrate și prelucrate datele, precum și condițiile care trebuie îndeplinite, inclusiv cerința de a notifica societatea dacă FSC propune schimbarea locației (locațiilor);

    g) dispoziții privind securitatea informațiilor și protecția datelor cu caracter personal, având în vedere Orientarea 4;

    h) dreptul societății de a monitoriza în mod regulat performanța FSC în cadrul angajamentului de externalizare în cloud, având în vedere Orientarea 6;

    i) nivelurile serviciilor convenite, care trebuie să includă obiective de performanță cantitative și calitative, pentru a permite o monitorizare în timp util, astfel încât, dacă nu sunt respectate nivelurile serviciilor convenite, să se poată lua măsuri corective adecvate, fără întârzieri nejustificate;

    j) obligațiile de raportare ale FSC față de societate și, după caz, obligațiile de a prezenta rapoarte relevante pentru funcția de securitate și funcțiile esențiale ale societății, precum rapoarte întocmite de funcția de audit intern a FSC;

    k) dispoziții privind gestionarea incidentelor de către FSC, inclusiv obligația FSC de a raporta societății, fără întârzieri nejustificate, incidentele care au afectat funcționarea serviciului contractat al societății;

l) dacă FSC trebuie să încheie o asigurare obligatorie împotriva anumitor riscuri și, dacă este cazul, nivelul asigurării necesare;

m) cerințele pentru ca FSC să implementeze și să testeze continuitatea activității și planurile de recuperare în caz de dezastru;

n) cerința ca FSC să acorde societății, autorităților sale competente și oricărei alte persoane desemnate de societate sau autorităților competente dreptul de a accesa („drepturi de acces") și de a inspecta („drepturi de audit") informațiile, sediile, sistemele și dispozitivele relevante ale FSC în măsura necesară pentru a monitoriza performanța FSC în cadrul angajamentului de externalizare în cloud și conformitatea sa cu cerințele de reglementare și contractuale aplicabile, având în vedere Orientarea 6;

o) dispoziții prin care să se asigure că datele pe care FSC le prelucrează sau le stochează în numele societății pot fi accesate, recuperate și returnate societății după caz, având în vedere Orientarea 5.

Orientarea 4. Securitatea informațiilor

29. O societate trebuie să stabilească cerințe de securitate a informațiilor în politicile și procedurile sale interne și în cadrul acordului scris de externalizare în cloud și să monitorizeze în permanență respectarea acestor cerințe, inclusiv pentru a proteja datele confidențiale, cu caracter personal sau alte date sensibile. Aceste cerințe trebuie să fie proporționale cu natura, amploarea și complexitatea funcției pe care societatea o externalizează către FSC și cu riscurile inerente acestei funcții.

30. În acest scop, în cazul externalizării unor funcții critice sau importante și fără a aduce atingere cerințelor aplicabile conform RGPD, o societate care aplică o abordare bazată pe riscuri trebuie, cel puțin:

a) *organizarea în domeniul securității informațiilor:* să se asigure că există o alocare clară a rolurilor și responsabilităților în materie de securitate a informațiilor între societate și FSC, inclusiv în ceea ce privește detectarea amenințărilor, gestionarea incidentelor și gestionarea patch-urilor, și să se asigure că FSC este capabil efectiv să își îndeplinească rolurile și responsabilitățile;
b) *gestionarea identității și accesului*: să se asigure că există mecanisme robuste de autentificare (de exemplu, autentificare dublă) și controale ale accesului, pentru a preveni accesul neautorizat la datele și la resursele de cloud back-end ale societății;
c) *criptarea și gestionarea cheilor de securitate:* să se asigure că tehnologiile de criptare relevante sunt utilizate, acolo unde este necesar, pentru date în tranzit, date în memorie, date în repaus și copii de rezervă ale datelor, în combinație cu soluții adecvate de gestionare a cheilor de securitate pentru a limita riscul accesului neautorizat la cheile de criptare; în special, societatea trebuie să aibă în vedere tehnologia și procesele de ultimă generație atunci când își alege soluția de gestionare a cheilor de securitate;
d) *securitatea operațiunilor și a rețelei:* să ia în considerare nivelurile adecvate de disponibilitate a rețelei, segregarea rețelei [de exemplu, izolarea „chiriașilor" în

mediul partajat al cloudului, separarea operațională în ceea ce privește webul, logica aplicației, sistemul de operare, rețeaua, sistemul de gestionare a bazei de date (DBMS) și straturile de stocare] și mediile de procesare (de exemplu, testarea acceptării de către utilizator, dezvoltare, producție);

e) *interfețe de programare a aplicațiilor (API):* să ia în considerare mecanismele de integrare a serviciilor cloud cu sistemele societății, pentru a asigura securitatea API-urilor (de exemplu, stabilirea și menținerea politicilor și procedurilor de securitate a informațiilor pentru API-uri pe mai multe interfețe de sistem, jurisdicții și funcții comerciale pentru a preveni divulgarea, modificarea sau distrugerea neautorizată a datelor);
f) *continuitatea afacerii și recuperarea în caz de dezastru*: să se asigure că există controale efective de continuitate a activității și de recuperare în caz de dezastru (de exemplu, prin stabilirea de cerințe minime de capacitate, selectarea opțiunilor de găzduire care sunt răspândite geografic, cu capacitatea de a comuta de la una la alta, sau solicitarea și revizuirea documentației care descrie ruta de transport a datelor societății între sistemele FSC, precum și luarea în considerare a posibilității de a reproduce imagini mecanice într-o locație de stocare independentă, care să fie suficient de bine izolată de rețea sau deconectată);
g) *localizarea datelor*: să adopte o abordare bazată pe riscuri în ceea ce privește locația (locațiile) de stocare și prelucrare a datelor (și anume, regiuni sau țări);
h) *conformitate și monitorizare*: să verifice dacă FSC respectă standardele de securitate a informațiilor recunoscute la nivel internațional și dacă a implementat controale adecvate de securitate a informațiilor (de exemplu, obligația FSC de a furniza dovezi că efectuează revizuiri relevante ale securității informațiilor și efectuarea de evaluări și teste periodice ale mecanismelor FSC de securitate a informațiilor).

Orientarea 5. Strategiile de ieșire

31. În cazul externalizării unor funcții critice sau importante, o societate trebuie să se asigure că este capabilă să iasă din angajamentul de externalizare în cloud fără întreruperi nejustificate ale activităților și serviciilor sale către clienții săi și fără a aduce atingere respectării obligațiilor sale în temeiul dispozițiilor aplicabile și fără a afecta confidențialitatea, integritatea și disponibilitatea datelor sale. În acest scop, o societate trebuie:

a) să elaboreze planuri de ieșire cuprinzătoare, documentate și suficient de mult testate. Aceste planuri trebuie actualizate după necesități, inclusiv în cazul unor modificări aduse funcției externalizate;
b) să identifice soluții alternative și să elaboreze planuri de tranziție pentru a elimina funcția și datele externalizate de la FSC și, după caz, de la orice subcontractant și să le transfere către FSC-ul alternativ indicat de societate sau direct înapoi către societate. Aceste soluții trebuie definite în raport cu provocările care pot apărea din cauza locației datelor, luând măsurile necesare pentru a asigura continuitatea activității în faza de tranziție;
c) să se asigure că acordul scris de externalizare în cloud include o obligație pentru FSC de a sprijini transferul ordonat al funcției externalizate și prelucrarea conexă

a datelor, de la FSC și orice subcontractant către un alt FSC, indicat de societate sau direct către societate, în cazul în care societatea activează strategia de ieșire. Obligația de a sprijini transferul ordonat al funcției externalizate și tratamentul aferent al datelor trebuie să includă, după caz, ștergerea în siguranță a datelor din sistemele FSC și ale oricărui subcontractant.

32. La elaborarea planurilor și soluțiilor de ieșire menționate la literele (a) și (b) de mai sus („strategia de ieșire”), societatea trebuie să aibă în vedere următoarele:

    a) să definească obiectivele strategiei de ieșire;
    b) să definească evenimentele declanșatoare care ar putea activa strategia de ieșire. Aceste evenimente trebuie să includă cel puțin încetarea angajamentului de externalizare în cloud la inițiativa societății sau a FSC, precum și oprirea sau o altă întrerupere gravă a activității comerciale a FSC;
    c) să efectueze o analiză a impactului economic, care să fie proporțională cu funcția externalizată, pentru a identifica ce resurse umane și de altă natură ar fi necesare pentru a implementa strategia de ieșire;
    d) să atribuie roluri și responsabilități pentru gestionarea strategiei de ieșire;
    e) să testeze caracterul oportun al strategiei de ieșire, folosind o abordare bazată pe riscuri (de exemplu, prin efectuarea unei analize a costurilor potențiale, a impactului, a resurselor și a implicațiilor temporale ale transferului unui serviciu externalizat către un furnizor alternativ);
    f) să definească criteriile de succes ale tranziției.

33. O societate trebuie să includă indicatori ai evenimentelor declanșatoare ale strategiei de ieșire în monitorizarea și supravegherea sa continuă a serviciilor furnizate de FSC în temeiul angajamentului de externalizare în cloud.

Orientarea 6. Drepturi de acces și de audit

34. O societate trebuie să se asigure că acordul scris de externalizare în cloud nu limitează exercitarea efectivă a drepturilor de acces și de audit ale societății și ale autorității competente și nici opțiunile de supraveghere asupra FSC.

35. O societate trebuie să se asigure că exercitarea drepturilor de acces și de audit (de exemplu, frecvența auditurilor și domeniile și serviciile de auditat) ia în considerare dacă externalizarea este legată de o funcție critică sau importantă, precum și natura și amploarea riscurilor și impactul care decurge din angajamentul de externalizare în cloud asupra societății.

36. În cazul în care exercitarea drepturilor de acces sau de audit sau utilizarea anumitor tehnici de audit creează un risc pentru mediul FSC și/sau pentru un alt client al FSC (de exemplu, prin impactul asupra nivelurilor serviciilor, confidențialității, integrității și disponibilității datelor), FSC trebuie să ofere societății o justificare clară a motivului pentru care acest lucru ar crea un risc, iar FSC trebuie să convină cu societatea asupra unor modalități alternative de a obține un rezultat similar [de exemplu, includerea unor

mecanisme de control specifice care să fie testate într-un raport specific/certificare specifică elaborat(ă) de FSC].

37. Fără a aduce atingere responsabilității lor finale cu privire la angajamentele de externalizare în cloud, pentru a utiliza mai eficient resursele de audit și pentru a reduce povara organizatorică asupra FSC și clienților săi, societățile pot utiliza:

    a) certificări de la terți și rapoarte de audit intern sau extern efectuate de terți, puse la dispoziție de FSC;
    b) audituri centralizate efectuate împreună cu alți clienți ai aceluiași FSC sau audituri centralizate efectuate de un terț auditor desemnat de mai mulți clienți ai aceluiași FSC.

38. În cazul externalizării unor funcții critice sau importante, societățile trebuie să evalueze dacă certificările de la terți și rapoartele de audit intern sau extern menționate la punctul 37 litera (a) sunt adecvate și suficiente pentru a se conforma obligațiilor sale în temeiul legislației aplicabile și, în timp, trebuie să urmărească să nu se bazeze doar pe aceste certificări și rapoarte.

39. În cazul externalizării unor funcții critice sau importante, o societate trebuie să utilizeze certificările de la terți și rapoartele de audit intern sau extern menționate la punctul 37 litera (a) numai dacă:

    a) este mulțumită de faptul că obiectul certificărilor sau al rapoartelor de audit acoperă sistemele cheie ale FSC (de exemplu, procesele, aplicațiile, infrastructura, centrele de date etc.), mecanismele de control identificate de societate și conformitatea cu legislația aplicabilă relevantă;
    b) evaluează temeinic și periodic conținutul certificărilor sau rapoartelor de audit și verifică să nu fie caduce rapoartele sau certificările;
    c) se asigură că sistemele-cheie și mecanismele de control importante ale FSC sunt incluse în viitoarele versiuni ale certificărilor sau ale rapoartelor de audit;
    d) este mulțumită de partea care realizează certificarea sau auditul (de exemplu, cu privire la calificările și expertiza acesteia, la reefectuarea/verificarea dovezilor din dosarul de audit subiacent, precum și în ceea ce privește rotația entității de certificare sau de audit);
    e) este mulțumită că certificările sunt emise și auditurile sunt efectuate conform unor standarde corespunzătoare și că includ un test de eficacitate a mecanismelor de control importante implementate;
    f) are dreptul contractual de a solicita extinderea domeniului de aplicare al certificărilor sau al rapoartelor de audit la alte sisteme și mecanisme de control relevante ale FSC; numărul și frecvența acestor cereri de modificare a domeniului de aplicare trebuie să fie rezonabile și legitime din perspectiva administrării riscurilor;
    g) își păstrează dreptul contractual de a efectua audituri individuale la fața locului, la aprecierea proprie, în ceea ce privește funcția externalizată.

40. O societate trebuie să se asigure că, înainte de o vizită la fața locului, inclusiv a unui terț desemnat de societate (de exemplu, un auditor), FSC transmite un preaviz într-un termen rezonabil, cu excepția cazului în care o notificare prealabilă timpurie nu este posibilă din cauza unei situații de urgență sau de criză sau din cauză că ar crea o situație în care auditul nu ar mai fi eficient. Un astfel de preaviz trebuie să includă locația și scopul vizitei, precum și personalul care va participa la vizită.

41. Având în vedere că serviciile cloud prezintă un nivel ridicat de complexitate tehnică și implică anumite provocări de natură jurisdicțională, personalul care efectuează auditul – care poate consta din auditorii săi interni sau din grupul de auditori care acționează în numele său – trebuie să aibă aptitudinile și cunoștințele adecvate pentru a evalua în mod corespunzător serviciile de cloud relevante și a efectua un audit eficient și relevant. Acest lucru trebuie să se aplice și personalului societății, care revizuiește certificările sau rapoartele de audit furnizate de FSC.

Orientarea 7. Subcontractarea externalizării

42. Dacă este permisă externalizarea în lanț a funcțiilor critice sau importante (sau a unor părți semnificative din acestea), acordul scris de externalizare în cloud dintre societate și FSC trebuie:

    a) să precizeze orice parte sau aspect al funcției externalizate care sunt excluse de la potențiala subcontractare;
    b) să indice condițiile care trebuie îndeplinite în cazul subcontractării;
    c) să precizeze că FSC poartă răspunderea și obligația de a supraveghea serviciile pe care le-a subcontractat, pentru a se asigura că toate obligațiile contractuale dintre FSC și societate sunt îndeplinite în permanență;
    d) să includă obligația FSC de a notifica societatea cu privire la orice intenție de subcontractare sau orice modificări semnificative la aceasta, mai ales atunci când acest lucru ar putea afecta capacitatea FSC de a-și îndeplini obligațiile în temeiul angajamentului de externalizare în cloud cu societatea. Perioada de notificare stabilită în acordul scris trebuie să permită societății suficient timp, cel puțin pentru a efectua o evaluare a riscului subcontractării propuse sau a modificărilor semnificative ale acesteia și pentru o contesta sau aproba în mod explicit, după cum se indică la litera (e) de mai jos;
    e) să se asigure că societatea are dreptul de a contesta subcontractarea planificată sau modificările semnificative aduse acesteia sau că este necesară o aprobare explicită înainte de intrarea în vigoare a subcontractării sau a modificărilor semnificative propuse;
    f) să se asigure că societatea are dreptul contractual de a rezilia angajamentul de externalizare în cloud cu FSC în cazul în care contestă subcontractarea propusă sau modificări semnificative aduse acesteia și în cazul unei subcontractări nejustificate (de exemplu, dacă FSC continuă cu subcontractarea fără notificarea societății sau încalcă grav condițiile de subcontractare stipulate în contractul de externalizare).

43. Societatea trebuie să se asigure că FSC supraveghează în mod adecvat subcontractantul.

Orientarea 8. Notificarea scrisă adresată autorităților competente

44. Societatea trebuie să comunice în scris și în timp util autorității sale competente angajamentul planificat de externalizare în cloud care vizează o funcție critică sau importantă. De asemenea, societatea trebuie să notifice în timp util și în scris autoritatea competentă cu privire la angajamentele de externalizare în cloud care privesc o funcție care anterior a fost clasificată ca fiind necritică sau neimportantă, dar apoi a devenit critică sau importantă.

45. Notificarea scrisă a societății trebuie să includă, ținând cont de principiul proporționalității, cel puțin următoarele informații:

    a) data de începere a acordului de externalizare în cloud și, după caz, următoarea dată de reînnoire a contractului, data de încetare și/sau perioadele de preaviz pentru FSC și pentru societate;
    b) o descriere succintă a funcției externalizate;
    c) un scurt rezumat al motivelor pentru care funcția externalizată este considerată critică sau importantă;
    d) numele și numele de marcă (dacă este cazul) al FSC, țara sa de înregistrare, numărul de înregistrare, identificatorul entității juridice (dacă este disponibil), adresa sa înregistrată, datele sale de contact relevante, precum și denumirea societății-mamă (dacă este cazul);
    e) legea de reglementare a angajamentului de externalizare în cloud și, dacă există, alegerea jurisdicției;
    f) modele de implementare în cloud și natura specifică a datelor care trebuie păstrate de FSC și locațiile (și anume, regiunile sau țările) în care vor fi stocate aceste date;
    g) data celei mai recente evaluări a caracterului critic sau a importanței funcției externalizate;
    h) data celei mai recente evaluări a riscului sau a celui mai recent audit al FSC, împreună cu un scurt rezumat al principalelor rezultate, și data următoarei evaluări planificate sau a următorului audit planificat;
    i) persoana fizică sau organul de decizie din cadrul societății care a aprobat angajamentul de externalizare în cloud;
    j) după caz, numele tuturor subcontractanților cărora le sunt subcontractate părți semnificative ale unei funcții critice sau importante, inclusiv țara sau regiunea în care sunt înregistrați subcontractanții, în care va fi furnizat serviciul subcontractat și în care vor fi stocate datele.

Orientarea 9. Supravegherea angajamentelor de externalizare în cloud

46. Autoritățile competente trebuie să evalueze riscurile care decurg din angajamentele de externalizare în cloud ale societăților în cadrul procesului lor de supraveghere. În

special, această evaluare trebuie să se concentreze asupra angajamentelor legate de externalizarea funcțiilor critice sau importante.

47. Autoritățile competente trebuie să fie convinse că pot asigura o supraveghere eficientă, în special atunci când societățile externalizează funcții critice sau importante care sunt efectuate în afara UE.

48. Autoritățile competente trebuie să evalueze, în cadrul unei abordări bazate pe riscuri, dacă societățile:

    a) dețin resursele necesare și au instituit procesele operaționale și de guvernanță relevante pentru a încheia, implementa și supraveghea în mod adecvat și eficient angajamente de externalizare în cloud;
    b) identifică și gestionează toate riscurile relevante asociate externalizării în cloud.

49. Atunci când sunt identificate riscuri de concentrare, autoritățile competente trebuie să monitorizeze evoluția acestor riscuri și să evalueze atât impactul lor potențial asupra altor societăți pe care le supraveghează, cât și stabilitatea pieței financiare.