Smjernice

EBA/GL/2019/04

28. studenoga 2019.

Smjernice EBA-e o upravljanju rizicima IKT-a i sigurnosnim rizicima

Obveze usklađivanja i izvješćivanja

Status ovih smjernica

1. Ovaj dokument sadrži smjernice izdane na temelju članka 16. Uredbe (EU) br. 1093/2010[1]. U skladu s člankom 16. stavkom 3. Uredbe (EU) br. 1093/2010 nadležna tijela i financijske institucije moraju ulagati napore da se usklade s ovim smjernicama.

2. U smjernicama se iznosi EBA-ino stajalište o odgovarajućim nadzornim praksama unutar Europskog sustava financijskog nadzora ili o tome kako bi se pravo Europske unije trebalo primjenjivati u određenom području. Nadležna tijela određena člankom 4. stavkom 2. Uredbe (EU) br. 1093/2010 na koja se smjernice primjenjuju trebala bi se s njima uskladiti tako da ih na odgovarajući način uključe u svoje prakse (npr. izmjenama svojeg pravnog okvira ili nadzornih procesa), uključujući i u slučajevima kada su smjernice prvenstveno upućene institucijama.

Zahtjevi u pogledu izvješćivanja

3. U skladu s člankom 16. stavkom 3. Uredbe (EU) br. 1093/2010 nadležna tijela moraju obavijestiti EBA-u o tome jesu li usklađena ili se namjeravaju uskladiti s ovim smjernicama, odnosno o razlozima neusklađenosti do ([dd.mm.gggg]). U slučaju izostanka obavijesti unutar tog roka, EBA će smatrati da nadležna tijela nisu usklađena. Obavijesti se dostavljaju slanjem ispunjenog obrasca koji se nalazi na internetskoj stranici EBA-e na adresu compliance@eba.europa.eu s naznakom „EBA/GL/2019/04”. Obavijesti bi trebale slati osobe s odgovarajućom nadležnošću za izvješćivanje o usklađenosti u ime svojih nadležnih tijela. Svaka se promjena statusa usklađenosti također mora prijaviti EBA-i.

4. Obavijesti će biti objavljene na internetskoj stranici EBA-e, u skladu s člankom 16. stavkom 3.

[1] Uredba (EU) br. 1093/2010 Europskog parlamenta i Vijeća od 24. studenoga 2010. o osnivanju europskog nadzornog tijela (Europskog nadzornog tijela za bankarstvo), kojom se izmjenjuje Odluka br. 716/2009/EZ i stavlja izvan snage Odluka Komisije 2009/78/EZ, (SL L 331, 15.12.2010., str. 12.).

Predmet, područje primjene i definicije

Predmet

5. Ove se smjernice temelje na odredbama članka 74. Direktive 2013/36/EU (Direktiva o kapitalnim zahtjevima) o internom upravljanju i proizlaze iz ovlasti za izdavanje smjernica utvrđenih u članku 95. stavku 3. Direktive (EU) 2015/2366 (Direktiva PSD2).

6. U ovim su smjernicama utvrđene mjere upravljanja rizikom koje financijske institucije (kako su definirane u točki 9. u nastavku) moraju poduzeti u skladu s člankom 74. Direktive o kapitalnim zahtjevima radi upravljanja svojim rizicima IKT-a i sigurnosnim rizicima za sve djelatnosti te koje pružatelji platnih usluga (kako su definirani u točki 9. u nastavku) u skladu s člankom 95. stavkom 1. Direktive PDS2 moraju poduzeti radi upravljanja operativnim i sigurnosnim rizicima (u daljnjem tekstu: rizici IKT-a i sigurnosni rizici) povezanima s platnim uslugama koje pružaju. Ove smjernice obuhvaćaju zahtjeve za informacijsku sigurnost, uključujući kibersigurnost, u mjeri u kojoj se informacije čuvaju u sustavima IKT-a.

Područje primjene

7. Ove se smjernice primjenjuju u odnosu na upravljanje rizicima IKT-a i sigurnosnim rizicima u financijskim institucijama (kako su definirane u točki 9.). Za potrebe ovih smjernica, pojam rizika IKT-a i sigurnosnih rizika odnosi se na operativne i sigurnosne rizike iz članka 95. Direktive PSD2 za pružanje platnih usluga.

8. Za pružatelje platnih usluga (kako su definirani u točki 9.) ove se smjernice primjenjuju na pružanje platnih usluga u skladu s područjem primjene i ovlaštenjima iz članka 95. Direktive PSD2. Za institucije (kako su definirane u točki 9.) ove se smjernice primjenjuju na sve djelatnosti koje obavljaju.

Adresati

9. Ove su smjernice upućene financijskim institucijama, što za potrebe ovih smjernica znači (1.) pružatelji platnih usluga kako su definirani u članku 4. stavku 11. Direktive PSD2 i (2.) institucije, što znači kreditne institucije i investicijska društva kako su definirana u članku 4. stavku 1. točki 3. Uredbe (EU) br. 575/2013. Ove se smjernice također primjenjuju na nadležna tijela kako su definirana u članku 4. stavku 1. točki 40. Uredbe (EU) br. 575/2013, uključujući Europsku središnju banku u vezi s pitanjima o zadaćama koje su joj dodijeljene Uredbom (EU) br. 1024/2013, te na nadležna tijela u skladu s Direktivom PSD2, kako su navedena u članku 4. stavku 2. točki i. Uredbe (EU) br. 1093/2010.

Definicije

10. Osim ako je drugačije naznačeno, pojmovi upotrijebljeni i utvrđeni u Direktivi 2013/36/EU (Direktivi o kapitalnim zahtjevima), Uredbi (EU) br. 575/2013 (Uredba o kapitalnim zahtjevima)

i Direktivi (EU) 2015/2366 (PSD2) imaju isto značenje u ovim smjernicama. Osim toga, za potrebe ovih smjernica primjenjuju se sljedeće definicije:

Rizik IKT-a i sigurnosni rizik	Rizik gubitaka uslijed povrede povjerljivosti, gubitka integriteta sustava i podataka, neprikladnosti ili nedostupnosti sustava i podataka ili nemogućnosti promjene informacijskih tehnologija (IT-a) unutar razumnog roka i uz razumne troškove u slučaju promjene zahtjeva okruženja ili poslovanja (to jest prilagodljivosti)[2]. To obuhvaća sigurnosne rizike koji proizlaze iz neadekvatnih ili neuspješnih internih postupaka ili vanjskih događaja, uključujući kibernapade ili neadekvatnu fizičku sigurnost.
Upravljačko tijelo	(a) Za kreditne institucije i investicijska društva, ovaj pojam ima isto značenje kao u definiciji navedenoj u članku 3. stavku 1. točki 7. Direktive 2013/36/EU. (b) Za institucije za platni promet ili institucije za elektronički novac ovaj pojam znači direktori ili osobe odgovorne za upravljanje institucijama za platni promet i institucijama za elektronički novac te, ako je to primjenjivo, osobe odgovorne za upravljanje aktivnostima platnih usluga institucija za platni promet i institucija za elektronički novac. (c) Za pružatelje platnih usluga navedene u članku 1. stavku 1. točkama (c), (e) i (f) Direktive (EU) 2015/2366 ovaj pojam ima značenje koje mu je dodijeljeno primjenjivim pravom EU-a ili nacionalnim pravom.
Operativni ili sigurnosni incident	Jedan događaj ili niz povezanih događaja koje financijska institucija nije planirala, a koji imaju ili će vjerojatno imati negativan učinak na cjelovitost, dostupnost, povjerljivost i/ili autentičnost usluga.
Više rukovodstvo	(a) Za kreditne institucije i investicijska društva ovaj pojam ima isto značenje kao u definiciji iz članka 3. stavka 1. točke 9. Direktive 2013/36/EU. (b) Za institucije za platni promet ili institucije za elektronički novac ovaj pojam znači fizičke osobe koje obavljaju izvršne funkcije unutar institucije, a koje su odgovorne i odgovaraju upravljačkom tijelu za svakodnevno upravljanje institucijom. (c) Za pružatelje platnih usluga navedene u članku 1. stavku 1. točkama (c), (e) i (f) Direktive (EU) 2015/2366 ovaj pojam ima značenje koje mu je dodijeljeno primjenjivim pravom EU-a ili nacionalnim pravom.

[2] Definicija iz Smjernica EBA-e o zajedničkim postupcima i metodologijama za postupak nadzorne provjere i ocjene od 19. prosinca 2014. (EBA/GL/2014/13), kako su izmijenjene Smjernicama EBA/GL/2018/03.

Sklonost preuzimanju rizika	Ukupna razina i vrste rizika koje su pružatelji platnih usluga i institucije spremni preuzeti u sklopu svoje sposobnosti podnošenja rizika, u skladu sa svojim poslovnim modelom, kako bi ostvarili svoje strateške ciljeve.
Funkcija revizije	(a) Za kreditne institucije i investicijska društva funkcija revizije jest funkcija kako je navedeno u odjeljku 22. Smjernica EBA-e o internom upravljanju (EBA/GL/2017/11). (b) Za pružatelje platnih usluga koji nisu kreditne institucije funkcija revizije mora biti neovisna u okviru pružatelja platnih usluga ili u odnosu na pružatelja platnih usluga i može biti funkcija interne i/ili vanjske revizije.
IKT projekti	Svaki projekt ili njegov dio u kojem se sustavi i usluge IKT-a mijenjaju, zamjenjuju, odbacuju ili provode. IKT projekti mogu biti dio širih programa IKT-a ili programa transformacije poslovanja.
Treća strana	Organizacija koja je uspostavila poslovne odnose ili sklopila ugovore sa subjektom u svrhu pružanja proizvoda ili usluge.[3]
Informacijska imovina	Skup informacija, materijalnih ili nematerijalnih, koje vrijedi zaštititi.
Imovina IKT-a	Softverska ili hardverska imovina koja se nalazi u poslovnom okruženju.
Sustavi IKT-a[4]	IKT koji je uređen kao dio mehanizma ili međusobno povezane mreže kojima se pruža podrška poslovanju financijske institucije.
Usluge IKT-a[5]	Usluge koje sustavi IKT-a pružaju unutarnjim ili vanjskim korisnicima. Primjeri obuhvaćaju unos podataka, pohranu podataka, obradu podataka i usluge izvješćivanja, ali i usluge praćenja te usluge podrške za potrebe poslovanja i odlučivanja.

[3] Definicija iz temeljnih elemenata skupine G7 za upravljanje kiberrizicima trećih strana u financijskom sektoru.
[4] Definicija iz Smjernica o procjeni rizika IKT-a u okviru postupka nadzorne provjere i ocjene (SREP) (EBA/GL/ 2017/05).
[5] ibid.

Provedba

Datum primjene

11. Ove se smjernice primjenjuju od 30. lipnja 2020.

Stavljanje izvan snage

12. Smjernice o sigurnosnim mjerama za operativne i sigurnosne rizike (EBA/GL/2017/17) izdane tijekom 2017. bit će stavljene izvan snage ovim smjernicama na datum početka primjene ovih smjernica.

Smjernice o upravljanju rizicima IKT-a i sigurnosnim rizicima

1.1. Proporcionalnost

1. Sve financijske institucije trebale bi poštovati odredbe utvrđene u ovim smjernicama na način koji je razmjeran i kojim su uzeti u obzir veličina financijskih institucija, njihova unutarnja organizacija te narav, opseg, složenost i rizičnost usluga i proizvoda koje financijske institucije pružaju ili namjeravaju pružati.

1.2. Upravljanje i strategija

1.2.1. Upravljanje

2. Upravljačko tijelo trebalo bi osigurati da su financijske institucije uspostavile prikladni okvir za interno upravljanje i nadzor za svoje rizike IKT-a i sigurnosne rizike. Upravljačko tijelo trebalo bi odrediti jasne uloge i odgovornosti u pogledu funkcija informacijskih i komunikacijskih tehnologija, upravljanja rizikom informacijske sigurnosti i kontinuiteta poslovanja, uključujući za upravljačko tijelo i njegove odbore.
3. Upravljačko tijelo trebalo bi osigurati da su broj i vještine osoblja financijskih institucija prikladni za pružanje podrške njihovim operativnim potrebama u području IKT-a i postupcima upravljanja rizicima IKT-a i sigurnosnim rizicima na kontinuiranoj osnovi te kako bi se zajamčila provedba njihove strategije IKT-a. Upravljačko tijelo trebalo bi osigurati da je dodijeljeni proračun prikladan za ispunjavanje prethodno navedenog. Nadalje, financijske institucije trebale bi osigurati da svi članovi osoblja, uključujući nositelje ključnih funkcija, prođu odgovarajuće osposobljavanje o rizicima IKT-a i sigurnosnim rizicima, uključujući o informacijskoj sigurnosti, na godišnjoj osnovi ili češće ako je to potrebno (također vidjeti odjeljak 1.4.7.).

4. Upravljačko tijelo općenito je odgovorno za uspostavu, odobravanje i nadzor provedbe strategije IKT-a financijskih institucija u okviru svoje cjelokupne poslovne strategije, kao i za uspostavu učinkovitog okvira za upravljanje rizicima IKT-a i sigurnosnim rizicima.

1.2.2. Strategija

5. Strategija IKT-a trebala bi biti usklađena s cjelokupnom poslovnom strategijom financijskih institucija i u njoj bi trebalo biti definirano sljedeće:

   a) način na koji bi se IKT financijskih institucija trebao razvijati radi učinkovitog pružanja podrške i sudjelovanja u njihovoj poslovnoj strategiji, uključujući razvoj organizacijske strukture, promjene sustava IKT-a i ključne ovisnosti s trećim stranama;
   b) planirana strategija i razvoj arhitekture IKT-a, uključujući ovisnosti o trećim stranama;
   c) jasni ciljevi u pogledu informacijske sigurnosti, s naglaskom na sustave IKT-a i usluge IKT-a, osoblje i postupke.

6. Financijske institucije trebale bi uspostaviti skupove akcijskih planova koji sadrže mjere koje valja poduzeti kako bi se postigao cilj strategije IKT-a. O njima treba obavijestiti cjelokupno relevantno osoblje (uključujući izvođače i treće strane, ako je to primjenjivo i relevantno). Akcijske planove trebalo bi redovito preispitivati kako bi se osigurala njihova relevantnost i prikladnost. Financijske institucije također bi trebale uspostaviti postupke za praćenje i mjerenje učinkovitosti provedbe svoje strategije IKT-a.

1.2.3. Korištenje usluga trećih strana

7. Ne dovodeći u pitanje Smjernice EBA-e za eksternalizaciju (EBA/GL/2019/02) i članak 19. Direktive PSD2, financijske institucije trebale bi osigurati učinkovitost mjera za smanjivanje rizika kako je definirano njihovim okvirom za upravljanje rizicima, uključujući mjere utvrđene u ovim smjernicama, ako su operativne funkcije platnih usluga i/ili usluga IKT-a i sustava IKT-a eksternalizirane, uključujući eksternalizaciju prema subjektima unutar grupe, ili kada se upotrebljavaju usluge treće strane.

8. Kako bi se osigurao kontinuitet usluga IKT-a i sustava IKT-a, financijske institucije trebale bi osigurati da ugovori i sporazumi o razini usluga (i za uobičajene okolnosti i u slučaju prekida usluga – također vidjeti odjeljak 1.7.2.) sklopljeni s pružateljima usluga (pružatelji usluga eksternalizacije, subjekti unutar grupe ili treće strane) uključuju sljedeće:

   a) prikladne i razmjerne ciljeve i mjere u pogledu informacijske sigurnosti, uključujući minimalne zahtjeve u pogledu kibersigurnosti; specifikacije životnog ciklusa podataka financijske institucije; svi zahtjevi u pogledu enkripcije podataka, mrežne sigurnosti i postupaka sigurnosnog praćenja i lokacije podatkovnih centara;
   b) postupke rješavanja operativnih i sigurnosnih incidenata, uključujući postupke eskalacije i izvješćivanja.

9. Financijske institucije trebale bi pratiti i tražiti jamstva razine usklađenosti tih pružatelja usluga sa sigurnosnim ciljevima, mjerama i ciljevima performansi financijske institucije.

1.3. Okvir za upravljanje rizicima IKT-a i sigurnosnim rizicima

1.3.1. Organizacija i ciljevi

10. Financijske institucije trebale bi utvrditi svoje rizike IKT-a i sigurnosne rizike te upravljati njima. Funkcija ili funkcije IKT-a zadužene za sustave, postupke i sigurnosne operacije povezane s IKT-om trebale bi imati uspostavljene odgovarajuće postupke i kontrole kako bi se osiguralo da se svi rizici utvrde, analiziraju, mjere, prate, da se njima upravlja, da se o njima izvješćuje i da je njima ovladano u skladu sa sklonošću preuzimanju rizika financijske institucije te da su projekti i sustavi koje pružaju i aktivnosti koje obavljaju u skladu s vanjskim i unutarnjim zahtjevima.

11. Financijske institucije trebale bi dodijeliti odgovornost za upravljanje rizicima IKT-a i sigurnosnim rizicima te za njihov nadzor kontrolnoj funkciji, u skladu sa zahtjevima iz odjeljka 19. Smjernica EBA-e o internom upravljanju (EBA/GL/2017/11). Financijske institucije trebale bi zajamčiti neovisnost i objektivnost te kontrolne funkcije na način da je na prikladan način odvojena od operativnih postupaka u vezi s informacijskim i komunikacijskim tehnologijama. Ta kontrolna funkcija trebala bi biti izravno odgovorna upravljačkom tijelu i trebala bi biti odgovorna za praćenje i kontrolu pridržavanja okvira za upravljanje rizicima IKT-a i sigurnosnim rizicima. Ta bi funkcija trebala osigurati da se rizici IKT-a i sigurnosni rizici utvrđuju, mjere, procjenjuju, da se njima upravlja, da se prate i da se o njima izvješćuje. Financijske institucije trebale bi zajamčiti da ova kontrolna funkcija nije odgovorna za bilo kakvu internu reviziju.

    Funkcija interne revizije trebala bi, u skladu s pristupom koji se temelji na procjeni rizika, imati sposobnost neovisnog preispitivanja i pružanja objektivnog jamstva usklađenosti svih aktivnosti u području IKT-a i sigurnosnih aktivnosti i jedinica financijske institucije s politikama i postupcima financijske institucije te s vanjskim zahtjevima, uz pridržavanje zahtjeva iz odjeljka 22. Smjernica EBA-e o internom upravljanju (EBA/GL/2017/11).

12. Kako bi okvir za upravljanje rizicima IKT-a i sigurnosnim rizicima bio učinkovit, financijske institucije trebale bi definirati i dodijeliti ključne uloge i odgovornosti te relevantne linije izvješćivanja. Ovaj bi okvir trebao biti u potpunosti integriran i usklađen s cjelokupnim postupcima upravljanja rizikom financijskih institucija.

13. Unutar okvira za upravljanje rizicima IKT-a i sigurnosnim rizicima trebali bi biti uspostavljeni postupci za:

    a) utvrđivanje sklonosti preuzimanju rizika IKT-a i sigurnosnih rizika, u skladu sa sklonošću preuzimanja rizika financijske institucije;
    b) utvrđivanje i procjenjivanje rizika IKT-a i sigurnosnih rizika kojima je financijska institucija izložena;
    c) utvrđivanje mjera za smanjivanje rizika, uključujući kontrole, u svrhu smanjivanja rizika IKT-a i sigurnosnih rizika;
    d) praćenje učinkovitosti tih mjera, kao i broja prijavljenih incidenata, uključujući za pružatelje platnih usluga, incidenata prijavljenih u skladu s člankom 96. Direktive PSD2

koji utječu na aktivnosti povezane s IKT-om i, ako je to potrebno, poduzimanje radnji za ispravljanje tih mjera;

e) izvješćivanje upravljačkog tijela o rizicima IKT-a i sigurnosnim rizicima i kontrolama;

f) utvrđivanje i procjenjivanje postojanja rizika IKT-a i sigurnosnih rizika koji proizlaze iz bilo kakvih većih promjena u sustavu IKT-a ili uslugama, procesima ili postupcima IKT-a i/ili nakon svakog značajnog operativnog ili sigurnosnog incidenta.

14. Financijske institucije trebale bi osigurati da se okvir za upravljanje rizicima IKT-a i sigurnosnim rizicima dokumentira i da se neprestano poboljšava na temelju „naučenih lekcija" tijekom njegove provedbe i praćenja. Upravljačko tijelo trebalo bi najmanje jedanput godišnje odobriti i preispitati okvir za upravljanje rizicima IKT-a i sigurnosnim rizicima.

1.3.2. Utvrđivanje funkcija, procesa i imovine

15. Financijske institucije trebale bi utvrditi, uspostaviti i redovito ažurirati mapiranje svojih poslovnih funkcija, uloga i podržavajućih procesa kako bi se utvrdila njihova pojedinačna važnost i njihova međuovisnost povezana s rizicima IKT-a i sigurnosnim rizicima.

16. Osim toga, financijske institucije trebale bi utvrditi, uspostaviti i redovito ažurirati mapiranje informacijske imovine kojom se pruža podrška njihovim poslovnim funkcijama i podržavajućim procesima, kao što su sustavi IKT-a, osoblje, izvođači i treće strane, te međusobne povezanosti s drugim unutarnjim i vanjskim sustavima i procesima kako bi mogli barem upravljati informacijskom imovinom koja podržava njihove kritične poslovne funkcije i procese.

1.3.3. Klasifikacija i procjena rizika

17. Financijske institucije trebale bi klasificirati utvrđene poslovne funkcije, podržavajuće procese i informacijsku imovinu iz točaka 15. i 16. prema njihovoj kritičnosti.

18. Kako bi se odredila kritičnost tih utvrđenih poslovnih funkcija, podržavajućih procesa i informacijske imovine, financijske institucije trebale bi barem razmotriti zahtjeve u pogledu povjerljivosti, cjelovitosti i dostupnosti. Potrebno je jasno odrediti odgovornost za informacijsku imovinu.

19. Prilikom provedbe procjene rizika, financijske institucije trebale bi preispitati primjerenost klasifikacije informacijske imovine i relevantne dokumentacije.

20. Financijske institucije trebale bi utvrditi rizike IKT-a i sigurnosne rizike koji utječu na utvrđene i klasificirane poslovne funkcije, podržavajuće procese i informacijsku imovinu, u skladu s njihovom kritičnošću. Ta bi se procjena rizika trebala provoditi i dokumentirati na godišnjoj osnovi ili u kraćim razmacima, ako je to potrebno. Takve procjene rizika također bi trebalo provoditi prilikom svake važnije promjene u infrastrukturi, postupaka ili procedura koji utječu na poslovne funkcije, podržavajućih procesa ili informacijske imovine te bi stoga trebalo ažurirati postojeću procjenu rizika financijskih institucija.

21. Financijske institucije trebale bi osigurati da neprestano prate prijetnje i ranjivosti relevantne za njihove poslovne procese, podržavajuće funkcije i informacijsku imovinu te bi trebale redovito preispitivati scenarije rizika koji utječu na njih.

1.3.4. Smanjivanje rizika

22. Na temelju procjene rizika financijske institucije trebale bi utvrditi koje su mjere potrebne kako bi se rizici IKT-a i sigurnosni rizici sveli na prihvatljive razine te jesu li potrebne promjene u postojećim poslovnim procesima, kontrolnim mjerama, sustavima IKT-a i uslugama IKT-a. Financijska institucija trebala bi uzeti u obzir vrijeme potrebno za provedbu tih promjena i vrijeme potrebno za poduzimanje odgovarajućih privremenih mjera za smanjenje rizika IKT-a i sigurnosnih rizika te kako bi ti rizici ostali unutar ograničenja sklonosti preuzimanju rizika IKT-a i sigurnosnih rizika financijske institucije.

23. Financijske institucije trebale bi definirati i provoditi mjere za smanjivanje utvrđenih rizika IKT-a i sigurnosnih rizika te zaštititi informacijsku imovinu u skladu s njezinom klasifikacijom.

1.3.5. Izvješćivanje

24. Financijske institucije trebale bi jasno i pravodobno obavijestiti upravljačko tijelo o ishodima procjene rizika. Takvim izvješćivanjem ne dovodi se u pitanje obveza pružatelja platnih usluga da nadležnim tijelima dostave ažuriranu i sveobuhvatnu procjenu rizika, kako je utvrđeno u članku 95. stavku 2. Direktive (EU) 2015/2366.

1.3.6. Revizija

25. Revizori s dostatnim znanjem, vještinama i stručnošću u području rizika IKT-a i sigurnosnih rizika te u području plaćanja (za pružatelje platnih usluga) trebali bi provoditi redovne revizije upravljanja, sustava i procesa/postupaka povezanih s rizicima IKT-a i sigurnosnim rizicima financijske institucije kako bi upravljačkom tijelu pružili neovisno jamstvo o njihovoj učinkovitosti. Revizori bi trebali biti neovisni unutar financijske institucije ili u odnosu na nju. Učestalost i usmjerenost takvih revizija trebale bi biti razmjerne relevantnim rizicima IKT-a i sigurnosnim rizicima.

26. Upravljačko tijelo financijske institucije trebalo bi odobriti plan revizije, uključujući sve revizije IKT-a i sve značajne izmjene plana. Plan revizije i njegovo izvršenje, uključujući učestalost revizije, trebali bi odražavati i biti razmjerni inherentnim rizicima IKT-a i sigurnosnim rizicima u financijskoj instituciji te bi plan trebalo redovito ažurirati.

27. Potrebno je uspostaviti formalni postupak daljnjih radnji, uključujući odredbe za pravodobnu provjeru i sanaciju kritičnih nalaza utvrđenih revizijom IKT-a.

1.4. Informacijska sigurnost

1.4.1. Politika informacijske sigurnosti

28. Financijske institucije trebale bi razviti i dokumentirati politiku informacijske sigurnosti kojom bi se trebala definirati načela i pravila na visokoj razini za zaštitu povjerljivosti, cjelovitosti i dostupnosti podataka i informacija financijskih institucija i njihovih klijenata. Za pružatelje platnih usluga ta je politika utvrđena u dokumentu o sigurnosnoj politici koji treba donijeti u skladu s člankom 5. stavkom 1. točkom (j) Direktive (EU) 2015/2366. Politika informacijske

sigurnosti trebala bi biti u skladu s ciljevima financijske institucije u pogledu informacijske sigurnosti i na temelju relevantnih rezultata postupka procjene rizika. Upravljačko tijelo trebalo bi odobriti tu politiku.

29. Politika bi trebala sadržavati opis glavnih uloga i odgovornosti upravljanja informacijskom sigurnošću te bi njome trebali biti postavljeni zahtjevi za osoblje i izvođače, postupke i tehnologiju u vezi s informacijskom sigurnošću, pri čemu je utvrđeno da osoblje i izvođači na svim razinama imaju odgovornosti u osiguravanju informacijske sigurnosti financijskih institucija. Politikom bi se trebala osigurati povjerljivost, cjelovitost i dostupnost kritične logičke i fizičke imovine, resursa i osjetljivih podataka financijske institucije, neovisno o tome jesu li u stanju mirovanja, u prijenosu ili upotrebi. Politiku informacijske sigurnosti trebalo bi priopćiti cjelokupnom osoblju i izvođačima financijske institucije.

30. Na temelju politike informacijske sigurnosti financijske institucije trebale bi uspostaviti i provoditi sigurnosne mjere za smanjivanje rizika IKT-a i sigurnosnih rizika kojima su izložene. Te bi mjere trebale obuhvaćati sljedeće:

    a) organizaciju i upravljanje u skladu s točkama 10. i 11.;
    b) logičku sigurnost (odjeljak 1.4.2);
    c) fizičku sigurnost (odjeljak 1.4.3);
    d) sigurnost IKT operacija (odjeljak 1.4.4.);
    e) praćenje sigurnosti (odjeljak 1.4.5.);
    f) provjera, ocjenjivanje i testiranje informacijske sigurnosti (odjeljak 1.4.6.);
    g) osposobljavanje i podizanje razine svijesti o informacijskoj sigurnosti (odjeljak 1.4.7.).

1.4.2. Logička sigurnost

31. Financijske institucije trebale bi definirati, dokumentirati i provoditi postupke za logičku kontrolu pristupa (upravljanje identitetima i pristupom). Te bi postupke trebalo provoditi, izvršavati, pratiti i redovito preispitivati. Postupci bi također trebali obuhvaćati kontrole za praćenje anomalija. Tim bi se postupcima trebalo barem provoditi sljedeće elemente, pri čemu pojam „korisnik" također obuhvaća tehničke korisnike:

    (a) **Načelo nužnosti pristupa informacijama (engl. *need to know*), načelo najmanjih povlastica (engl. *least privilege*) i segregacije dužnosti:** financijske institucije trebale bi upravljati pravima pristupa za informacijsku imovinu i njezinim podržavajućim sustavima na temelju načela nužnosti pristupa informacijama, uključujući pristup na daljinu. Korisnicima bi trebalo dodijeliti najmanja prava pristupa koja su strogo potrebna za izvršavanje njihovih dužnosti (načelo „najmanjih povlastica"), odnosno radi sprečavanja neopravdanog pristupa velikom skupu podataka ili sprečavanja dodjele kombinacija prava pristupa koja bi se mogla upotrebljavati za zaobilaženje kontrola (načelo „segregacije dužnosti").

    (b) **Odgovornost korisnika:** financijske institucije trebale bi u najvećoj mogućoj mjeri ograničiti uporabu generičkih i zajedničkih korisničkih računa te osigurati da se korisnici mogu identificirati u pogledu aktivnosti provedenih u sustavima IKT-a.

(c) **Prava povlaštenog pristupa:** financijske institucije trebale bi provoditi pouzdane kontrole povlaštenog pristupa sustavu na način da će strogo ograničiti i pomno nadzirati račune s povećanim pravima pristupa sustavu (npr. administratorski računi). Kako bi se osigurala sigurna komunikacija i smanjili rizici, administrativni pristup na daljinu kritičnim sustavima IKT-a trebalo bi odobravati samo na temelju načela nužnosti pristupa informacijama i ako se upotrebljavaju pouzdana rješenja za autentifikaciju.

(d) **Evidentiranje aktivnosti korisnika:** trebalo bi evidentirati i pratiti barem sve aktivnosti korisnika s povlaštenim pristupom. Zapise o pristupu trebalo bi osigurati na način da se spriječe neovlaštene izmjene ili brisanje te ih čuvati tijekom razdoblja koje je razmjerno kritičnosti utvrđenih poslovnih funkcija, podržavajućih procesa i informacijske imovine, u skladu s odjeljkom 1.3.3., ne dovodeći u pitanje zahtjeve u pogledu čuvanja podataka utvrđene pravom EU-a i nacionalnim pravom. Financijska institucija trebala bi upotrebljavati te informacije radi olakšavanja utvrđivanja i istraživanja neuobičajenih aktivnosti koje su otkrivene tijekom pružanja usluga.

(e) **Upravljanje pristupom:** prava pristupa trebalo bi pravovremeno odobriti, povući ili izmijeniti, u skladu s prethodno utvrđenim tijekom odobrenja (engl. *approval workflow*) u koji je uključen poslovni vlasnik informacija kojima se pristupa (vlasnik informacijske imovine). U slučaju prestanka radnog odnosa, prava pristupa trebalo bi odmah povući.

(f) **Ponovno certificiranje pristupa:** prava pristupa trebalo bi povremeno preispitivati kako bi se osiguralo da korisnici ne posjeduju prevelike povlastice te da su prava pristupa povučena kada više nisu potrebna.

(g) **Metode autentifikacije:** financijske institucije trebale bi provoditi metode autentifikacije koje su dovoljno pouzdane za primjereno i učinkovito osiguravanje usklađenosti s politikama i postupcima za kontrolu pristupa. Metode autentifikacije trebale bi biti razmjerne kritičnosti sustava IKT-a, informacija ili procesa kojima se pristupa. To bi trebalo uključivati barem složene zaporke ili pouzdanije metode autentifikacije (kao što je autentifikacija na temelju dvaju elemenata) na temelju relevantnog rizika.

32. Elektronički pristup podatcima i sustavima IKT-a putem aplikacija trebao bi biti ograničen na najmanju mjeru potrebnu za pružanje odgovarajuće usluge.

1.4.3. Fizička sigurnost

33. Potrebno je definirati, dokumentirati i provoditi mjere fizičke sigurnosti financijskih institucija radi zaštite njihovih prostorija, podatkovnih centara i osjetljivih područja od neovlaštenog pristupa i opasnosti povezanih s okolišem.

34. Fizički pristup sustavima IKT-a trebalo bi dopustiti samo ovlaštenim pojedincima. Ovlaštenja bi trebalo dodjeljivati u skladu sa zadatcima i odgovornostima pojedinaca te bi ona trebala biti ograničena na osobe koje su primjereno osposobljene i koje se primjereno prati. Fizički pristup trebalo bi redovito preispitivati kako bi se osiguralo brzo povlačenje suvišnih prava pristupa kada za njima više nema potrebe.

35. Odgovarajuće mjere za zaštitu od opasnosti povezanih s okolišem trebale bi biti razmjerne važnosti zgrada i kritičnosti operacija ili sustava IKT-a koji se nalaze u tim zgradama.

1.4.4. Sigurnost IKT operacija

36. Financijske institucije trebale bi provoditi postupke za sprečavanje pojave sigurnosnih problema u sustavima IKT-a i uslugama IKT-a te bi trebale smanjiti njihov utjecaj na pružanje usluga IKT-a. Ti postupci trebaju uključivati sljedeće mjere:

    a) utvrđivanje potencijalnih ranjivosti koje bi trebalo procijeniti i sanirati na način da je osigurano da su softver i ugrađeni programi (engl. firmware) ažurirani, uključujući softver koji financijske institucije pružaju svojim unutarnjim i vanjskim korisnicima, primjenom kritičnih sigurnosnih zakrpa ili provedbom kompenzacijskih kontrola;
    b) implementaciju osnovnih sigurnosnih postavki svih mrežnih komponenti;
    c) implementaciju segmentacije mreže, sustava sprečavanja gubitka podataka i enkripcije mrežnog prometa (u skladu s klasifikacijom podataka);
    d) implementaciju zaštite krajnjih točaka, uključujući poslužitelje, radne stanice i mobilne uređaje; financijske institucije trebale bi procijeniti ispunjavaju li krajnje točke definirane sigurnosne standarde prije nego što im je odobren pristup korporativnoj mreži;
    e) provjeru uspostave mehanizama za potvrdu cjelovitosti softvera, ugrađenih programa i podataka;
    f) enkripciju podataka u mirovanju i u prijenosu (u skladu s klasifikacijom podataka).

37. Financijske institucije trebale bi neprestano utvrđivati utječu li promjene u postojećem operativnom okruženju na postojeće sigurnosne mjere ili je potrebno donošenje dodatnih mjera radi prikladnog smanjivanja povezanih rizika. Te promjene trebale bi biti dio formalnog procesa upravljanja promjenama financijskih institucija kojim bi se trebalo osigurati da su promjene pravilno planirane, testirane, dokumentirane, odobrene i provedene.

1.4.5. Praćenje sigurnosti

38. Financijske institucije trebale bi uspostaviti i provoditi politike i postupke za otkrivanje neuobičajenih aktivnosti koje bi mogle utjecati na informacijsku sigurnost financijskih institucija i na odgovarajući način odgovoriti na te događaje. Kao dio tog kontinuiranog praćenja, financijske institucije trebale bi implementirati primjerene i učinkovite mogućnosti za otkrivanje fizičkih ili logičkih upada te povreda povjerljivosti, cjelovitosti i dostupnosti informacijske imovine. Procesima kontinuiranog praćenja i otkrivanja trebalo bi obuhvatiti:

    a) relevantne unutarnje i vanjske čimbenike, uključujući poslovne funkcije i administrativne funkcije IKT-a;
    b) transakcije radi otkrivanja zlouporaba pristupa koje su počinile treće strane ili drugi subjekti, kao i unutarnjih zlouporaba pristupa;
    c) potencijalne unutarnje i vanjske prijetnje.

39. Financijske institucije trebale bi uspostaviti i provoditi procese i organizacijske strukture za utvrđivanje i neprekidno praćenje sigurnosnih i operativnih prijetnji koje bi mogle značajno

utjecati na njihovu sposobnost pružanja usluga. Financijske institucije trebale bi aktivno pratiti tehnološka kretanja kako bi osigurale da su svjesne sigurnosnih rizika. Financijske institucije trebale bi provoditi mjere za otkrivanje, primjerice mogućih curenja informacija, zlonamjernog softvera i drugih sigurnosnih prijetnji, javno poznatih ranjivosti softvera i računalne opreme te bi trebale provjeravati jesu li dostupna odgovarajuća nova sigurnosna ažuriranja softvera.

40. Postupak praćenja sigurnosti također bi trebao pomoći financijskoj instituciji da razumije narav operativnih ili sigurnosnih incidenata, utvrdi trendove i podupre istrage na razini organizacije.

1.4.6. Provjera, procjenjivanje i testiranje informacijske sigurnosti

41. Financijske institucije trebale bi provoditi različite provjere, procjene i testiranja informacijske sigurnosti kako bi se osiguralo učinkovito utvrđivanje ranjivosti u njihovim sustavima IKT-a i uslugama IKT-a. Primjerice, financijske institucije mogu provoditi analizu nedostataka u odnosu na standarde informacijske sigurnosti, provjere usklađenosti, internih i vanjskih revizija informacijskih sustava ili provjere fizičke sigurnosti. Nadalje, institucija bi trebala razmotriti dobre prakse kao što su provjere/revizije izvornog koda, procjene ranjivosti, penetracijska testiranja i vježbe „crvenog tima" (engl. *red team exercises*).

42. Financijske institucije trebale bi uspostaviti i implementirati okvir za testiranje informacijske sigurnosti kojim se potvrđuju pouzdanost i učinkovitost njihovih mjera informacijske sigurnosti i osigurati da se tim okvirom uzimaju u obzir prijetnje i ranjivosti utvrđene praćenjem prijetnji te postupkom procjene rizika IKT-a i sigurnosnih rizika.

43. Okvirom za testiranje informacijske sigurnosti trebalo bi osigurati da testiranja:

    a) provode neovisni ispitivači s dovoljno znanja, vještina i stručnosti u testiranju mjera informacijske sigurnosti te koji nisu uključeni u razvoj mjera informacijske sigurnosti;
    b) uključuju ispitivanja ranjivosti i penetracijska testiranja (uključujući penetracijska testiranja vođena prijetnjama, ako su potrebna i primjerena) koja su razmjerna razini rizika utvrđenog u poslovnim procesima i sustavima.

44. Financijske institucije trebale bi provoditi kontinuirana i ponavljajuća testiranja sigurnosnih mjera. Za sve kritične sustave IKT-a (točka 17.) ti se testovi trebaju provoditi najmanje jedanput godišnje te će za pružatelje platnih usluga biti dio sveobuhvatne procjene sigurnosnih rizika koji se odnose na usluge platnog prometa koje pružaju u skladu s člankom 95. stavkom 2. Direktive PSD2. Sustavi koji nisu kritični trebali bi se redovito testirati primjenom pristupa koji se temelji na riziku, barem jedanput svake tri godine.

45. Financijske institucije trebale bi osigurati da se testovi sigurnosnih mjera provode u slučaju promjena infrastrukture, procesa ili postupaka te ako su promjene provedene zbog značajnih operativnih ili sigurnosnih incidenata ili zbog isporuke/objave novih ili znatno izmijenjenih kritičnih aplikacija dostupnih putem interneta.

46. Financijske institucije trebale bi pratiti i procjenjivati rezultate provedenih testiranja i u skladu s njima ažurirati svoje sigurnosne mjere, a u slučaju kritičnih sustava IKT-a to bi trebale činiti bez odgađanja.

47. Za pružatelje platnih usluga okvirom za testiranje trebale bi se obuhvatiti i sigurnosne mjere relevantne za 1. platne terminale i uređaje koji se upotrebljavaju za pružanje platnih usluga; 2. platne terminale i uređaje koji se upotrebljavaju za autentifikaciju korisnika platnih usluga; i 3. uređaje i softver koje korisnicima platnih usluga pruža pružatelj platnih usluga za izradu/primanje koda za autentifikaciju.

48. Na temelju uočenih sigurnosnih prijetnji i učinjenih promjena, potrebno je provesti testiranje kako bi se obuhvatili scenariji relevantnih i poznatih potencijalnih napada.

1.4.7. Osposobljavanje i podizanje razine svijesti o informacijskoj sigurnosti

49. Financijske institucije trebale bi uspostaviti programe za osposobljavanje, uključujući periodične programe osviještenosti o sigurnosti, za sve članove osoblja i izvođače kako bi osigurali da su osposobljeni za izvršavanje svojih dužnosti i odgovornosti u skladu s relevantnom sigurnosnom politikom i postupcima u cilju smanjenja ljudskih pogrešaka, krađa, prijevara, zlouporaba ili gubitaka te da znaju kako rješavati rizike povezane s informacijskom sigurnošću. Financijske institucije trebale bi osigurati da se programom osposobljavanja pruži osposobljavanje za sve članove osoblja i izvođače najmanje jedanput godišnje.

1.5. Upravljanje IKT operacijama

50. Financijske institucije trebale bi upravljati svojim IKT operacijama na temelju dokumentiranih i provedenih procesa i procedura (koji za pružatelje platnih usluga obuhvaćaju dokument o sigurnosnoj politici u skladu s člankom 5. stavkom 1. točkom (j) Direktive PSD2) koje je odobrilo upravljačko tijelo. Tim skupom dokumenata trebalo bi se definirati kako financijske institucije upotrebljavaju, prate i nadziru svoje sustave i usluge IKT-a, uključujući dokumentiranje kritičnih IKT operacija te bi se financijskim institucijama trebalo omogućiti ažuriranje popisa imovine IKT-a.

51. Financijske institucije trebale bi osigurati da je izvršavanje njihovih IKT operacija usklađeno sa zahtjevima njihova poslovanja. Kada je to moguće, financijske institucije trebale bi održavati i poboljšati učinkovitost svojih IKT operacija, uključujući, ali ne ograničavajući se na potrebu razmatranja načina na koji bi se moguće pogreške koje proizlaze iz izvršavanja ručnih zadataka svele na najmanju moguću mjeru.

52. Financijske institucije trebale bi provoditi postupke evidentiranja zapisa i praćenja za kritične IKT operacije kako bi se omogućilo otkrivanje, analiza i ispravljanje pogrešaka.

53. Financijske institucije trebale bi ažurirati popis svoje imovine IKT-a (uključujući sustave IKT-a, mrežne uređaje, baze podataka itd.). Popis imovine IKT-a treba sadržavati konfiguraciju imovine IKT-a te veze i međuovisnosti između različite imovine IKT-a, kako bi se omogućili pravilni postupci upravljanja konfiguracijama i upravljanja promjenama.

54. Popis imovine IKT-a trebao bi biti dovoljno detaljan kako bi se omogućila brza identifikacija imovine IKT-a, njezine lokacije, sigurnosne klasifikacije i vlasništva. Trebalo bi dokumentirati međuovisnost imovine kako bi se pomoglo u odgovoru na sigurnosne i operativne incidente, uključujući kibernapade.

55. Financijske institucije trebale bi pratiti životni ciklus imovine IKT-a i upravljati njome kako bi se osiguralo da i dalje ispunjava zahtjeve u pogledu poslovanja i upravljanja rizicima te da im pruža podršku. Financijske institucije trebale bi pratiti podržavaju li vanjski ili interni dobavljači i razvojni inženjeri njihovu imovinu IKT-a te jesu li primijenjene sve relevantne zakrpe i nadogradnje na temelju dokumentiranih postupaka. Potrebno je procijeniti i smanjiti rizike koji proizlaze iz zastarjele ili nepodržane imovine IKT-a.

56. Financijske institucije trebale bi provoditi postupke planiranja i praćenja performansi i kapaciteta kako bi pravodobno spriječile, otkrile i odgovorile na značajne probleme u pogledu rada sustava IKT-a i manjka kapaciteta IKT-a.

57. Financijske institucije trebale bi definirati i provoditi postupke za izradu sigurnosnih kopija i restauraciju podataka i sustava IKT-a kako bi se osiguralo da ih se, ako je to potrebno, može ponovno oporaviti. Opseg i učestalost izrade sigurnosnih kopija trebali bi se utvrditi u skladu sa zahtjevima poslovanja za oporavak i s kritičnošću podataka i sustava IKT-a te se trebaju procjenjivati u skladu s provedenom procjenom rizika. Testiranje postupaka izrade i restauracije podataka sa sigurnosnih kopija trebalo bi provoditi u pravilnim razmacima.

58. Financijske institucije trebale bi osigurati da su sigurnosne kopije podataka i sustava IKT-a pohranjene na siguran način i da su dovoljno udaljene od primarne lokacije na način da nisu izložene istim rizicima.

3.5.1 Upravljanje IKT incidentima i problemima

59. Financijske institucije trebale bi uspostaviti i provoditi postupak upravljanja incidentima i problemima radi praćenja i bilježenja operativnih i sigurnosnih IKT incidenata te kako bi se financijskim institucijama omogućilo da u slučaju prekida pravovremeno nastave ili ponovno krenu obavljati kritične poslovne funkcije i procese. Financijske institucije trebale bi odrediti primjerene kriterije i pragove za klasifikaciju događaja kao operativnih ili sigurnosnih incidenata, kako je navedeno u odjeljku „Definicije" ovih smjernica, kao i rane pokazatelje opasnosti koji bi trebali služiti kao upozorenje o aktiviranju ranog otkrivanja tih incidenata. Takvim kriterijima i pragovima za pružatelje platnih usluga ne dovodi se u pitanje klasifikacija većih incidenata u skladu s člankom 96. Direktive PSD2 i Smjernicama o izvješćivanju o značajnim incidentima u skladu s Direktivom PSD2 (EBA/GL/2017/10).

60. Kako bi se smanjio utjecaj štetnih događaja i kako bi se omogućio pravovremeni oporavak, financijske institucije trebale bi uspostaviti odgovarajuće postupke i organizacijske strukture radi osiguravanja dosljednog i cjelovitog nadzora, postupanja te daljnjeg praćenja operativnih i sigurnosnih incidenata te kako bi se osiguralo da su glavni uzroci utvrđeni i uklonjeni kako bi se spriječio nastanak ponovljenih incidenata. Postupkom upravljanja incidentima i problema trebalo bi se uspostaviti sljedeće:

    a) postupci za utvrđivanje, praćenje, evidentiranje, kategorizaciju i klasifikaciju incidenata u skladu s prioritetom, na temelju kritičnosti poslovanja;
    b) uloge i odgovornosti za različite scenarije incidenta (npr. pogreške, neispravni rad, kibernapadi);

c) postupci upravljanja problemom za utvrđivanje, analizu i rješavanje glavnih uzroka jednog ili više incidenata – financijska institucija trebala bi analizirati operativne ili sigurnosne incidente koji bi mogli utjecati na financijsku instituciju, a koji su utvrđeni ili su nastali u okviru organizacije i/ili izvan nje te bi trebala razmotriti ključne pouke stečene iz tih analiza i u skladu s njima ažurirati sigurnosne mjere;
d) učinkoviti interni komunikacijski planovi, uključujući postupke obavješćivanja o incidentima i postupcima eskalacije, koji obuhvaćaju i pritužbe klijenata povezanih sa sigurnošću, kako bi se osiguralo sljedeće:
    i) incidenti s potencijalno visokim negativnim učinkom na kritične sustave IKT-a i usluge IKT-a prijavljeni su odgovarajućem višem rukovodstvu i višem rukovodstvu u području IKT-a;
    ii) upravljačko tijelo obavještava se na *ad hoc* osnovi u slučaju značajnih incidenata i barem je obaviješteno o učinku, odgovoru i dodatnim kontrolama koje je potrebno definirati zbog nastanka incidenata.
e) postupci odgovora na incidente kako bi se ublažili učinci povezani s incidentima i kako bi se osiguralo da usluga pravodobno postane operativna i sigurna;
f) posebni planovi za vanjsku komunikaciju za kritične poslovne funkcije i procese u svrhu:
    i) suradnje s relevantnim dionicima kako bi se učinkovito odgovorilo na incident i oporavilo od njega;
    ii) pružanja pravodobnih informacija vanjskim stranama (npr. klijentima, drugim sudionicima na tržištu, nadzornom tijelu), kada je to potrebno i u skladu s primjenjivim propisima.

1.6. Upravljanje IKT projektima i promjenama

1.6.1. Upravljanje IKT projektima

61. Financijska institucija trebala bi uspostaviti proces upravljanja programom i/ili projektima kojim su definirane uloge i odgovornosti potrebne za učinkovitu podršku provedbi strategije IKT-a.

62. Financijska institucija trebala bi na odgovarajući način pratiti i smanjivati rizike koji proizlaze iz njihova portfelja IKT projekata (upravljanje programom), također uzimajući u obzir rizike koji mogu proizaći iz međuovisnosti različitih projekata i ovisnosti višestrukih projekata o istim resursima i/ili stručnosti.

63. Financijska institucija trebala bi uspostaviti i provoditi politiku upravljanja IKT projektima u koja obuhvaća barem:

a) ciljeve projekta;
b) uloge i odgovornosti;
c) procjenu rizika projekta;
d) plan, vremenski okvir i korake projekta;
e) ključne etape (engl. *milestones*);
f) zahtjeve za upravljanje promjenama.

64. Politikom upravljanja IKT projektima trebalo bi osigurati da zahtjeve informacijske sigurnosti analizira i odobrava funkcija koja je neovisna od funkcije razvoja.

65. Financijska institucija trebala bi osigurati da su sva područja na koja utječe IKT projekt zastupljena u projektnom timu te da projektni tim raspolaže znanjem potrebnim za osiguravanje sigurne i uspješne provedbe projekta.

66. O uspostavi i napretku IKT projekata i njihovim povezanim rizicima trebalo bi izvješćivati upravljačko tijelo, pojedinačno ili skupno, ovisno o važnosti i veličini IKT projekata , redovito i na *ad hoc* osnovi, kako je to potrebno. Financijske institucije trebale bi uključiti projektni rizik u svoj okvir upravljanja rizicima.

1.6.2. Nabava i razvoj sustava IKT-a

67. Financijske institucije trebale bi izraditi i provoditi postupak kojim se uređuju nabava, razvoj i održavanje sustava IKT-a. Taj bi postupak trebao biti osmišljen korištenjem pristupa koji se temelji na procjeni rizika.

68. Financijska institucija trebala bi osigurati da relevantno tijelo za upravljanje poslovanjem prije svake nabave ili razvoja sustava IKT-a jasno definira i odobri funkcionalne i nefunkcionalne zahtjeve (uključujući zahtjeve u pogledu informacijske sigurnosti).

69. Financijska institucija trebala bi osigurati da su uspostavljene mjere za smanjivanje rizika od nenamjernih promjena ili namjerne manipulacije sustava IKT-a tijekom razvoja i uvođenja u produkcijsko okruženje.

70. Financijske institucije trebale bi definirati metodologiju za testiranje i odobravanje sustava IKT-a prije njihove prve uporabe. Ta bi metodologija trebala uzeti u obzir kritičnost poslovnih procesa i imovine. Testiranjem bi se trebalo osigurati da novi sustavi IKT-a funkcioniraju kao što su predviđeni. Također bi trebale upotrebljavati testna okruženja koja na odgovarajući način odražavaju produkcijsko okruženje.

71. Financijske institucije trebale bi testirati sustave IKT-a, usluge IKT-a i mjere informacijske sigurnosti kako bi se utvrdile moguće sigurnosne slabosti, povrede i incidenti.

72. Financijska institucija trebala bi uvesti odvojena okruženja IKT-a kako bi osigurala primjerenu segregaciju dužnosti i ublažila učinak neprovjerenih promjena u produkcijskim sustavima. Konkretno, financijska institucija trebala bi osigurati odvajanje produkcijskih okruženja od razvojnih, testnih i drugih neprodukcijskih okruženja. Financijska institucija trebala bi osigurati cjelovitost i povjerljivost produkcijskih podataka u neprodukcijskim okruženjima. Pristup produkcijskim podatcima ograničiti na ovlaštene korisnike.

73. Financijske institucije trebale bi provoditi mjere za zaštitu cjelovitosti izvornih kodova sustava IKT-a koji se razvijaju interno. Također bi trebale detaljno dokumentirati razvoj, implementaciju, rad i/ili konfiguraciju sustavâ IKT-a kako bi se smanjila nepotrebna ovisnost o stručnjacima za tu tematiku. Gdje je primjenjivo, dokumentacija sustava IKT-a treba sadržavati barem korisničku dokumentaciju, tehničku dokumentaciju sustava i operativne postupke.

74. Postupci nabave i razvoja sustavâ IKT-a financijskih institucija također bi se trebali primjenjivati i na sustave IKT-a koje razvijaju ili kojima upravljaju krajnji korisnici poslovne funkcije izvan organizacije IKT-a (npr. računalne aplikacije za krajnje korisnike) primjenom pristupa koji se temelji na procjeni rizika. Financijska institucija trebala bi voditi registar ovakvih aplikacija koje su podrška kritičnim poslovnim funkcijama ili procesima.

1.6.3. Upravljanje IKT promjenama

75. Financijske institucije trebale bi uspostaviti i provoditi postupak upravljanja IKT promjenama u kako bi se osiguralo da se sve promjene sustavâ IKT-a bilježe, testiraju, procjenjuju, odobravaju, provode i provjeravaju na kontrolirani način. Financijske institucije trebale bi postupati s promjenama tijekom izvanrednih situacija (tj. promjene koje se moraju uvesti što je prije moguće) slijedeći postupke kojima se pružaju odgovarajuće zaštitne mjere.

76. Financijske institucije trebale bi utvrditi utječu li promjene u postojećem operativnom okruženju na postojeće sigurnosne mjere te je li potrebno donošenje dodatnih mjera za smanjivanje povezanih rizika. Te bi promjene trebale biti u skladu s formalnim postupkom upravljanja promjenama financijskih institucija.

1.7. Upravljanje kontinuitetom poslovanja

77. Financijske institucije trebale bi uspostaviti dobar proces za upravljanje kontinuitetom poslovanja kako bi u najvećoj mogućoj mjeri osigurali svoje sposobnosti za neprekidno pružanje usluga te kako bi ograničile gubitke u slučaju poremećaja (prekida) poslovanja u skladu s člankom 85. stavkom 2. Direktive 2013/36/EU i glavom VI. Smjernica EBA-e o internom upravljanju (EBA/GL/2017/11).

1.7.1. Analiza utjecaja na poslovanje

78. U okviru dobrog upravljanja kontinuitetom poslovanja, financijske institucije trebale bi provoditi analizu utjecaja na poslovanje (engl. BIA) analiziranjem svoje izloženosti znatnijim prekidima poslovanja i procjenom njihovih potencijalnih učinaka (uključujući na povjerljivost, cjelovitost i dostupnost), kvantitativno i kvalitativno, uporabom unutarnjih i/ili vanjskih podataka (npr. podatci trećih strana relevantni za poslovni proces ili javno dostupni podatci koji mogu biti relevantni za analizu utjecaja na poslovanje) i analizu scenarija. U analizi utjecaja na poslovanje također treba razmotriti pitanje kritičnosti utvrđenih i klasificiranih poslovnih funkcija, podržavajućih procesa, trećih strana i informacijske imovine te njihovih međuovisnosti, u skladu s odjeljkom 1.3.3.

79. Financijske institucije trebale bi osigurati da su njihovi sustavi IKT-a i usluge IKT-a osmišljeni i usklađeni s njihovom analizom utjecaja na poslovanje, primjerice s redundantnošću određenih kritičnih komponenti kako bi se spriječili prekidi izazvani događajima koji utječu na te komponente.

1.7.2. Planiranje kontinuiteta poslovanja

80. Na temelju svoje analize utjecaja na poslovanje, financijske institucije trebale bi uspostaviti planove za osiguravanje kontinuiteta poslovanja (planovi kontinuiteta poslovanja), na način da su dokumentirani i odobreni od njihovih upravljačkih tijela. U planovima bi se osobito trebali uzeti u obzir rizici koji bi mogli negativno utjecati na sustave IKT-a i na usluge IKT-a. Tim planovima trebali bi se održavati ciljevi za zaštitu i, ako je to potrebno, ponovnu uspostavu povjerljivosti, cjelovitosti i dostupnosti njihovih poslovnih funkcija, podržavajućih procesa i informacijske imovine. Ako je to potrebno, tijekom uspostave tih planova financijske bi se institucije trebale koordinirati s relevantnim unutarnjim i vanjskim dionicima.

81. Financijske institucije trebale bi uspostaviti planove kontinuiteta poslovanja kako bi osigurale da mogu primjereno reagirati na moguće scenarije propasti i da mogu ponovno uspostaviti rad svojih kritičnih poslovnih aktivnosti nakon prekida unutar ciljanog vremena oporavka (engl. *RTO*, odnosno najduljeg razdoblja unutar kojeg se sustav ili proces mora ponovno uspostaviti nakon incidenta) i ciljane točke oporavka podataka (engl. *RPO*, odnosno najduljeg vremenskog razdoblja tijekom kojeg je prihvatljivo da su podatci izgubljeni u slučaju incidenta). U slučajevima znatnijeg prekida poslovanja koji zahtijevaju pokretanje konkretnih planova kontinuiteta poslovanja, financijske institucije trebale bi prioritizirati aktivnosti kontinuiteta poslovanja primjenom pristupa koji se temelji na riziku, koji se može temeljiti na procjenama rizika koje se provode u skladu s odjeljkom 1.3.3. Za pružatelje platnih usluga to može uključivati, na primjer, podupiranje daljnje obrade kritičnih transakcija, pri čemu se i dalje ulažu napori usmjereni na oporavak.

82. Financijska institucija u svojem bi planu kontinuiteta poslovanja trebala bi razmotriti čitavi niz različitih scenarija kojima bi mogla biti izložena, uključujući ekstremne, ali moguće scenarije, te procijeniti potencijalni učinak koji bi ti scenariji mogli imati. Na temelju tih scenarija financijska institucija trebala bi opisati kako se osiguravaju kontinuitet sustava i usluga IKT-a, kao i informacijska sigurnost financijske institucije.

1.7.3. Planovi za odgovor i oporavak

83. Na temelju analize utjecaja na poslovanje (točka 78.) i mogućih scenarija (točka 82.) financijske institucije trebale bi izraditi planove za odgovor i oporavak. Tim bi se planovima trebalo utvrditi koji uvjeti mogu potaknuti aktiviranje planova i koje bi se mjere trebale poduzeti kako bi se osigurali dostupnost, kontinuitet i oporavak barem kritičnih sustava IKT-a i usluga IKT-a financijskih institucija. Planovi za odgovor i oporavak trebali bi biti usmjereni prema postizanju ciljeva oporavka poslovanja financijskih institucija.

84. U planovima za odgovor i oporavak trebale bi se razmotriti kratkoročne i dugoročne mogućnosti oporavka. Planovi bi trebali biti:

    a) usmjereni na oporavak operacija kritičnih poslovnih funkcija, podržavajućih procesa, informacijske imovine i njihove međuovisnosti kako bi se izbjegli štetni učinci na funkcioniranje financijskih institucija i financijski sustav, uključujući platne sustave i

korisnike platnih usluga, te kako bi se osiguralo izvršenje platnih transakcija koje su u tijeku;

b) dokumentirani i stavljeni na raspolaganje poslovnim jedinicama i jedinicama za podršku te lako dostupni u izvanrednim situacijama;
c) ažurirani u skladu s poukama stečenima iz incidenata, testiranja, novih utvrđenih rizika i prijetnji te promijenjenih ciljeva i prioriteta oporavka .

85. U planovima bi se također trebale razmotriti alternativne mogućnosti u slučajevima u kojima oporavak možda neće biti izvediv u kratkoročnom razdoblju zbog troškova, rizika, logistike ili nepredviđenih okolnosti.

86. Nadalje, u okviru planova za odgovor i oporavak financijska institucija trebala bi razmotriti i provoditi mjere za osiguranje kontinuiteta kako bi ublažila slučajeve propasti trećih strana, koji su od ključne važnosti za kontinuitet pružanja usluga IKT-a financijskih institucija (u skladu s odredbama Smjernica EBA-e o eksternalizaciji (EBA/GL/2019/02) u vezi s planovima kontinuiteta poslovanja).

1.7.4. Testiranje planova

87. Financijske institucije trebaju povremeno testirati svoje planove kontinuiteta poslovanja. Posebno bi trebale osigurati da se planovi kontinuiteta poslovanja njihovih kritičnih poslovnih funkcija, podržavajućih procesa, informacijske imovine i njihove međuovisnosti (uključujući one koje pružaju treće strane, ako je to potrebno) testiraju barem jedanput godišnje u skladu s točkom 89.

88. Planove kontinuiteta poslovanja potrebno je ažurirati najmanje jedanput godišnje, na temelju rezultata testiranja, aktualnih saznanja o prijetnjama i pouka stečenih iz prethodnih događanja. Ako je to potrebno, sve promjene u pogledu ciljeva oporavka (uključujući zadana ciljana vremena oporavka i ciljane točke oporavka podataka) i/ili promjena poslovnih funkcija, podržavajućih procesa i informacijske imovine, također bi se trebale smatrati osnovom za ažuriranje planova kontinuiteta poslovanja.

89. Financijske institucije bi testiranjem svojih planova kontinuiteta poslovanja trebale pokazati kako mogu osigurati održivost svojeg poslovanja sve dok se ponovno ne uspostave kritične operacije. Posebno bi trebale:

    a) obuhvaćati testiranje prikladnog niza ozbiljnih, ali mogućih scenarija, uključujući one koji su uzeti u obzir prilikom izrade planova kontinuiteta poslovanja (kao i testiranje usluga koje pružaju treće strane, ako je to primjenjivo); ovo bi trebalo obuhvaćati prebacivanje kritičnih poslovnih funkcija, podržavajućih procesa i informacijske imovine u okruženje za oporavak od katastrofe (engl. *disaster recovery environment*) te bi se trebalo dokazati da se može održati ovaj način tijekom dostatno reprezentativnog vremenskog razdoblja i da se nakon toga može ponovno uspostaviti uobičajeni rad;
    b) biti osmišljeni na način da se njima preispituju pretpostavke na kojima se temelje planovi kontinuiteta poslovanja, uključujući sustave upravljanja i planove za komuniciranje u kriznim situacijama i
    c) obuhvaćati postupke za provjeru sposobnosti njihova osoblja i izvođača, sustava IKT-a i usluga IKT-a da na odgovarajući način odgovore na scenarije definirane u točki 89. podtočki (a).

90. Rezultate testiranja treba dokumentirati, a sve utvrđene nedostatke koji proizlaze iz testiranja treba analizirati, obraditi i o njima izvijestiti upravljačko tijelo.

1.7.5. Komuniciranje u kriznim situacijama

91. U slučaju prekida poslovanja ili izvanredne situacije te tijekom provedbe planova kontinuiteta poslovanja, financijske institucije trebale bi osigurati postojanje učinkovitih mjera za komuniciranje u kriznim situacijama kako bi svi relevantni interni i vanjski dionici, uključujući nadležna tijela kad je to propisano nacionalnim propisima te vanjske pružatelje usluga (pružatelje usluga eksternalizacije, subjekte u okviru grupe ili treće strane), bili pravodobno i primjereno informirani.

1.8. Upravljanje odnosima s korisnicima platnih usluga

92. Pružatelji platnih usluga trebali bi uspostaviti i provoditi procese za jačanje svijesti korisnika platnih usluga o sigurnosnim rizicima povezanim s platnim uslugama osiguravanjem pomoći i smjernica korisnicima platnih usluga.

93. Pomoć i smjernice koje se nude korisnicima platnih usluga trebale bi se ažurirati s obzirom na nove prijetnje i ranjivosti, a o promjenama bi trebalo obavještavati korisnike platnih usluga.

94. Ako je to dopušteno u okviru funkcionalnosti proizvoda, pružatelji platnih usluga trebali bi dopustiti korisnicima platnih usluga da onemoguće određene platne funkcionalnosti povezane s platnim uslugama koje pružatelj platnih usluga pruža korisniku platnih usluga.

95. Ako je pružatelj platnih usluga, u skladu s člankom 68. stavkom 1. Direktive (EU) 2015/2366, pristao na ograničenja potrošnje platitelja za platne transakcije izvršene putem određenog platnog instrumenta, pružatelj platnih usluga trebao bi platitelju omogućiti da prilagodi ta ograničenja do iznosa najvišeg dogovorenog ograničenja.

96. Pružatelji platnih usluga trebali bi omogućiti da korisnici platnih usluga primaju upozorenja o iniciranju ili neuspjelim pokušajima iniciranja platnih transakcija čime im se omogućuje da otkriju prijevarno ili zlonamjerno korištenje njihovim računima.

97. Pružatelji platnih usluga trebali bi informirati korisnike platnih usluga o ažuriranjima u pogledu sigurnosnih postupaka koja utječu na korisnike platnih usluga s obzirom na pružanje platnih usluga.

98. Pružatelji platnih usluga trebali bi korisnicima platnih usluga pružiti pomoć s obzirom na sva pitanja, zahtjeve za podršku i obavijesti o nepravilnostima ili problemima u pogledu sigurnosnih pitanja povezanih s platnim uslugama. Korisnici platnih usluga trebali bi biti primjereno informirani o tome kako je moguće dobiti tu pomoć.